Asian Journal of Convergence in Technology **Volume IV Issue III**
ISSN No.:2350-1146, I.F-5.11

Symmetric Data encryption using trusted third party Objects in IOT

Prof.Rohini S. Hanchate, Computer Engineering Department, D.Y.Patil Institute of Engineering & Technology Ambi,Pune,India,rohini.shanchate@gmail.com
Prof.Sarika Kadam, Computer Engineering Department, D.Y.Patil Institute of Engineering & Technology Pimpri,Pune,India,sarikaengg.patil3@gmail.com

***Abstract*—In modern period, the number of elegant things are organized, typically referred to as "Internet of Things" (IoT) devices, is rapidly increasing due to almost infinite applications, which are rapidly getting part of the everyday life, such as wearable technologies, smart grid, Smart Traffic Light System , smart cities, smart transport etc..**
In order to secure the communication between IoT devices and Internet servers, and guarantee to the customer's on new emerging IoT technologies, efficient cryptographic mechanism is necessary. To achieve integrity and legitimacy there must be Authenticated Encryption (AE) algorithms applied to smart devices responsible for communication.

***Index Terms*—IOT, security, encryption, decryption, mixed encryption.**

I. INTRODUCTION

Internet of things is a network of connecting various devices or things so that to share the information in order to achieve more automated things. These things can be sensors actuators, software, hardware and network connectives. IOT is growing rapidly therefore, Internet of Things desires to be built in such a way to avoid hazard to their security and privacy Internet of things is a network of connecting various devices or things so that to share the information in order to achieve more automated things and to create a smart environment. These things can be sensors actuators, software, hardware and network connectives. Though new world of smart devices will make human life easier with rapidly growing technologies, Internet of Things desires to be built to avoid hazard to their security and privacy. In the IOT, to communicate with smart things all objects associated to the comprehensive Internet which leads to new challenges in security and privacy where huge data sensed and exchanged by smart objects, to prevent unauthorized identification objects i.e., confidentiality, authenticity, and integrity In this context, the more independent and intelligent systems get, problems like the authentication and privacy of Objects emerge, and accountability of things in their acting will have to be considered. Prior to Transfer the data to objects or things, the procedure of encryption along

with secret key is applied on data to generate cipher text and later user reproduces the original data by applying decryption by using identical private key which may share 2 by different objects. The key mechanism of the IoT Security model is dependent upon confidentiality, integrity and availability. In the context of IoT, confidentiality caters for protecting privacy of IoT devices; integrity looks after the data contained within the device while availability covers accessibility of the device. This article will focus

on the aspects of maintaining integrity in data communication. Figure1 shows security assessment parameter on the aspects of maintaining data integrity [1] [2].

Figure 1 security assessment parameter

II. LITERATURE SURVEY

Encryption Algorithms: The There are various encryption algorithms are developed, An Based Encryption Based on Attribute (ABE) and demonstrable data decryption technique by Junzuo et al.[3],is designed to achieve data security in cloud based system. The major drawback of ABE are, data computing and storage overhead for verifying user data. SIT is Symmetric key block cipher[4] consist of plain text with 64- bit key, in Symmetric Algorithm to generate confusion and diffusion it consist of encryption 3 rounds , each round is based on some mathematical computations, increase in number of rounds will intensify in security which leads to power consumption, in SIT it requires the 64 bit key to encrypt 64-bit data which is given input to the key Expansion and further it converts to the 4 bit and concatenated to generate 16 bits, this 16-bit value and F-function is used to generate the 4*4 matrix the obtained Keys are transformed into four arrays of 16 bits that is referred as Key Rounds. This Key Rounds are k1,,k2,k3,k4,k5 is used to encrypt the plain text where plain text is divided into 16-bits(PT0-PT15)(PT16-PT31) etc…as bits proceed swapping operation applied to Plain Text this is to obtain the confusion in Cipher Text ,further XNOR operation applied for Round Keys which is obtained by Key Expansion and shifting ,swapping and substitution is applied to obtain Cipher Text. 3 Hybrid Encryption Algorithm[5] which offers benefits of symmetric key and Asymmetric key performance with strong security and with lower implementation complexity in this approach it consist of server ,transmission interface ,two way communication channel and client object server object is responsible for encryption and key management, communication channels are responsible for transmission of encrypted data and client is liable for decryption and sending the key, hybrid encryption algorithm[5] is combination of MD5 and ECC, AES algorithm. The comparison between various approaches are discussed below:

Table 1: comparison of encryption algorithm

Algorithm/parameters	AES	ECC	Hybrid encryption
Implementation	Software based		Software based
Speed	**High**	**High**	**Moderate**
Memory requirement	Small	Medium	Very small

1) Security issues:

a). Heterogeneity in technologies

In earlier, IoT is a technology that allows all sorts of objects to connect. By doing so, heterogeneity issue is raising even in Security matters. There is for example no uniform international encoding standard for RFID tag; this can create access problems or errors in reading process for the user [6]. Not only tags are different, but even data itself. Data can in fact come with different or even incompatible formats. This can result in data loss or destruction, causing privacy exposure. There should be a process of unification of formats and protocols in order to guarantee a better security in IoT [7].

b) Encryption

Encryption is one of the fundaments of the modern internet security. Information can in fact not be send directly (or it can be intercepted on the way and be potentially misused from malicious parties). Encryption is the part where information is coded with the help of a key into another serial of characters. Only parts with the key can retrieve the original message and read it. Unfortunately, the classical encryption algorithms and standards cannot be applied for the IoT. Many "things" do not support those algorithms that require a big memory [8]. The "things" were in fact not designed in the first term to be connected, but rather to fulfill their natural function (clothes, walls, fridges...). This does not mean that those objects do not need to be protected, in the contrary, it is necessary. One of the suggestions given to encrypt data in IoT is then Lightweight cryptography. The term "lightweight"[9] should not be mistaken with weak (in terms of cryptographic protection), but should instead be interpreted as referring to a family of cryptographic algorithms with smaller footprint, low energy consumption, and low computational power needs, which will resolve both energy and security challenges. Lightweight cryptography contains different sorts of algorithms that can be used, all of them are under studies, one can give as examples: Symmetric ciphers for lightweight crypto, asymmetric ciphers and homomorphism.

c) Trust Management

Trust is an important and necessary criteria in all transactions. Technology and IoT are not an exception, and exchanges in IoT should all come from and to trusted parts. However, heavy encrypting and complex computing are not possible in IoT. This means that the trust system should be simple, but efficient. During the authentication period, user should easily be able to login, while having a secure system in front of him. This can be difficult as it looks as a paradox. A secure system is usually complicated and difficult to use for a novice user, while a four number PIN code is rather easy to break and presents a weak security model. Then, one challenge research is actually highlighting is to invent new rich authentication mechanisms, that can be used for IoT, having a better security, but also being simple for use for any costumer and supported by the sensors.

III. PROPOSED WORK

In the proposed encryption System, the sender object and the receiver object to share message they use secret key to encrypt and decrypt agree on a secret (shared) key in Cloud Computing [10]. In Symmetric cryptography, Objector thing Ai and Bi agree on the encryption technique used further used to encrypt or decrypt communication data, Secret key. Object Ai starts transfer its data encrypted with hash code to Trusted Third party object and TTPO to IOT Server (cloud Server) figure 2 on the other side object Bi uses the same hash code to decrypt the encrypted messages.

To access the outsourced encrypted files from IOT server it requires small data structure Block Status Table (BST) for inserting the data blocks which is implemented using linked list. It consists of two feature such as BSTnj and BNj , where BSTnj specify the sequence number of physical storage of data block j in the file and data blocks number is given by BSTsj. Initially the data Object A stores table entries as BSTnj = BSTsj = j.

In order to analyze security aspects of IoT, a reference architecture model Figure 2 will consider in the following.

A model of IoT Security Architecture:

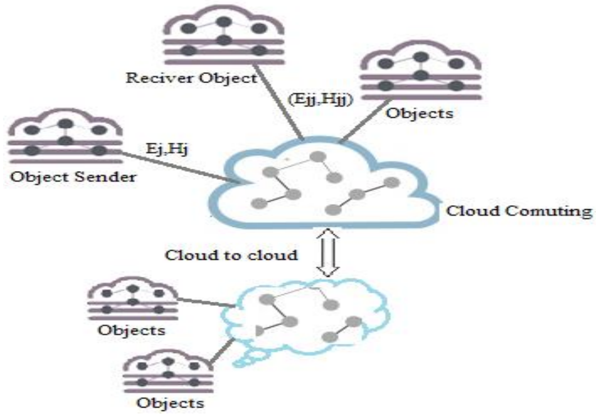

Figure2 IoT Security

The following are the sequence of steps for storing and accessing data in the server.

1. The data sender splits the source data into blocks of each carry 128 characters and prepare BST table by applying encryption algorithm for blocks ,then send the key ,encrypted data file and Block Status Table to trusted third party object(TTPO)
2. TTPO then sends the encrypted data (Ei) and calculate hash value (Hj) from Block Status Table (BST) to IOT Server (IOTS) for the storage.
3. the authorized object request for the data to TTPO and IOTS
4. TTPO verifies the authorized user and sends a request to IOTS Server
5. TTPO sends encrypted file/data and hash value to the Objecti.
6. IOTS Server which is another Object which sends the BST and encrypted data to the Objectj.
7. The receiving Objectj compares the hash value by calculate hash code using BST Table and encrypted file received from the Cloud Server, it verify the hash value received from TTPO if both the hash values are verified then Objectj gets the key for decryption and decrypt the blocks.

To achieve confidentiality data or the content that data is set of blocks. To define the block size as given bellow.

B = {b1, b2, b3,…..bm } …….(1)

each data block and an Encryption key is a set of characters defined below,

S = {c1,c2,c3, ... cn } ……(2)

& K = {k1,k2,k3…..ki}……..(3)
Fsize is given by

$$\delta = \sum_{i=0}^{B} \left|bm\right| \text{…….Eq.(1)}$$

Encoding: It will map each character to ASCII code and split into digit and Character and sum up with ASCII range
Circular Array (CA): it is used to shift operation applied on Character and Key .
Key Selector: Selecting key character for block of cipher text, so two keys are selected for each block of data.
Circular array Inverter (CaI): inverts the circular array to achieve higher security.
Shifter (CAS): it shift the array based on Eq.2

$$CA >> 2\left|Xi\right|\%5 \text{………Eq.(2)}$$

For encryption CA, Key selector, CaI, shifter is required

Thus, IoT can be broken down into three major layers as shown in Figure 3. Sensors collect data, gateways and communication units relay the information collected, applications and services analyze the information, and take actions. This architecture highlighting also some security aspects that are related to the three main layers:
Devices: The Devices Layer is divided between nodes and network. It includes Radio-frequency Identification (RFID) security and Wireless sensors network (WSN) [11]. Face in the IoT context many issues that we will define, such as heterogeneity, Cryptographic algorithms or Node trust management.

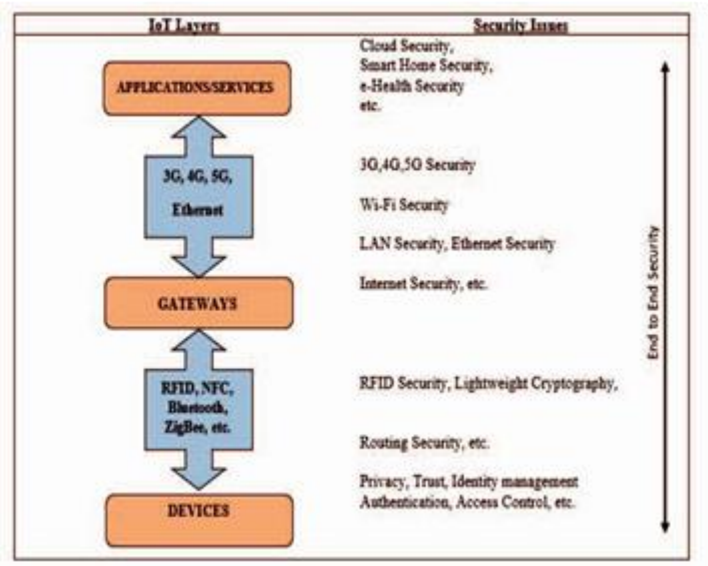

Figure 3: Security Architecture for IoT

Gateways: It is the layer regarding transport of data and tools used for it. This layer gathers security standards that are responsible of transporting data in 3/4/5G and WIFI networks.
Applications/Services: IoT applications are subjects to many attacks that can come from External services. Usual attacks to be stopped are Denial of Service (DDoS) attacks and Third Party attacks. Security should be guaranteed into IoT applications (such as smart home or intelligent traffic), and platforms for support, such as cloud computing should be monitored.

IV. CONCLUSIONS & FUTURE WORK

Internet of Things is for sure an amazing and exciting area, with many challenges ahead. In first section defined formally IoT After a general presentation of the challenges, IoT Architecture for security. This architecture helped us to exhibit data Integrity security issue mainly. In this article, the aim was to give a general image of IoT security, with a special focus on data integrity & encryption. The proposed new encryption algorithm provides efficient data communication for data transfer among the Objects scatted over the network

References

[1]. Lin, Jie, et al. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications." IEEE Internet of Things Journal (2017).
[2]. Talwana, Jonathan Charity, and Huang Jian Hua. "Smart World of Internet of Things (IoT) and Its Security Concerns." Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on. IEEE, 2016.
[3]. JunzuoLai,Deng R H,ChaowenGuan,JianWeng,Attribute-Based Encryption with Verifiable Outsourced Decryption, in IEEE Transactions on Information Forensics and Security, vol.8 (8), pages 1-7,2011
[4]. Usman, Muhammad, et al. "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things." arXiv preprint arXiv:1704.08688 (2017).
[5]. Xin, Mingyuan. "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System." Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2015 International Conference on. IEEE, 2015.
[6]. Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016, August). Internet of Things (IoT): Taxonomy of security attacks. In Electronic Design (ICED), 2016 3rd International Conference on (pp. 321-326). IEEE.
[7]. Zhou, Jun, et al. "Security and privacy for cloud-based IoT: challenges."IEEE Communications Magazine 55.1 (2017): 26-33.
[8]. Said, Omar. "Development of an innovative internet of things security system." Int. J. Comput. Sci. Issues (IJCSI) 10.6 (2013): 155-161.
[9]. Grabovica, Minela, et al. "Provided security measures of enabling technologies in Internet of Things (IoT): A survey." Zooming Innovation in Consumer Electronics International Conference (ZINC), 2016. IEEE, 2016.
[10]. Prakash, G. L., Manish Prateek, and Inder Singh. "Data encryption and decryption algorithms using key rotations for data security in cloud system." Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference on. IEEE, 2014.
[11]. Zhang, Zhi-Kai, et al. "IoT security: ongoing challenges and research opportunities." Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. IEEE, 2014.