

# Encryption/Decryption Scheme for IoT Communication to the Avoidance of Man-in-the-Middle Attack

Prashant Singh<sup>1</sup> Sakar Gupta<sup>2</sup>

<sup>1,2</sup>Poornima College of Engineering, Jaipur, Rajasthan, India

**Abstract**— This paper proposed a secure technique for data encryption and decryption for In-ternet of Thing (IoT) communication. The main aim of this research is to sort out the issue of Man-in-the-Middle attack. Currently, it becomes difficult to secure data from attacker as they can easily uncover the encryption key. Therefore, an algorithm is suggested here for random key generation for data encryption and decryption. In this algorithm, principle of spiral wheel is used for rearranging the character sequences to produce ciphers. It changes the sequence of characters in a particular sequence. It is based on the concept of centroid of the sequence to ob-tain the median of the pattern based on even and odd numbers. This method comes into Symmetric key algorithms. It produces a highly reliable and secured communication interface for IoT to prevent from the attacks.  
**Keywords:** Internet of Things, Man-in-the-Middle Attack, Ciphers

## I. INTRODUCTION

Nowadays, people day-to-day activities depend on Internet of Things i.e. IoT. It uses the constrained devices for actuating and sensing the operations. In 1999, Kevin Ashton coined the term and concept of IoT. It offers the concept to interconnect the internet with daily life common objects. Such gadgets assembled globally to gather numerous information with the performing of definite tasks with minimal or no hu-man intervention. Currently, global cyber market mostly controlled by IoT and its principles. With a survey record by Gartner, in the end of 2020, 21 billion intercon-nected devices will mark their presence [1]. A giant network will demonstrate their limitless applications in the world of internet. Some of the applications can be de-ployed as to develop smart logistics, smart grids and to create smart cities etc. How-ever, every innovations come with tremendous challenges. For example, constrained devices featured in IoT have their limitations as throughput, short lifetime, limited computational capacity etc. Such aspects generate new challenges for researchers, communication experts and computer/cyber experts [2]. It becomes must to provide an efficient and sustainable environment for making the effective communication between these constrained devices. Therefore, it becomes a challenge to provide effi-cient network due to the requirement of different standards and protocols used by different devices. Therefore, there is a need to develop a heterogeneous network that has the potential to make communication with each devices in secured as well as efficient way.

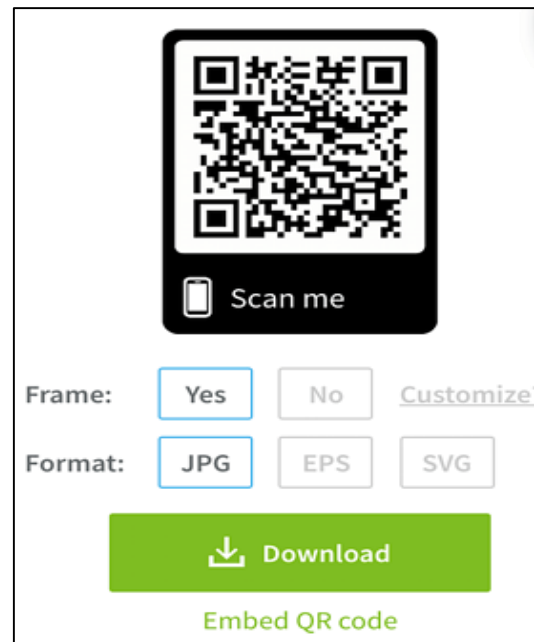


Fig. 1: Onboarding solution based on QR code [3].

For IoT environment, security plays one of the major role. Past years witness the exponential growth in number of cybercrimes and cyber-attacks [3]. Constraint de-vices contain low or no security feature that make them the main target for cyber attackers. Recent years reported numerous cases in which attackers got control over such constrained devices and result as the mounting of DDoS attacks using bots. IoT does not support the security and network protocols used in traditional internet due to the low throughput of network and constrained nature of the devices. There is always the need for new protocols in IoT for security and communication purposes due to low power consumption, less throughput and low computational complexity etc. IoT environment demands lightweight security protocols to run its applications [4-5]. It should include the strong authentication protocols for secured devices and networks. An entity's identity verifies by authentication process. For best authentication proto-col, the process should include double different credential of user for secured practic-es. IoT entities cannot afford the inclusion of cartographic primitives that makes the authentication process more challenging. In traditional market, they have high com-putational complexity. However, utilization of gateways as middle-ware for compu-tation increases the threshold of computational complexity. In such scheme, IoT devices are slightly less powerful than the gateway nodes [6]. In last few years, several schemes on authentication for network and constrained devices have been pro-posed and some of them are explained in upcoming sections.

## II. BACKGROUND

Traditional ways include access control mechanism for inter-organizational data sharing in current systems [6]. Data hold

by a trusted server performed the access control. It includes managing a set of user's information by the server with their rights to access and deliver the information in between authorized users. According to a policy, one key in cryptographic system can decrypt multiple ciphertexts. It works on the concept of Attributed-Based Encryption (ABE) [7]. Later, there is a refinement of ABE in two certain directions. These are as Key-Policy ABE and Cypher text-Policy ABE. In first one [5], attributes are set for each ciphertexts. Here, with an integrated policy, the decryption keys are generated to decide the decryption order of the documents. In another one, [2] mimics a role-based access control. In such scheme, system provides the keys to users based on the encrypted ciphertexts and their roles with a specific access policy. In recent studies, the overhead concept is considerable for the restriction of devices. On the other hand, key management prefers the concept of attribute-based encryption [1]. Symmetric algorithms are preferred for huge amount of data encryption in sensors directly due to performance reasons. Dynamic restrictions not occurred in the concept of attribute-based encryption, as they require the access during the operation time.

Broadcast authentication protocol TESLA follows the Hash-chains as a tool [7]. This concept utilizes the elements with hash-chains assigned to definite time-slots. To strengthen the stream ciphers, Rivest [8] used a pattern of backward and forward hash chains. Another system named as BAC systems contains four distinct energy efficiency classes [3]. It has more control capabilities with more fine-grained sensors arranged in a higher efficiency class. Currently, an organization having large building area and complexes can easily comprise tens of thousands of sensors. It generates a good amount of data stream providing the insight the building actions. It leads to the need for more protection from the attackers, specifically during the outsourcing handling of the data. One of the major research project named as BaaS in the EU FP-7 [4] targets to increase building energy efficiency. It can be performed through assessing and analyzing the data of operational building that advances the regulation schemes accordingly. It provides an IoT platform for the interconnection of multiple buildings through data repository, BMS and internet services for batch analysis and real time application.

### III. CLASSIFICATION OF ATTACKS IN IOT

IoT needs to address the security in the designed system i.e. the most important concerns. Efficient data communication demands high-level security from random cyber-attacks [9]. Attacks such as Sybil, eavesdropping, message modification, traffic analysis and Denial of Service (DoS) etc. are harming the people and institutions by obtaining their access information as well as gain financial benefits [10]. The exponential growth of IoT attracts the cyber-attackers with more number and in complex manner. It becomes sophisticated to breach the security with new tools [11-12].

Most of the user data are spread in the large area and distributed in nature as they are attended by them. Therefore, it becomes easier to attain physical access of the devices by the attackers. Apart from such access, another aim for intruder is to hit on data communication process as all the

processes happened in open environment as wire-less communication. IoT features sensors as its key element. They have limited energy capabilities and processing. Therefore, complex security schemes failed to provide protection from vulnerable attacks. Security vulnerability occurred due to the gaps and loopholes present in authentication. It offers unauthorized access to devices. It results disturbing and harming the systems through random attacks that includes a definite goal performed by criminals, hackers or even government agencies. Classification of attacks have been made in two ways depending on the type of attackers. First is inexperienced attackers or unstructured attacks with their hacking tools. Second is structured attacks through experienced people with the known of vulnerability of attack and performed by writing script/codes by using sophisticated tools. Figure 2 illustrates the different ways to perform the attacks.

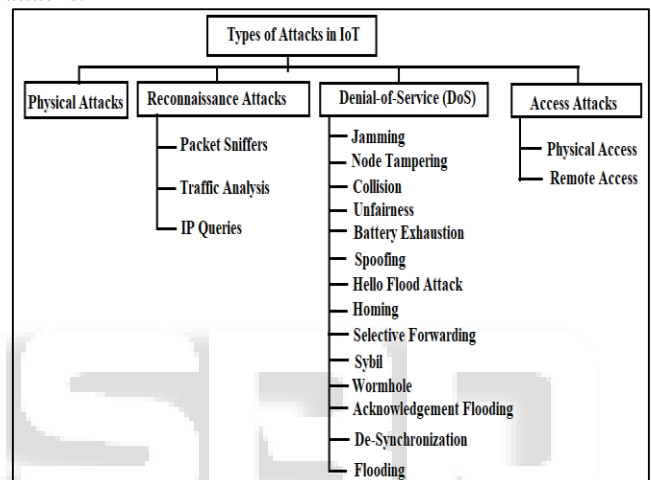


Fig. 2: Classification of type of attacks in IoT [13].

#### A. Physical Attacks

It include the attack that physically temper the device due to the data distribution in the open environment with unattended information. It offers the opportunity to attackers to disturb the communication [7-8].

#### B. Reconnaissance Attacks

It involves the use of packet sniffer tools or traffic analysis for data extraction by the attackers. They also tries to find out the IP address of targeted device.

#### C. Denial of Services (DoS)

It consists the unavailability of resources and system by attacker leads to blocking the access of information. It is due to the limited capabilities of sensor that makes to exhaust the device and cut the connection to system. These type of attacks placed on the layer of TCP models such as transport layer, network layer, physical layer, datalink layer and application layer. All have the same intention as to block the transfer of information. It is sub-divided into different techniques that can be discussed as follow [14-15].

##### 1) Jamming:

Attackers block the communication channel between the two layers in order to prevent data communication by controlling the signals.

2) *Node Tempering:*

Attackers physically disturb and temper the node in order to attain the control like hijacking it and access the information.

3) *Collision:*

It is performed by adding a duplicate or fake node in the network to capture it and then to produce unnecessary traffic. It creates collisions between the data result as dropping the valid packet containing information.

4) *Unfairness & Battery Exhaustion:*

It is the node de out situation through repeat-ed collisions attacks result in the Battery exhaustion. It occurs mostly in conditions like limited battery power such as Wireless Sensor Network (WSN) as nodes have very limited battery power [16].

5) *Spoofing:*

It misleads the data communication by the use of evil node for changing the direction.

6) *Hello Flood Attacks:*

In this, user received hello packer b attackers for making them to use compromise node. This will forward the packets to its neighbor. They assume that it belongs to them leads to create congestion because of the generation of to the network.

7) *Homing:*

In this black hole is created by finding the node near to the sink or the cluster node. They try to disable the node for black hole generation.

8) *Selective forwarding:*

In this data is forwarded by malicious node through selective nodes rather than all nodes. It results as packet drop due to the congestion on a node.

9) *Sybil:*

This attack consists multiple identities of the node in the network to tem-per the flow of traffic. It makes them isolate from the main system to disturb the communication and utilize them for malicious purpose.

10) *Wormhole:*

This attack malicious record the data of packets with the delivery of them at different locations. It is a critical attack in which the transmission of data is done selectively. It follows a defined route for data at the implementation of launch of the network. Malicious nodes are present in the shortest route.

11) *Acknowledgment Flooding:*

In this attack, the nodes provide the false information to get the acknowledgment from the malicious node and create spoofing at the neighboring node.

12) *Flooding:*

It is performed by high traffic congestion through the generation of unnecessary messages.

13) *De-synchronization:*

It consists fake information produced at both ends of communications. It makes to retransmit the data many times in order to correct the error but results as energy exhaustion at one or both ends.

D. *Access Attacks*

In this, attackers obtain the remote or physical access of the system devices using IP addressing. Later, they temper and use the devices for malicious purposes.

IV. PROPOSED ALGORITHM

This paper presents a novel algorithm of encryption/ decryption process to avoid at-tack from IoT system. It give a process to generate signature for the device which is only one time applicable to prevent from Man-in-the-Middle (MiM) attack. Proposed algorithm is named as Quondam Signature Algorithm (QSA). Algorithm for the pro-cess is explained as format setting and signature generation.

A. *Algorithm for format setting*

- 1) Step 1: Start
- 2) Step 2: Client Connection Request = CR  
Time Stamp = TS  
Client Identity = CI
- 3) Step 3: The process is divided into two parts as,
  - 1) CI = MAC ADD  
= 8 Digit HEXADECIMAL  
= 8×4
  - 2) TS = Set current system's date & time in definite format as MM DD YYYY hh mm  
= 12 Digit CHARACTER

B. *Algorithm for Signature Generation*

- 1) Step 1: Get system date & time in specific format as (D[ ]) and (T [ ])
- 2) Step 2: Append system as date & time to form the time stamp vector TS[ ],  
TS[ ] = D[ ] + T[ ]
- 3) Step 3: Multiply time stamp vector TS[ ] with substitution matrix S[ ].
- 4) Step 4: Pre-installed at C & S to authentic users.
- 5) Step 5: Achieve Quondam matrix QM [ ].

$$\begin{matrix}
 S[ ]_{12 \times 12} \\
 \begin{matrix}
 S_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & S_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & S_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & S_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & S_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & S_6 & 0 & 0 & 0 & 0 & 0 & 0 \\
 = & 0 & 0 & 0 & 0 & 0 & S_7 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & S_8 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & S_9 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & S_{10} & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & S_{11} & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & S_{12}
 \end{matrix}
 \end{matrix}$$

Where,  $S_1, S_2, \dots, S_{12} \neq 0$ .

- 6) Step 6: Achieved the value of  $QM_{12 \times 12}$  [ ].
- 7) Step 7: Extract diagonal elements from  $QM_{12 \times 12}$  [ ] to form 12 character long QS[ ].
- 8) Step 8: Append QS[ ] with CI[ ] and send it to server of  $M_{20 \times 1}$  as,  
 $M_{20 \times 1} = [ M_1 M_2 M_3 \dots M_{20}]$
- 9) Step 9: Server receives message from client as  $M_{20 \times 1}$ .
- 10) Step 10: Encryption finish
- 11) Step 11: Server separates QS[ ] & CI[ ] as,  
 $M_{20 \times 1} = QS[ ]_{12 \times 1} + CI[ ]_{8 \times 1}$
- 12) Step 12: Forms Quondam signature as  $DM[ ]_{12 \times 12}$ .
- 13) Step 13: Obtained TS[ ] with the equation as,  
 $TS[ ] = QM[ ] \times S^{-1}$
- 14) Step 14: Decryption finish

## V. RESULT AND DISCUSSION

After implementation of the process on C# tool using load MTC and RTC, the process run successfully. It shows better results as cost in communication and communication overhead [17]. Figure 3 illustrates the achieved results in form of cost in communication (bit) for the existing systems. It depicts the exchange procedure between payload header and multiple messages during Physical Unclonable Function (PUF) authentication in terms of communication cost. Communication cost is defined as the number of bits interchanged over the network during authentication.

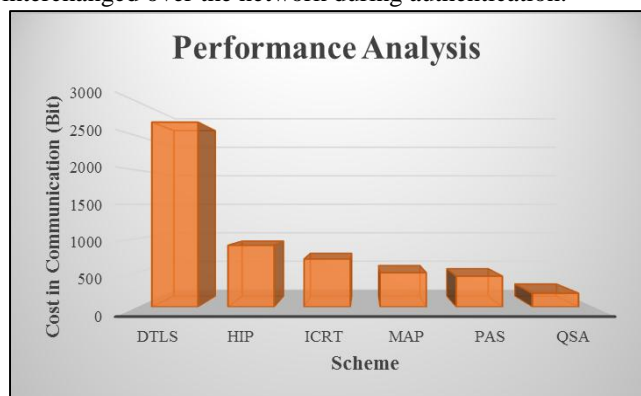


Fig. 3: Cost in communication during authentication.

## VI. CONCLUSION

In this paper, novel algorithms are proposed for data encryption and decryption to solve the issue of random attacks on IoT. This process generates one time accessible device signature as Quondam signature algorithm (QSA). It solves the issue of man-in-the-middle attack. Results shows the requirement of less cost in communication bits of proposed algorithm. It can also extendable towards the time frame for better analysis. Various schemes in terms cost in communication were being compared to prove the significance of the results. Same work can apply as the solution of other attacks resent in the IoT systems. It is a secure command for executing the protocol with the options to fill certain parameters for smart phones or other smart devices for IoT.

## REFERENCES

[1] Das, M. L.: Two-factor user authentication in wireless sensor networks, *IEEE Transactions on Wireless Communications*, 8(3), 1086-1090 (2009).  
 [2] Xue, K., Changsha, Hong, P. and Ding, R.: A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, *Journal of Network and Computer Applications*, 36(1), 316-323 (2013).  
 [3] Farash, M. S., Turkanovic, M., Kumari, S. and Holbl, M.: An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment, *Ad Hoc Networks*, 36, 152-176 (2016).  
 [4] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E.: Wireless sensor networks: a survey, *Computer networks*, 38(4), 393-422 (2002).

[5] Hwang, M. S. and Li, L. H.: A new remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, 46(1), 28-30 (2000).  
 [6] Xu, J., Zhu, W. T. and Feng, D. G.: An improved smart card based password authentication scheme with provable security, *Computer Standards & Interfaces*, 31(4), 723-728 (2009).  
 [7] Yu, S.: Big privacy: Challenges and opportunities of privacy study in the age of big data. *IEEE access* 4, 2751-2763 (2016).  
 [8] J. Song, A. Kunz, M. Schmidt, and P. Szczytowski. *Connecting and Managing M2M Devices in the Future Internet*. Springer *Journal of Mobile Networks and Applications*, 19(1), 4–17, (2014).  
 [9] Amirhossein, S.: Improving the Security of Internet of Things Using Encryption Algorithms, *International Scholarly and Scientific Research & Innovation*, 11(5), (2017). F.: Article title. *Journal* 2(5), 99–110 (2016).  
 [10] Arbia, R. S., Enrico, N., Yacine and C., Zied C.: A roadmap for security challenges in the Internet of Things, *Digital Communications and Networks* April 2017, <http://dx.doi.org/10.1016/j.dcan.2017.04.003>.  
 [11] Alajmi, N.: *Wireless Sensor Networks Attacks and Solutions*, arXiv preprint arXiv:1407.6290 (2014).  
 [12] Diaz, A. and Pablo, S.: Simulation of attacks for security in wireless sensor network, *Sensors* 16(11), (2016).  
 [13] Rashid, H. and Irfan, A.: Review of Different Encryption and Decryption Techniques Used for Security and Privacy of IoT in Different Applications, *IEEE International Conference on Smart Energy Grid Engineering*, (2018).  
 [14] Muhammad, A. I., Oladiran, G. O. & Magdy, A. B.: A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches (*Global Journal of Computer Science and Technology: E Network, Web & Security*, 16(7), (2016).  
 [15] Borgohain, T., Uday, K. and Sugata S.: Survey of security and privacy issues of Internet of Things." arXiv preprint arXiv:1501.02211 (2015).  
 [16] El, M., Otmane, M. L. and Mostafa, B.: Internet of Things Security: Layered classification of attacks and possible Countermeasures, *Electronic Journal of Information Technology* 9 (2016).  
 [17] Mughal, M. A., Luo, X., Mahmood, Z. and Ullah, A.: Physical Unclonable Function Based Authentication Scheme for Smart Devices in Internet of Things, *IEEE International Conference on Smart Internet of Things*, (2018).