Indonesian Journal of Electrical Engineering and Computer Science
Vol. 19, No. 1, July 2020, pp. 526~534
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v19.i1.pp526-534

Secure vehicle to vehicle voice chat based MQTT and coap internet of things protocol

Noor A. Hussein, Mohamed Ibrahim Shujaa
Department of Computer Engineering Techniques, Electrical Engineering Technical College, Iraq

Article Info

Article history:

Received Oct 15, 2019
Revised Dec 11, 2019
Accepted Jan 13, 2020

Keywords:

CoAP Protocol
DNA
Internet of things
LFSR
MQTT Protocol
OTP
Raspberry pi
Speech recognition
V2V
VANET
Voice chat

ABSTRACT

The congestion of road traffic is one of the most problems facing the ambulance transportation to provide fast healthcare service for patient. In this work, ambulance tracking with messages transfer system has been designed and implemented such that a central monitoring and tracking unit can observe ambulance using MQTT IoT protocol. Where each vehicle is occupied with an intelligent embedded system (Raspberry Pi) unit. When an ambulance is being in the road, it will communicate with other vehicle or road traffic by means of CoAP IoT protocol as a direct device to device communication. The proposed system has been designed such that driver use voice chat and the system are completely hand free. The voice message is being transfer into text by using speech recognition based Google API library, and then the received text message is converted again to speech by using text to speech algorithm. An encryption–decryption process-based stream cipher has been used. The message between IoT nodes has been 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.

Corresponding Author:

Noor A.Hussein,
Department of Computer Engineering Techniques,
Electrical Engineering Technical College, MTU, Baghdad, Iraq.
Email: Noor.alaa.hussein@gmail.com

1. INTRODUCTION

Internet of things (IoT) can be considered as physical devices with feasibility of internet connectivity such that these "things" can upload, download, and share information between them, [1]. Such system can connect sensors which help in monitoring and control any electrical or mechanical system. It is an intelligent network for different smart devices which communicate by means of wire or wireless connectivity through the internet to achieve the required goal [2]. Generally speaking, IoT deals with three things: Sensing and data processing locally, data sharing and transfer between IoT nodes (or nodes with servers), data analysis in servers. Different IoT protocols are available to improve the connectivity and reliability the networks such as MQTT, REST, CoAP, etc. such network require to share a huge information which might use 4G or 5G network to satisfy these requirement [3]. Some application of IoT is adopted such as internet of healthcare (IoTH), industrial internet of things (IIoT), smart cities, environmental monitoring, etc.

Vehicle Ad-Hoc network (VANET) is one of the most attracted applications of IoT which is growing rapidly since its offer safety enhanced. VANETs are an emerging type of network which facilities communication between vehicles on road. This application is one of the important elements of intelligent transportation system (ITSs) [4]. It consists of vehicles and roadside equipment that is able to communicate between each other by wireless and multi-hop communication. A large with rapid development of the IoT application, security of IoT is an important issue among which threats that can exploit some possible weakness [5]. IoT, security are divided into two parts: first the security of communication network which

require securing the network from any intruder device which can send or receive information in the network, hence an authentication and authorization mechanism is required. Secondly, the information itself should be secure also by means of encryption techniques. Cryptography is mainly used to secure information by sharing secret key over different devices. Two type of key are available, symmetric and asymmetric [6]. In symmetric keys are used on both sides sender and receiver while, in asymmetric two different keys are used. Well known symmetric key algorithms are AES, DES, and OTP while RSA, ECC and Diffe-Hellman are known asymmetric. Different techniques are available for key generation; one of the most used is Linear Feedback Shift Register (LFSR) which is used to generate stream series of key according to the required polynomial and number of bits. Cryptography may change 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 [7, 8].

Traditional ambulance uses phone call to provide the required tasks, also the ambulance uses the sireon to inform other vehicle in the road which cause a disturbance to patient and other peoples in the street. In this work, ambulance tracking with secure data transfer system has been design and implemented such that a central monitoring and tracking unit can observe ambulance using MQTT protocol. Where each vehicle is provided with an embedded system (Raspberry pi3) unit. When an ambulance is being in the road it will communication with other vehicles or road traffic by means of CoAP protocol. Chat between drivers has been designed and implemented using speech recognition library based Google API.

2. LITERATURE SURVEY

Road congestion is one of the most issues that cause delay especially for services provide by authorities. This problem has taken more attention for researches to provide different solutions. Mektoubi et al., [9] propose base an mqtt protocol for secured communication of data and key exchanges in IoT network. Huang et al., [10] propose a publish-subscribe pattern to preserve privacy in fog computing using (CoAP) application protocol. Venkatesh et al., [11] introduce an IoT scenario to clear the traffic light by sending a command such that the ambulance would have a clear path without any delay. They used an embedded system to control traffic light. Mittal et al., [12] proposed smart home system with multi-function where voice commands are used to control the home appliances. The proposed system can recognize user voice independent of the accent with a dedicated hardware module. The proposed system can be used by counselor to record speech of patent and convert it to text in data base system.

Misbahuddin et al., [13] proposed a central monitoring and control system using the internet for traffic management system for smart city controlled by traffic using smartphone. Ahsan et al., [14] proposed a wireless detection, and monitoring system for vehicle speed. An intelligent wireless monitoring is designed to identify speed of vehicle with a protocol laboratory environment which produces random data of vehicle speed. Dhall et al., [15] discussed the connected cars concept for car maintenance they uses MQTT protocol to implement the predictive system by sharing different types of data with backend application.

An encryption technique has been proposed by Anwar et al., [16] which uses symmetric key exchange, DNA computing hybridization, and one time pad technique. Begum et al., [17] propose a hybrid cryptography algorithm using One Time Pad, RSA, and DNA computing for text hiding and protection for attackers. Wardana and Perdana et al. [18] propose an access control security system in IoT which uses MQTT protocol for communication and fog computing architecture.

3. PRELIMINARIES

3.1. IoT protocols

IoT protocols can be divided into four basic categories which are: application, service discovery, infrastructure, and other influential protocols [19]. 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 [20].

Table 1. IoT Standard protocols

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		

3.2. MQTT protocol

The message Queuing Telemetry Transport (MQTT) protocol is a machine to machine M2M protocol runs over TCP/IP. It uses a publish/subscribe model between IoT nodes. A broker (cloud server) is the station where the publisher node sends their messages in a specific topic and the client node check the topics [21]. Nodes may subscribe in some topics and not in other topics. 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 [22]. In this work, messages are transfer between central monitoring and central unit and ambulances has been encrypted in publisher node and decrypted in the subscriber side using One Time Pad (OTP) technique and DNA computing. Figure 1 Show schematic diagram at MQTT protocol.

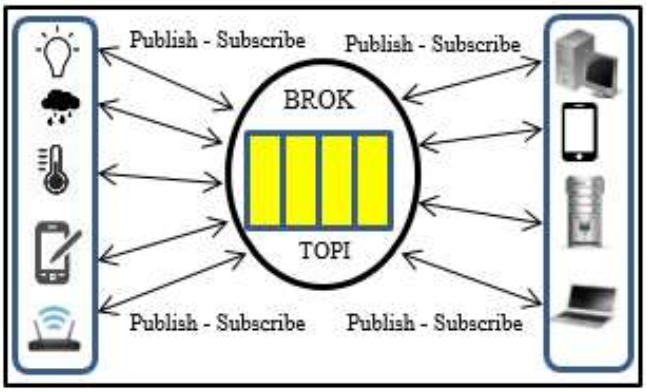


Figure 1. Schematic diagram at MQTT protocol

3.3. CoAP protocol

CoAP is one of IoT protocol which is a light weight RESTful designed for devices with constrained resource such as computation and storage. Its work is based on UDP protocol with the some server-client scheme as in http. It consists of two sublayer structure: "request-response" and "message" respectively. The request-response layer is the same work of http which handles pairs request and response using tokens. The other sublayer "message" is designed to manage message exchanges between end points with reliable delivery. The CoAP protocol consists of a standard method which is GET, POST, PUT, AND DELET [23]. Figure 2 show a schematic diagram of CoAP protocol.

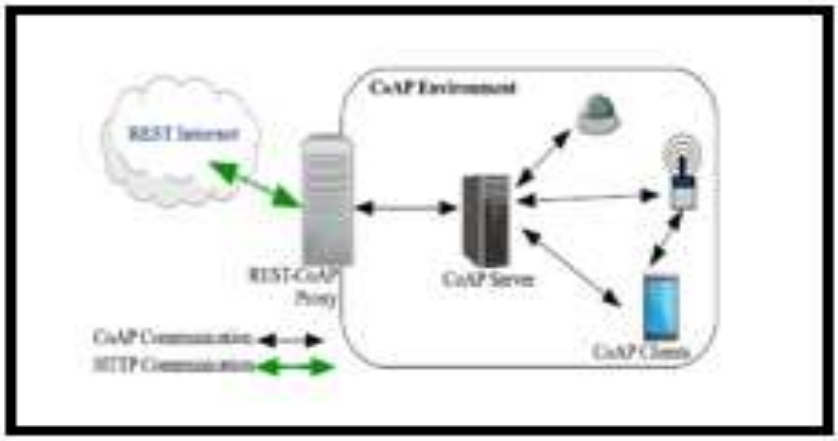


Figure 2. Show a schematic diagram of CoAP protocol

3.4. 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 [24]. 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 [25]:

$$Message = mi = m1, m2, m3, \ldots, mn, mi \in [0,1] \quad (1)$$

the key sequence by PRNG is:

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

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:

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

3.5. 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 shown in Figure 3 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 [26, 27]. (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. Such that A=00; T=01; C=10; and G=11.

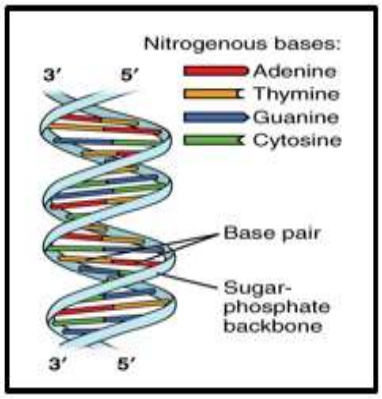


Figure 3. DNA Structure

Table 2. Addition operation for the DNA

+	**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

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

3.6. 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 4 shows a 16 bit LFSR, the characteristic polynomial is $x^{16} + x^{15} + x^{13} + x^4 + 1$ [28]. 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).

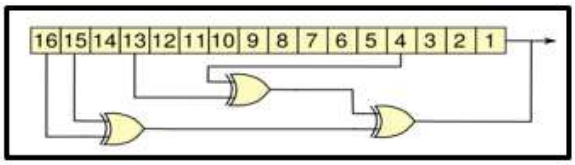


Figure 4. A-16 bit LFSR

4. PROPOSED SYSTEM DESIGN

Figure 5. Shows system design; it consists of a control and emergency monitoring and tracking CEMT which monitor and communicate with ambulance by using MQTT protocol. The CMET is located in the hospital, its responsibility is to send command and arrange the work of ambulance if there any emergency case. Also, it tracks the ambulance when moving in the city. Each ambulance vehicle can communicate with other cars on the road as a (V2V) by means of voice to text and text to voice; this has been done by using CoAP along with MQTT protocol. The proposed system works as follows:

a. When an emergency case is happened for a patient. The CMET send a message to ambulance in the hospital via mqtt. The message structure is shown in Figure 6. Which include task such as the location of the patient and his status, etc.
b. When an ambulance moves to the patient location, it will send its latitude and longitude to the CMET which will convert it to a location in the maps. For this, a google maps has been used and a python library "geopy" is used.

c. In any region, the ambulance will broadcast its IP address and a list of parts for communication using MQTT message such that vehicle in this region will receive these data.
d. Ambulance driver can now start conversation with other cars by sending voice message. Which would be converting into a text message and send to other vehicle using CoAP.
e. Vehicles receives text message and convert it into a speech message such that the driver's vehicle respond to the required command.

In this work, four commands have been proposed namely: "Forward", "Right", "Left" and "Finish". If the ambulance drivers want to speed up forward and there are some vehicles in front of the ambulance, he can send speech command message "forward". This message is converted into a text message and sent to all cars. When vehicle receive an encrypted text message, it will converts it into a speech message again. The final goal of this work is to implement a hard free personal assistance for vehicle a driver which uses speech recognition to convert speech into text and in the other side (other vehicles) convert the text into speech. By doing so, the proposed system will not effect on the drivers focus on the road. The proposed system is achieved by using different libraries based python such as: speech recognition, Pyaudio and espeak. The speeches recognizer has been designed by using Google's speech recognition application interface (API). Figure 6 show a standard message format for ambulance: provided by central monitoring units which consists of task number, patent location, patent status, etc.

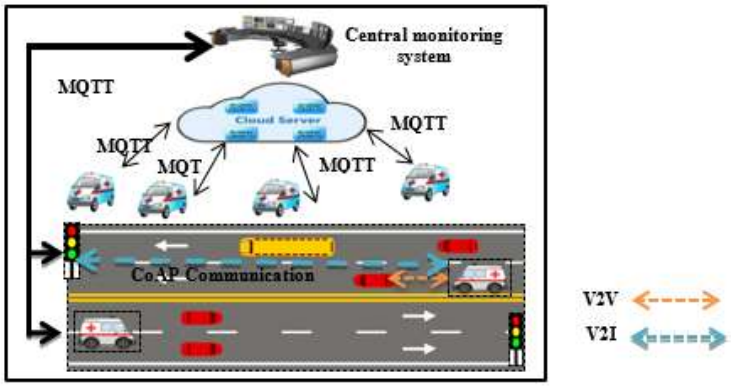


Figure 5. Propose system design

Contact name	: Noor alaa
Task No.	: BG096002
Location Patient	: Saydia
Proposed path	: Emergency Event
Patient (Gender, Name, Age)	: Male, Ali, 55
Status Patient	: Dangerous
Accident Type	: Car Accident

Figure 6. Standard message for vehicle ambulance

5. RESULTS AND DISUSSION

The encryption works in the following steps:

- Convert the plain text into a binary form. For example a message "hello world" is converted to:
1000000000001011100000000000101101000000000001010100000000000110100000000000100101000000000001100101000000000111001010000000011110010100000000111100101000000011111001010000001011110010100000011011

- 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:

AAAATCCAAAAATCTTAAAATCGAAAAATCGAAAAATCGGAAAAACAAAAAATGTGAAAATC GAA AATGACAAAATCGAAAAATCTA

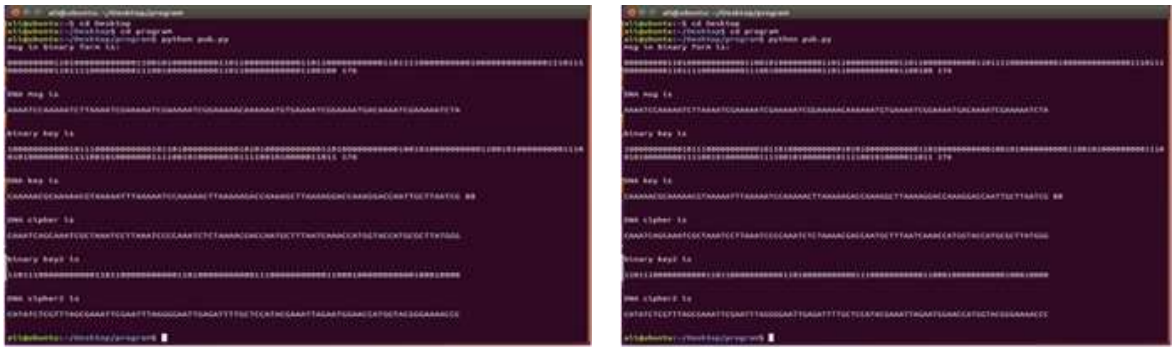
- Generate a PRNG using the 16-bit LFSR which will generate an array with 16-bit binary of each element. In this step, an algorithm is used to combine these numbers to generate a binary sequence with a length equal to the length of the original binary plain text message:
1000000000001011100000000000101101000000000001010100000000000110100000000000100101000000000011001010000000001110010100000000111100101000000011111001010000001011110010100000110 11

- The binary key message is also encoded into a genome sequence in the same manner in step 2:
CAAAAACGCAAAAACGTAAAAATTTAAAAATCCAAAAACTTAAAAAGACCAAAAGCTTAAAA GA CCAAAGGACCAATTGCTTAATCG

- By using Table 2 (Addition rules) then the DNA sequence is:
CAAATCAGCAAATCGCTAAATCCTTAAATCCCCAAATCTCTAAAACGACCAATGCTTTAATC AACC ATGGTACCATGCGCTTATGGG

- 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):
1101110000000000011011000000000001101000000000011100000000000110001000000000001000100 000

- 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 Figure 7, Table 2 (Addition rules), Table 3 (Subtraction rules) are used:
CATATCTCGTTTAGCGAAATTCGAATTTAGGGGAATTGAGATTTTGCTCCATACGAAATTAG AATGGAACCATGGTACGGGAAAACCC



(a) (b)

Figure 7. System implementation, a) encryption process, b) decryption process

Information security is one of te 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.

The proposed system has been designed and implemented to track and monitor the ambulances while it moves in the roads by solving the congestion by prevent using traditional siren. Two IoT protocols have been used which are MQTT and CoAP. The MQTT use publish/subscribe scheme which is used to transfer messages between monitoring and ambulance while the CoAP use for direct communication between ambulance and vehicles in the road. Figure 8(a and b) shows the methods used which are GET and PUT while Figure 8(c) show the server side implementation. The proposed system show good results where fast and reliable data transfer has been achieved.

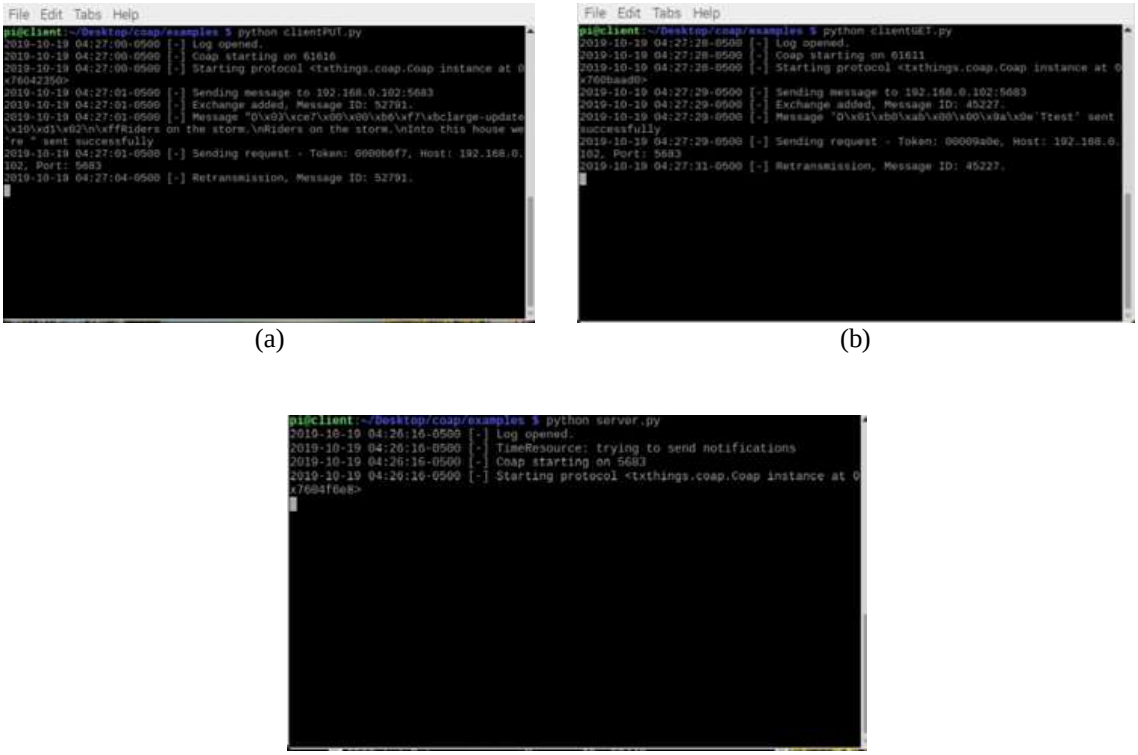


Figure 8. Implementation of CoAP protocol, a) PUT method, b) GET, c) Server

6. CONCLUSION

In this work, a secure message between ambulance and central emergency monitoring and tracking unit based MQTT IoT protocol and other vehicles in the road using CoAP IoT protocol. The message has been encrypted using OTP and DNA computing. The proposed work shows fast encryption/decryption process where the main point in this work is to not affect the overall process of the system and guaranteed emergency services on time. Key generation based on LFSR is not good enough since it suffers from key repetation which has been solved in this work by combining different key to generat a single key.

REFERENCES

[1] Ray, P. P., "A survey on Internet of Things architectures," *Journal of King Saud Universit Computer and Information Sciences*, vol. 30, no. 3, pp. 291-319, July 2018.
[2] Kamaruddin, F., Malik, N. N. N. A., Murad, N. A., Latiff, N. M. A. A., Yusof, S. K. S. and Hamzah, S. A., "IoT-based intelligent irrigation management and monitoring system using arduino," *TELKOMNIKA*, vol. 17, no. 5, pp. 2378-2388, October 2019.
[3] Li, S., Da Xu, L. and Zhao, S., "5G Internet of Things: A survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1-9, June 2018.
[4] Eze, E. C., Zhang, S. J., Liu, E. J., Eze, J. C.," Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development," *International Journal of Automation and Computing*, vol. 3, no. 1, pp.1-18, January 2016.
[5] laba, 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, June 2017.
[6] Pereira, G. C., Alves, R. C., Silva, F. L. D., Azevedo, R. M., Albertini, B. C. and Margi, C. B., "Performance evaluation of cryptographic algorithms over IoT platforms and operating systems," *Security and Communication Networks*, vol. 2017, pp. 16, August 2017.
[7] Azuaje, R., "Securing IoT: Hardware vs Software," *Journal of Advances in Information Technology*, vol. 9, no. 3, pp. 79-83, August 2018.
[8] Sari. C. A., Ardiansyah. G., Setiadi. D. R., Rachmawanto, E. H., "An improved security and message capacity using AES and Huffman coding on image steganography," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control*), vol. 17(5): 2400-2409, October 2019.

[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, pp. 1-6, 2016.
[10] Huang, J., Tsai, Po, and Liao, I, "Implementing Publish/Subscribe Pattern For Coap In Fog Computing Environment," *2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, pp. 198-203, 2017.
[11] Venkatesh, H., Perur, S. D. and Jagadish, M. C., "An approach to make way for intelligent ambulance using IoT," In *International Journal of Electrical and Electronics Research*, vol. 3, no. 1, pp. 218-223, March 2015.
[12] Mittal, Y., Toshniwal, P., Sharma, S., Singhal, D., Gupta, R. and Mittal, V. K., "A voice-controlled multi-functional smart home automation system," *2015 Annual IEEE India Conference (INDICON)*, New Delhi, pp. 1-6, 2015.
[13] Misbahuddin, S., Zubairi, J. A., Saggaf, A., Basuni, J., Sulaiman, A. and Al-Sofi, "A.: IoT based dynamic road traffic management for smart cities," *2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET)*, Islamabad, pp. 1-5, 2015.
[14] Ahsan, M., Haider, J., McManis, J. and Hashmi, M. S. J, "Developing intelligent software interface for wireless monitoring of vehicle speed and management of associated data," in IET Wireless Sensor Systems, vol. 6, no. 3, pp. 90-99, June 2016.
[15] Dhall, R. and Solanki, V., "An IoT Based Predictive Connected Car Maintenance," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 4, no. 3, pp. 16-22, March 2017.
[16] Anwar, T., Kumar, A., and Paul, S., "DNA Cryptography Based on Symmetric Key Exchange," *International Journal of Engineering and Technology (IJET)*, vol. 7, no. 3, pp. 938-950, July 2015.
[17] Begum, M., Ferdush, J., and Moazzam, G. M., "A Hybrid Cryptosystem using DNA, OTP and RSA," *International Journal of Computer Applications*, vol. 172, no. 8, pp. 30-33, August 2017.
[18] 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, pp. 118-123, 2018.
[19] Ibrahim, A. K. M., Rashid, R. A., Hamid, A. H. F. A., Sarijari, M. A. and Baharudin, M. A., "Lightweight IoT middleware for rapid application development," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 17, no. 3, pp.1385-1392, June 2019.
[20] Ngu, A. H., Gutierrez, M., Metsis, V., Nepal, S. and Sheng, Q.Z., " IoT middleware: A survey on issues and enabling technologies," in *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 1-20, February 2017.
[21] Mayub, A., Shidiq, M. R., Oktiawati, U. Y. and Rosyid, N. R., "Implementation smart home using Internet of Things (IoT)," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 17, no. 6, pp. 3126-3136, December 2019.
[22] Krishna, P. G., Ravi, K. S., Kumar, V. S. and Kumar, M. S., "Implementation of MQTT protocol on Low Resourced Embedded Network," *International Journal of Pure and Applied Mathematics (IJPAM)*, vol.116, no. 6, pp.161-166, 2017.
[23] Iglesias-Urkia, M., Orive, A. and Urbieta, A., "Analysis of CoAP implementations for industrial Internet of Things: A survey," *Procedia Computer Science*, vol. 109, pp. 188-195, 2017.
[24] Kaur, J., & Kaler, N., "Design and Implementation of an OTP Based Data Security Model Incoperating AES and Sha2 in Cloud Environment," *International Journal of Computers and Technology*, vol. 17, no. 1, pp. 7081-7091, January 2018.
[25] 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, no. 4, pp.334-343, January 2018.
[26] Vadaviya, D. O., and Prof. Tandel, P. H., "Secure Encryption Techniques Using DNA Computation," *International Journal of Modern Trends in Engineering and Research*, vol. 2, no. 7, pp. 2349-9745, July 2015
[27] Zhang, X.; Zhou, Z.; and Niu, Y., "An Image Encryption Method Based on the Feistel Network and Dynamic DNA encoding," *IEEE Photonics Journal*, vol. 10, no. 4, pp. 1-14, August 2018.
[28] 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, no. 3, pp. 225-232, 2018.