International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Smart Devices Security with Armstrong Number Encryption Standard Algorithm using MQTT Protocol-An Iot Application

P. Sushma

Submitted: 18/10/2023 **Revised**: 16/12/2023 **Accepted**: 24/12/2023

Abstract: In the ERA of Digital world where internet of things tookthe lead seat, smart devices play a major role. Smart devices use many protocols on the network for communication like MQTT, CoAP, AMQP, XMPP etc. One of the protocols that is majorly used in the smart devices in MQTT. MQTT is a lightweight, publish and subscribe protocol. These Smart devices using MQTT protocol can be controlled from a remote place by using smart phones or a computer. With this way of communications between the devices there is a need for a strong, yet simple method of protecting the data being communicated over the public networks. MQTT does not use any encryption algorithm to keep the communications simple and light weight. This contributed for the enlarged scope of the research and development activities in the security issues of MQTT messages. This paper focuses on providing a simple and a strong encryption algorithm, Armstrong number encryption standard for the IoT devices communicating using MQTT protocol by retaining the simplicity of the MQTT protocol.

Keywords*: Encryption, Armstrong Number encryption standard, security, confidentiality, IoT security.*

1. Introduction

Internet of Things is one of the emerging technologies that have brought about revolutionary changes universally. Internet of things is the networks of physical objects called things. These things are implanted with sensors, actuators, software, network connectivity and other technologies for collecting and exchanging data amount themselves or for cloud storage. These things are also called as smart devices as they are automated to work on their own. These smart devices also can be controlled from a remote device like a laptop, mobile phone, etc. The statistical analysis on IoT show a huge growth of IoT devices in different sectors like Smart Homes, smart cities, smart environment, smart irrigation, smart transportation, healthcare, manufacturing etc. Figure. 1 shows the statistics of increase in IoT devices in different sectors. It is expected to reach 31.5 billions IoT devices across the global by 2025.

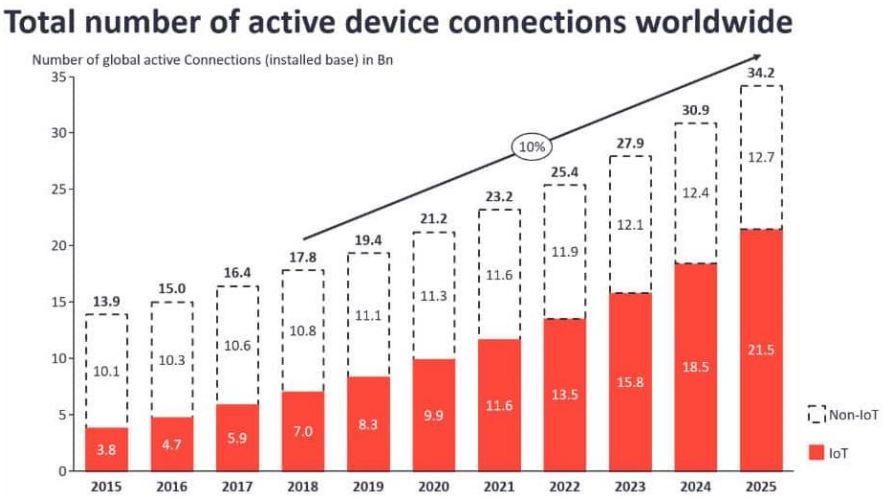

Fig 1 IoT analytics statistics from 2015 to 2025

Source :IoT Analytics Research 2018

Department of Computer Science and Engineering (Cyber Security), Vignana Bharathi Institute of Technology, Aushapur, Ghatkesar.
polasi.sushma@gmail.com

IoT devices are generally constrained devices that work on limited battery power, small bandwidth and high latency. So the security algorithms cannot be having huge computations process. But the smart devices require sufficient security measures for the

communications. Various protocols like COAP, XMPP, AMQP, MQTT etc are used by Smart devices for communications. Different protocols propose varied solutions for the security of the data communicated between these devices. MQTT (Message queuing and telemetry transport) protocol is one of the prominently used protocols in IoT for communications. It is an Oasis Standard messaging protocol for IoT devices. Smart devices uses MQTT publish and subscribe protocol which is light weight for the communications. It specifically is good for the constrained devices. Unlike traditional client /server communications, MQTT architecture involves Publishers, subscribers and MQTT brokers.

MQTT protocol works on following ports for the communications:

S.No.	Port number	Encrypted or not
1.	1883	Unencrypted
2.	8883	Encrypted
3.	8884	Encrypted client certificate required
4.	8080	Websocket, unencrypted
5.	8081	Websocket, encrypted

Table 1: MQTT ports for communications

2. Literature Review

In the revolutionary era of Internet of things there is a need for security communications between the things. Ahmed et al. (2022), has performed a survey on the existing encryption algorithms and revealed the performance of the algorithm based on different security mechanisms. Loopholes of each algorithms were listed, the attacks which they cannot address were mentioned. Among the existing algorithm based on the criteria of security mechanism the compatibility of the algorithms is mentioned.

Zahraa et al., (2020), also discuss about the performance of different encryptions algorithms. Both symmetric and asymmetric algorithms are considered and a survey is performed on those algorithm to present different factors like the efficiency, flexibility and security of the algorithms.

Bhanot et al., (2015) has done research on ten different encryption algorithms to analyse the efficiency of algorithms. The encryption algorithms on which the team have performed the analysis are: Symmetric algorithms: Data encryption standard, triple Data encryption standard, Advanced encryption standard, Rivest Cipher5, BLOWFISH, TWOFISH, THREEFISH and International data encryption standard.Asymmetric algorithms: Elliptic curve cryptography and RSA algorithms.

Boppana et. al., discussed about the security threats of MQTT protocol in the industrial IoT. Authors focused on the threat model in the unencrypted MQTT protocol which can cause major losses in the field of industries, agriculture and any remote sensing areas where human intervention in minimum with IoT devices. Attacker could easily gain the access to the IoT devices which can causes launching of man in middle attack and cross site scripting attacks. Authors proposed the solution which can avoid the above mentioned attacks.

Bastos et al., also discussed about the usage of IoT devices which are drastically increasing because of the availability of low price little to zero secure IoT devices in the market. Every home is equipped with smart devices which are doors for attackers to intrude and take the control of the devices. This is in fact a great threat for the devices which are originating DDoS attack that are in return affecting the million of devices from obtaining the access to the internet services. Authors, emphasises on improved security measures for the safe and secure communications across the IoT devices, specifically in home and city environment. A solution was proposed which could predict future attacks on data protocols and their connectivity.

Hue et. al., presented concepts related to privacy enhancement for the secure communication for IoT devices. And addressed issues related to resistant to statistical analysis attacks and dynamic support for new client participation.

Mathews et al., have discussed about the Encryption in MQTT with respect to protocol recommendation. MQTT proposes a secure means of communication using Transport layer security/ secure socket layer. Author even mentioned that TLS/SSL is computation intensive and proposed a simple lightweight message encryption approach.

Munshi et al., focussed on the security issues of the smart homes using simple techniques of smart grid secure transmissions flags. Authors surveyed the different types of threats, technical barriers, challenges and difficulties that smart home can face and came up

with a solution of improving the security of smart homes by using MQTT secure transmission flags.

Stusek et al., have done a survey and comparative studies on different types of IoT protocols, their data usage, over heads etc. Authors discussed majorly about the IoT protocol usage in massive IoT networks, Cellular networks, Narowband IoT etc.

3. Research Gap

MQTT provides security to the communications of IoT devices in three layers. In network layer, user can use VPNs for the communications. In Transport layer, smart devices can communicate using TLS/SSL. And finally in Application layer, MQTT can use the method of encrypting payload their by forgoing the security measures offered in Network and transport layer.

MQTT uses two ports for communications in application layer. Port 1883 and port 8883 as mentioned in the above table. This paper focuses on port 1883 which is unencrypted. 8883 port makes use of TLS/SSL for providing security to the MQTT payloads. This causes the packet size to be increased. This paper focuses on securing the data that is communicated over the MQTT port 1883. A simple encryption algorithm is proposed to secure the communications between constrained IoT devices over the public network using Armstrong number encryption standard.

4. Methodology

With the advent of Internet of things in the recent years many protocols have surfaced and are in use. Few of the frequently used IoT protocols are CoAP, AMQP, DDS MQTT. Arya Yudidharma et al.,(2022) have done a systematic literature review and found out that MQTT protocol performance is better than other protocols in terms of constrained devices. MQTT protocol is used in IoT devices for message transfer. MQTT protocol maintains a small packet size for faster transmission of data between publisher and subscriber. In this process MQTT ignore the security of the packets transferred. Rajaram et al., used Advanced Encryption Standard with 128 bits key and encrypted the packets to secure the data transfers. In this paper the focus is on encrypting the data using Armstrong number encryption standard algorithm.

Armstrong Number Encryption Standard is a process used to encrypt and decrypt plaintext inputs which is in the form of binary data by creating a cryptographic chain wherein each cipher text block is dependent on the last. Armstrong Number Encryption Standard (ANES) is a cryptographic method used for turning plaintext into cipher text and back again. ANES uses Armstrong number as a secret key and also uses a random number as an Initialization Vector to enhance the security of data. The chaining feature of ANES can identify the change of even a single bit in transit. Destination system can identify that the data is compromised and ask for retransmission of data. Same block of data though repeated, will not be same for next time because of IV initialization vector usage.

ANES basically uses simple operations like

- Circular left shift
- Circular right shift and
- XOR operations.

These simple computations makes the algorithm a light weight algorithm. Essentially, in ANES, each plaint text block is XORed (numerically combined) with the previous cipher text block and then encrypted. An XOR is a coding mechanism used to combine different inputs. It is used in this case to facilitate the combination of plaintext blocks and encryption keys. The process repeats itself until all plaintext blocks have been successfully turned into ciphertext blocks.

ANES uses arbitrary size plain text. Based on the block size and the number of blocks too, the algorithm works. For each session this value may change, keeping the sessions unpredictable and secure from the hacker.

The data published from source to destination remains encrypted by using Armstrong number encryption standard

5. Mathematical Approach

Encryption process

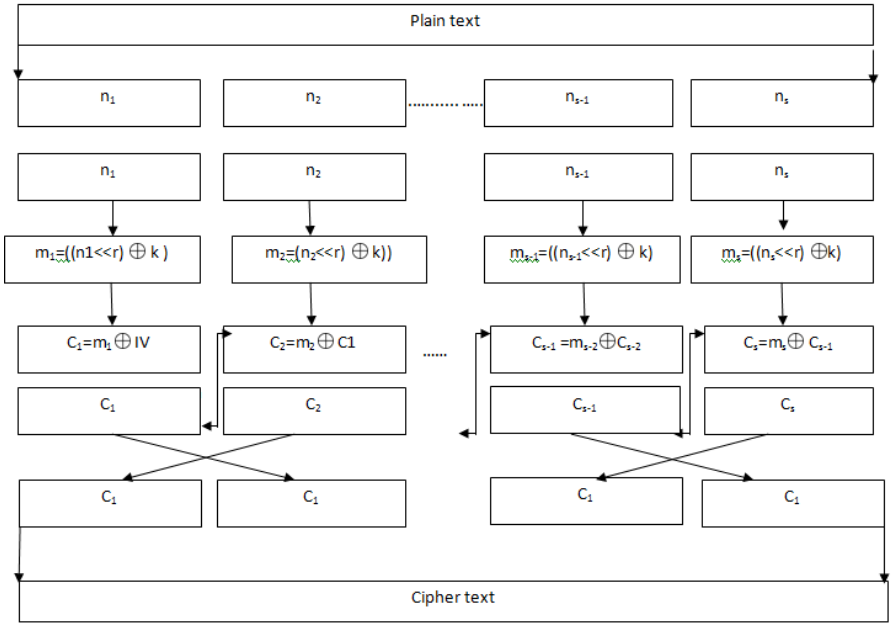

Fig.2 ANES encryption

Plain text is converted to binary stream of data as depicted in Fig.2

Step 1: The binary stream of data is divided into 's' consecutive 'b' bit blocks.

Say n1, n2, n3....ns-1, ns

Last block is parsed with 0 bits to form 'b' size bit block.

Step 2: value 'r' is calculated as number of bits in each block / total number of blocks

Then the first block n1 is circular left shifted by r times and then XORed with Armstrong number 'K' and let the result be 'm1'

Step 3: m1 is XORed with a random number 'IV' which is also called as initialization vector to generate the first block of cipher. Let it be C1. Initialization vector can change for every encryption on the text.

Step 4: Transformation operation is performed where first and second blocks are interchanged. Similarly, third and fourth blocks. Finally last and last before blocks are interchanged to form the final cipher text, 'C'. If we don't have even number of blocks then last block is forwards as it is to form the final block of cipher text.

Step 5: This C is transferred over the network to the destination node.

Decryption process

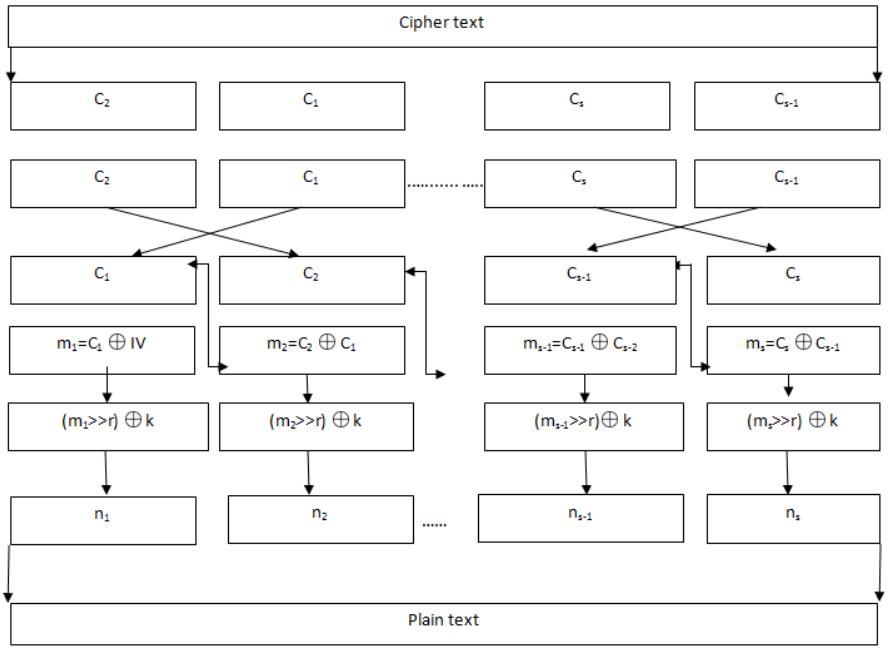

Fig.3 ANES Decryption

Decryption is a process of converting cipher text to plain text.

Fig. 3 depicts the steps involved in the ANES decryption.

Step 1: Cipher text "C" is divided into 's' cipher blocks of size 'b'.

Say C1, C2, C3, C4...Cs-1, Cs.

Step 2: Reverse transformation is performed on these blocks, so that the cipher blocks sets in order.

First block is interchanged with the second block Third with fourth and finally 's-1' block with 's' block.

Step 3: First block C1 is XORedwith random number IV which is also called as initialization vector to obtain m1 block. For the next block of cipher previous block will serve as the input in the place of initialization vector. In this ways the blocks are chained.

C1-> C2, C2->C3...Cs-1 to Cs

Step 4: This 'm1' block is XORed with Armstrong number 'K' and then right shifted.

This 'n1' will be the input plain text first block.

Step 5: above steps are repeated for the remaining blocks as well to obtain the plain text blocks

N1, n2, n3, n4....ns.

Armstrong number encryption standard algorithm is implemented using python script experimentally and checked over huge datasets with varying payload length. The time taken to encrypt and decrypt the payload is displayed in the bellow table 2. It presents detailed information of the time taken for encryption and decryption process separately using Armstrong number encryption standard algorithm. It even showcases the overall time taken for both encryption and decryption process together.

Graphical interpretation of the Encryption and decryption process is also presented in Fig. 4 and Fig. 5.

Fig.6 gives the graphical comparative study of encryption and decryption process using Armstrong number encryption standard algorithm.

DataSet	Length	Encryption Time (In MS)	Decryption Time (In MS)	Overall Time (In MS)	Average Time (100 Length) (IN MS)
1	~5000	34	33	67	0.67
2	~8000	78	60.77	138.77	1.39
3	~10000	89.76	65	154.76	2
4	~30000	463.01	472.55	935.56	9
5	~50000	1375.45	1301.47	2676.92	27
6	~70000	2423.89	2596.74	5020.63	50
7	~90000	3714.19	3533.27	7247.46	72

Table 2: Data analytics of encryption and decryption with different sizes of payload in MS using ANES

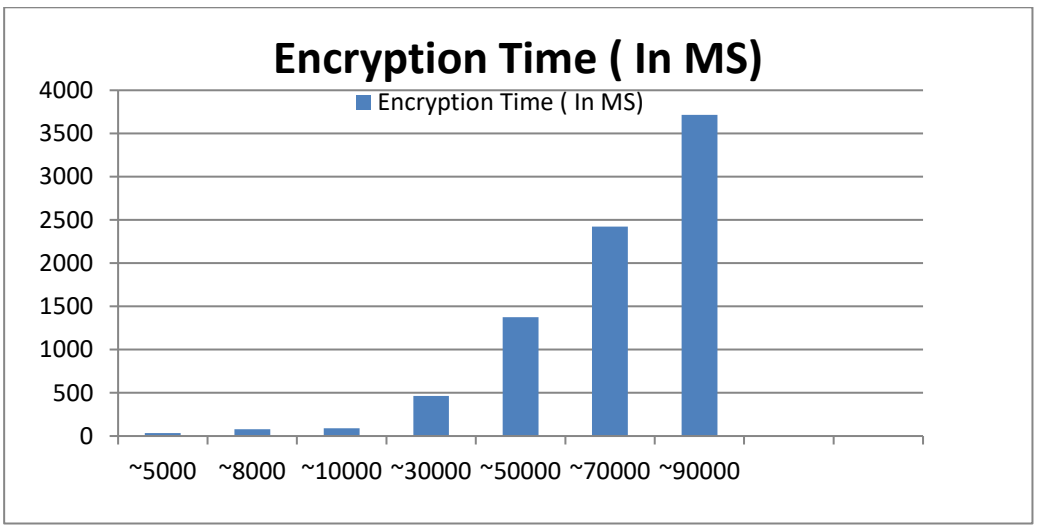

Fig 4. Time taken for Encryption process with different sizes of payloads

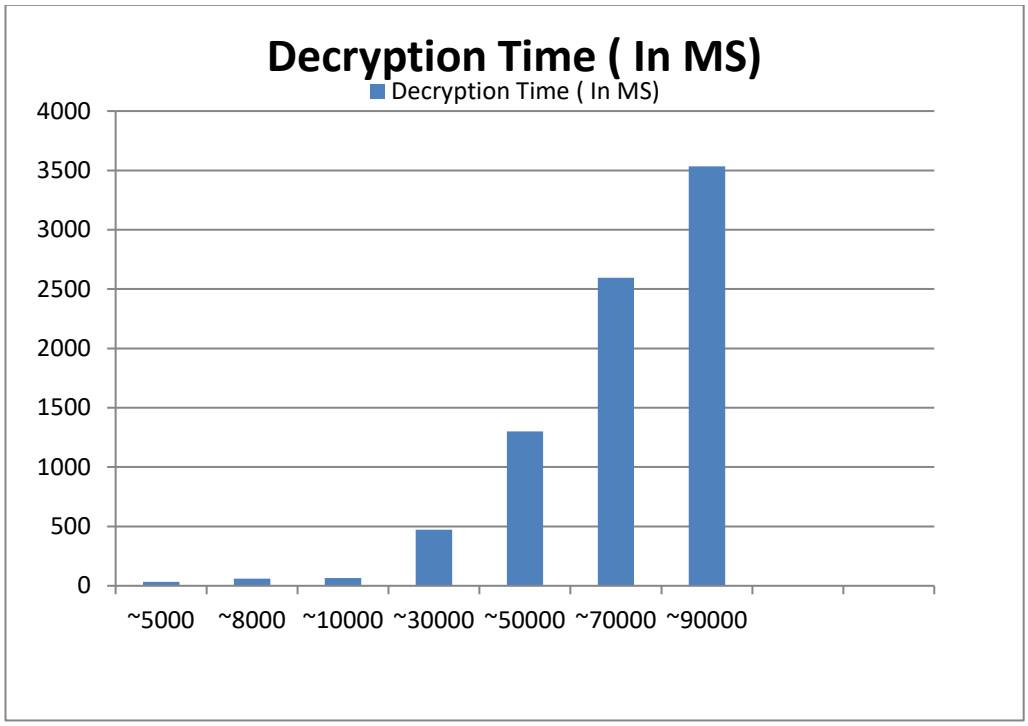

Fig 4. Time taken for decryption process with different sizes of payloads

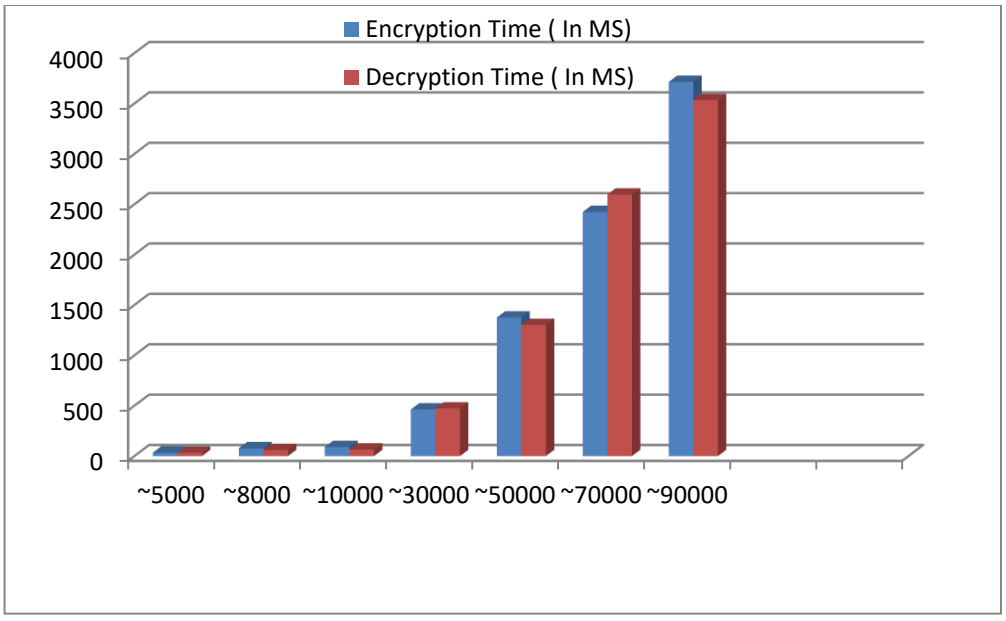

Fig 6. Comparative study of time taken for encryption and decryption process for different sizes of payload

6. Conclusion

Armstrong number encryption standard serve the purpose of maintaining the confidentiality of data in MQTT over the port 1883 by retaining the simplicity of the protocol. ANES works efficiently on the smart devices as the operations that this algorithm uses are restricted to basic XOR and circular shift algorithms. This is a assert when considering the constrained devices, where memory and battery usage takes the priority. From the experimental analysis of both encryption and decryption process we can infer that decryption is faster than encryption process. The future scope of this algorithm is to simulate the same over microcontroller and check for the strength of the algorithm by performing different types of attacks over the network transit.

References

[1] Ahmed, Attique& Naeem, Muhammad &Uk, Ijeacs. (2022). Analysis of Most Common Encryption Algorithms. 04. 08-13. 10.24032/IJEACS/0402/003.

[2] Zahraa Ch. Oleiwi *et al* 2020 *J. Phys.: Conf. Ser.* **1664** 012051Overview and Performance Analysis of Encryption

AlgorithmsDOI 10.1088/1742-6596/1664/1/012051

[3] [3]Sćepanović, I., &Sćepanović, V. (2022). Does Smart Home Have Wide Open Doors? Mqtt Communication Protocol Standardization - Potential Missing Ring Of The Iot Networks Security Chain. Social Informatics Journal, 1(1), 23–29. https://doi.org/10.58898/sij.v1i1.23-29

[4] F. Hmissi and S. Ouni, "TD-MQTT: Transparent Distributed MQTT Brokers for Horizontal IoT Applications," 2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2022, pp. 479-486, doi: 10.1109/SETIT54465.2022.9875881.

[5] T. K. Boppana and P. Bagade, "Security risks in MQTT-based Industrial IoT Applications," 2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS), 2022, pp. 1-5, doi: 10.1109/COINS54846.2022.9854993

[6] Bhanot, Rajdeep, and Rahul Hans. "A review and comparative analysis of various encryption algorithms." International Journal of Security and Its Applications 9.4 (2015): 289-306[6]

[7] D. Bastos ; M. Shackleton ; F. El-Moussa "Living in the Internet of Things: Cybersecurity of the IoT " - 2018, 2018 page (7 pp).

[8] Hue, A.; Sharma, G.; Dricot, J.-M. Privacy-Enhanced MQTT Protocol for Massive IoT. Electronics 2022, *11*, 70. https://doi.org/10.3390/electronics11010070

[9] S. P. Mathews and R. R. Gondkar, "Protocol Recommendation for Message Encryption in MQTT," 2019 International Conference on Data Science and Communication (IconDSC), Bangalore, India, 2019, pp. 1-5, doi: 10.1109/IconDSC.2019.8817043.

[10] Munshi, A. Improved MQTT Secure Transmission Flags in Smart Homes. *Sensors* **2022**, *22*, 2174. https://doi.org/10.3390/s22062174

[11] M. Stusek, K. Zeman, P. Masek, J. Sedova and J. Hosek, "IoT Protocols for Low-power Massive IoT: A Communication Perspective," *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Dublin, Ireland, 2019, pp. 1-7, doi: 10.1109/ICUMT48472.2019.8970868.

[12] P.Sushma, V V Hara Gopal, "Armstrong Number Encryption Standard for Smart devices - An IoT based Encryption Algorithm" 2022 Vol-12, Issue-12, No. 03, December 2022, 2347- 7180.

[13] P. M R and B. Bhowmik, "IoT Evolution and Recent Advancements," *2023* 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 1725-1730, doi: 10.1109/ICACCS57279.2023.10112761.

[14] P.Sushma, V V Hara Gopal, "SECURE SMART HOMES USING MQTT PROTOCOL –AN IOT APPLICATION" , National Conference Proceeding published by International Journal of Advance Research in Science and Engineering Volume No 6, Issue 1, September 2017 Pg No: 170-174 ISSN : 2319 – 8354

[15] J. A. Cujilema Paguay, G. A. Hidalgo Brito, D. L. Hernandez Rojas, and J. J. Cartuche Calva, "Secure home automation system based on ESP-NOW mesh network, MQTT and Home Assistant platform", *IEEE LAT AM T*, vol. 21, no. 7, pp. 829–838, Jul. 2023.

[16] E. Shahri, P. Pedreiras, and L. Almeida, "Extending MQTT with Real-Time Communication Services Based on SDN," *Sensors*, vol. 22, no. 9, p. 3162, Apr. 2022, doi: 10.3390/s22093162

[17] M. Singh, M. A. Rajan, V. L. Shivraj and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015, pp. 746-751, doi: 10.1109/CSNT.2015.16.

[18] Arya Yudidharma, Nicholas Nathaniel, Tang Nyquel Gimli, Said Achmad, Aditya Kurniawan, "A systematic literature review: Messaging protocols and electronic platforms used in the internet of things for the purpose of building smart homes", Procedia Computer Science, Volume 216, 2023, Pages 194-203, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.127.

[19] B.K.S.Rajaram, Krishna Prakash N, "Secure MQTT using AES for Smart Homes in IoT Network" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-5S March, 2019