# STUDY ON SECURITY ISSUES IN INTERNET OF THINGS

[1]R.NANDHINI, [2]P.SRILAKSHMI, [3]APARNA R
[1,2]Final Year Student, S.S.S. Shasun Jain College for Women
T.Nagar,Chennai-600017
[3]Asst. Professor, S.S.S. Shasun Jain College for Women
T.Nagar,Chennai-600017

**Abstract :** Internet of Things (IoT) is a group of devices and appliances connected using embedded sensors, internet which is used for exchange of data. This IoT is a fast-growing technology in today's world. With the rapid growth in IoT, there is a rapid growth of data due to which securing the data is also important. Cryptographic algorithms are used to secure these data. In this paper, we propose a study about the cryptographic algorithms used along with IoT and the related security issues during data transfer.

**Keywords:-** IoT, Security Algorithms, IoT Applications, RFID, Encryption.

## 1. Introduction

Internet of things is growing fast, day by day. Its applications are widely used in our world today. According to a survey the number of connected things will be drastically increased in the near future [1]. Various devices are connected with internet which helps in a smooth communication between them. There is a transfer of data within the connected devices. This transfer of data doesn't involve human interaction. This IoT is used by radio frequency identification [RFID] [2] which basically is a microchip. It helps in the wireless transmission. IoT's application areas include medicine, agriculture and household fields. Hence, it is important to secure the data used in IoT. IoT can compute and communicate on its own. Security brings about data integrity. Using a few encryption algorithms[3], we can secure the data and reduce the risk of data theft comparatively.

This paper is organized as follows. Section II briefly explains IOT Layers, Its Operations and Security Issues, Section III elaborates Encryption Algorithms, Section IV gives Conclusion of the work.

### 2. IOT Layers, Its Operations and Security Issues

There are three layers in the IOT Architecture. They are

- Perception Layer,
- Network Layer and
- Application Layer.

#### 1. Perception Layer

The perception layer is also called as object layer. It contains the sensors and actuators for identifying any particular operations. This layer is responsible for digitizing and transferring data to the object abstraction layer through secure channels. Object layer collects the necessary information from the physical objects and

converts that to digital signal and pass it to network layer. The collection of sensors and actuators is the object layer that forms WSN (Wireless Sensor Network).

At this level the security issue includes the physical security provided for the sensing devices and security for the collection of information. Due to simple and weak protective capability of sensing nodes the security of WSN, RFID and M2M terminal [4] are affected.

WSN:

Security is a challenging thing for WSN as it is not easy for always watching the sensor nodes but in order to prevent the transmission of data from attackers it must be secured. The WSN security requirements are availability, confidentiality, integrity and authentication and other requirements such as localization, self organization and data freshness.

In sensor node, the data flows from several intermediate stages so the leakage of the data will be more. In such situation the data confidentiality provides encrypted data so that only the receiver can decrypts it to get back the original data.

The data received by the receiver should not be modified by the intruder that is data integrity. The data authentication verifies that the data is received from the authenticated node[5].

The data availability ensures that the data is available even after the attack. While transmitting data using location details of the sinking nodes, the location must be secured otherwise the malicious nodes may control the non secured data by sending false signal strengths or replaying signals. This is source localization .One of the marvelous thing with the security in WSN is self-organizing; they don't have any particular infrastructure for the nodes to be organized and have self healing property. Data freshness make sure that only the new and fresh data is transmitted and no old data is being transmitted or replayed. The freshness can be checked by including some time related counter.

RFID:

It is an automatic technology for identification of objects and human beings. This technology mainly uses RFID tags for exchanging data without manual support. The attacks and security issues of the tags are:

Table1: Various attacks & its Consequences

| **Attacks** | **Process** | **Consequence** |
|---|---|---|
| Unauthorized tag disabling | It Incapables RFID tags temporarily or permanently | The RFID tag malfunction and misbehave under the scan of tag reader |
| Unauthorized tag cloning | Dishonest reading once identification information of the tag is compromised | Fake security and new vulnerability will be introduced |
| Unauthorized tag tracking | The dishonest reader trace the tag | Leakage of sensitive information |
| Replay | With the tag's response the dishonest reader impersonates the tag. | Faking the availability of tag. |

**2. Network Layer**

IoT faces a lot of risks and issues in network layer such as virus attack, destruction, confidentiality, integrity, man-in-the-middle attack. The most common attack is Dos attack which is caused by enormous need of nodes for data transfer. And also sending large amount of huge data causes congestion. Some of the security requirement at this network layer is Identity authentication, Anti-ddos, Encryption mechanism, communication security. Earlier by-hop encryption mechanism was adopted; using this in the transmission process the information is encrypted[6]. In case of communication security TLS/SSL or IPsec are used to encrypt the link in the transport layer and protect security of network later. Protecting sensors are used to protect the privacy of the humans and objects from the physical world.

3. Application Layer

The security required for variety of application environment are different, and one of the characteristics are data sharing[7]. The responsibility of traffic management is carried by this layer. At this level only the path-based DOS attack was initiated. Only at this level the service requested by the customer will be provided. For a large scale development of IOT application this layer was very useful. It is the top most layers that consist of formulas, business logic and UI to user end. The security requirement[8][9] in this layer is authentication and key agreement, privacy protection, security education and management. Some of the application layer protocols are CoAP which has a transport UDP and security DTLS, MQTT which has a transport TCP and security TLS/SSL, XMPP which has a transport TCP and security TLS/SSL, RESTFUL which has a transport HTTP and security[10] HTTPS, AMQP which has a transport TCP and security TLS/SSL, Web socket which has a transport TCP and security TLS/SSL, DDS which has a transport TCP/UDP and security TLS/SSL, SMQTT which has a transport TCP and has own security[11]. As technology gets updated every day, android/mobile applications [12] can be linked with IoTs with incorporated and in-built security handling techniques in the future.

## 3. Encryption Algorithms

**1. ECC (Elliptical Curve cryptography)**

ECC is a public key cryptography, in this type one key is used for encryption while the other is used for decryption. This algorithm is based on elliptic curve theory [3]. ECC comes with a 164-bit key which can achieve a level of security while the others need 1024 bit key [4] Even with low computing power and battery usage we receive the same level of security and this is commonly used for mobile applications. The main advantage of this algorithm is the small key size and storage.

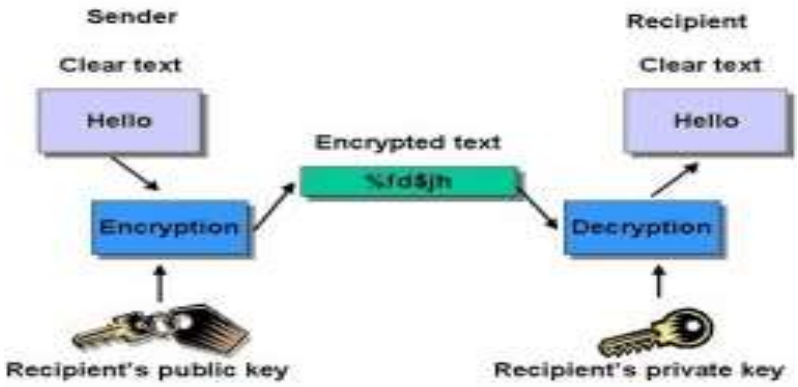
**2. mCrypton**

mCrypton algorithm is designed for tiny devices like RFID tags and sensors. This has 3 key types 64 bits, 96 bits and 128 bits. This helps us in enabling much compact implementation of hardware and software. This is commonly used as a security block for applications like smart cards, security tokens. In devices with low cost RFID tags and sensors it is not possible to execute primitive due to cost constraints.

This is designed with extreme efficiency in usage of the resource and consumption of power. This algorithm is based on the architecture of crypton[5]. This has better flexibility due to variant key sizes [6].

**3. AES ( Advanced encryption standard)**

This algorithm is used for electronic encryption of data. It uses either public or private key. It has variable key length of 128/192/256 bits [6]. Each key could encrypt or decrypt a 128 bit data. AES is proven to be a relaiable algorithm. AES ensures a high security.




## 4. Conclusion

IoT is growing day by day in a very effective manner. It is not only being used in homes but also in every place to make life simpler and easier. Now IoT is something that has the world in a hand. Another newer technology is mobile applilcations [12], it can also be collaborated with IoT for better performance. Since it is being utilized massively some issues will also take place which is nothing but the security. Security plays a vital role. Only when it is trustworthy, it will be used by everyone. In order to maintain security many algorithms can be used, which helps in building secure network of thing. The security issue may occur in any layer so at each and every stage protection are to be ensured. Many algorithms were already been proposed and some are yet to be proposed to have more reliable and secure IoT. Hence, this paper gives a clear understanding about the IoT application areas and the solution for its security related problems.

## Acknowledgment

Sincere thanks to the Department of Computer Applications, S.S.S. Shasun Jain College for consistent support in carrying the research work.

## Refercences

[1] The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved Wei Zhou, Yuqing Zhang, and Peng Liu, Member, IEEE

[2] Improving the Security of Internet of Things Using Encryption Algorithms Amirhossein Safi

[3] Research Issues on Elliptic Curve Cryptography and Its applications Dr.R.Shanmugalakshmi and M.Prabu, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009

[4] Lim, C.H.: A revised version of CRYPTON: CRYPTON v1.0. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 31–45. Springer, Heidelberg (1999)

[5] Lim C.H., Korkishko T. (2006) mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors. In: Song JS., Kwon T., Yung M. (eds) Information Security Applications. WISA 2005. Lecture Notes in Computer Science, vol 3786. Springer, Berlin, Heidelberg

[6]P.srilakshmi and R.Aparna, "Cryptography In Network Security, A Much Needed Technique". International Journal Of Advance Research In Computer Science, volume 9, special issue no 1, February 2018.

[7]Suchitra.C, Vandhana.C.P "Internet of thing and security issue" Internation jounal of computer science and mobile computing ,volume.5,issue.1

[8]Hui Suo, Jiafu Wan,Caifeng Zou, Jianqi Liu "Security in the internet of things: Review" 2012 International conference on computer science and Electronic Engineering

[9] Jitender Grover, Shikha Sharma "Security issue in Wireless Sensor Network- A Review" Department of Computer science and Engineering

[10] Makkad Asim" Security in Application Layer Protocols for IOT: A Focus on COAP" International Journal of Advanced Research in Computer Science- Volume 8, No. 5, May – June 2017

[11] Gurudatt Kulkarni, Ramesh Sutar, Sangita Mohite "RFID Security Issues & Challenges" International Conference on Electronics and Communication Systems (ICECS'14).

[12] R.Nandhini and R.Aparna, "Android and Its Background Developments". International Journal of Advance Research In Computer Science, volume 9, special issue no 1, February 2018.