ISSN 2278-3091
Volume 10, No.1, January - February 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse531012021.pdf
https://doi.org/10.30534/ijatcse/2021/531012021

Security of IoMT healthcare data using cryptographic techniques

Ranjeeta Pandhare[1], Swatee S. Nikam[2]
[1]Assistant Professor, India, ranjeeta.pandhare@gmail.com
[2]Researcher, India, swatee24@gmail.com

ABSTRACT

This paper is based on security measures to be provided to IoT related data, as there is an increasing demand to secure the IoT devices, networks and applications. The network resources are getting affected as the cybercrimes are increasing day-by-day. In this paper, first we highlight upon the key challenges and security issues in IoT architecture and then focus upon the case study of IoT application in healthcare IoMT, In Healthcare, prevention and cure have seen various advancement in technological schema. The Medical equipment when used with the Internet of Things are termed as Internet of Medical things (IOMT). IoMT is transforming healthcare industry by providing large scale connectivity for medical devices, patients, physicians, clinical and nursing staff who use them and facilitate real-time monitoring supporting the knowledge gathered from the connected things. Security constraints for IoMT take confidentiality, integrity and authentication as prime key aspect. These can be achieved by the integration of physical devices like sensors for connectivity and communication in cloud-based facility which in course is delivered by interface. Access Control security is obtained through key generation for data owners and the user of private health records while the data confidentiality is obtained by use of Advanced Encryption Standard (AES) as an efficient encryption algorithm.

Key words: Internet-of-Things (IoT), Security, IoMT, Cloud , Personal Health Records (PHR)

1. INTRODUCTION

During recent times Internet has penetrated in our everyday life. Many things have been revolutionized the way we manage our lives. Internet of things (IoT) is on top of this list. IoT is the huge network of connected things and people, enable users to gather and analyze data through the utilization of connected devices. With the increasing applications of IoT, perhaps in the near future, people can acquire benefits in manufacturing, retailing, health care, and other aspects of life [1]. Security is the major challenge for the IoT, as the IoT devices are increasing from millions of devices to tens of billions. With the increasing number of devices, there is increasing chance to exploit vulnerabilities in the cheap and low standard devices designed which leads to the security breaches in IoT. It is therefore necessary to understand the impact of security breaches on these devices. Firstly, we concentrate on the information obtained by hackers from IoT devices and network. In the figure1 , we show that there is several information such passwords, emails, login credentials, locations etc. that can be obtained by malicious hackers from various IoT devices like smart TV, smart camera, connected cars, Wi-Fi routers, medical devices etc [2]. Basically, the electronic devices like TV, refrigerators when connected to the internet become an IoT Devices. The statistics show that there are IoT devices have been increases from 8 million (year 2012) to 50 billion by the year 2020.

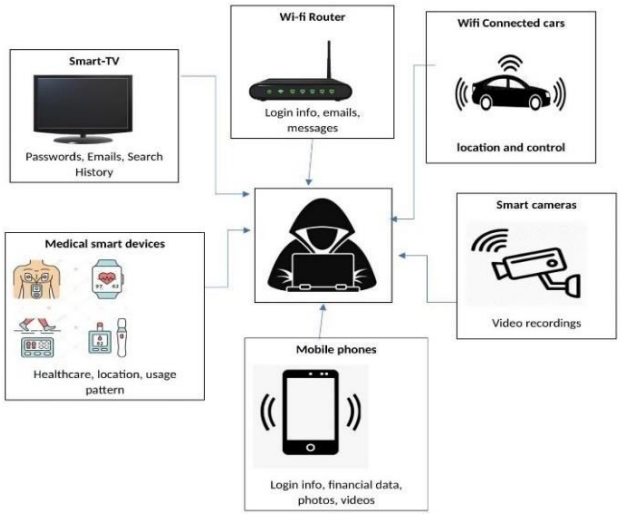

Figure 1. Information obtained by hackers from IoT devices

2. PREVIOUS LITERATURE

In [3], we come across that the Social Internet of Things (SIoT) is another worldview where Internet of Things (IoT)

combines with social networks permitting the individuals and devices to interact, and encourage data sharing. Security and privacy issues are an excellent challenge for IoT but it is also necessary to enable factors to make a "trust ecosystem.".

In [4], they have suggested that there are three classifications of security concerns namely Confidentiality, Integrity and Availability (CIA) in digital security. These categories CIA are also applicable to the IoT as a whole and they, individually, require explicit attention; trust and privacy are also ubiquitous security concerns in this arena. Thus, it highlights that, IoT security (IoTSec) is required in all layers of the IoT environment and it can be specific to the IoT layer in question.

In [5], they have presented taxonomy for IoT which would help researchers better understand and recognize (a) the critical domains where IoT is severely used, (b) the security requirements and challenges of IoT (c) existing security solutions that have been proposed or implemented.

In [6], in order to determine the problem and issues of attacks on the IoT devices, an Intelligent Security Framework is proposed. In this paper they have proposed the technique which consists of (1) the light weight Asymmetric cryptography for securing the End-To- End devices to protect the IoT service gateway and the low power sensor nodes (2) implementation of Lattice-based cryptography for securing the Broker devices or Gateway and the cloud services.

According to [7], it highlights upon the four layers of IoT which are application, access gateway, internet, and the edge technology layer. These four layers consists of an open network of IoT. Though, others break down the layers into three, the internet, application, and perception layer

In the paper [18] on Cyber vulnerabilities on Smart Healthcare, the authors have focused on the research questions related to the security breaches on smart healthcare such as the kind of attacks on health care devices and privacy protection for healthcare equipment. The proposed platform in the paper uses blockchain technology in order to consider security and privacy issues of healthcare system. The blockchain application can provide security to the different types of sensitive transactions on the system.

In the paper [19] for Secure Edge of Things for Smart Healthcare Surveillance Framework, the authors have proposed the Fully Homomorphic Encryption (FHE) as it has the ability to analyze and store the data in the encrypted form. IoT devices and cloud computing and encrypted analysis results can be retrieved by data owners and decrypted in a secure side

This paper [20] presents a secure lightweight authentication scheme that protects personal health information and guarantee secure communication. The proposed platform allows doctors to follow the real-time status of patient's bio-signals and equipped with an emergency rescue mechanism using remote health app and M2M patient monitoring screen. The analysis of security and encryption scheme to secure the medical information is conducted with the aid of fuzzy interface controller and the results show that the suggested scheme achieves better result than the state-of-the-art authentication mechanisms as it reduces the overhead of the access time and the key generation time is the highest among the transfer and verification time.

In the paper [21], the AES-128 based SeLPC (Secure Low Power Communication) is proposed to achieve the secure and low-power-consumption goal for LoRaWAN (Long Range Wide Area Network). Only application layer data encryption is considered. LoRaWAN is a long-distance communication protocol which uses AES-128 encryption method in order to ensure communication security.

3. SECURITY

3.1 Attacks on IoT Devices and Infrastructure

Some of attacks done on IoT devices and infrastructures are as given as below

1. Malware attacks [8]
   Malware attacks are the most frequent kind of attacks which targets a device's login credentials. But recently, other types of malware such as ransomware have been there onto IoT devices. The main types of malware that can infect any smart device –virus, worms, Trojans, adware
2. Password attacks
   Password attacks are the dictionary or brute force attacks that mainly target a device's login credentials by bombarding it with countless passwords and username variations until the desired one is found
3. IoT sniffer attacks
   In sniffer attacks, a malicious hacker captures the Internet traffic information, for example, emails, Passwords, credit card information which goes into and out of a smart gadget.
4. IoT spoofing
   Spoofing is an attack which disguises device A to look like device B. A disguised device A will trick the router into allowing the device B on the network, if device B has access to the network. The disguised device A now can communicate with the router and can inject malware into it. This malware spreads to all other devices on the network once it is injected.
5. Data leakage [5]
   Data Leakage or Data loss refers to losing the data due to hardware or software failure and the natural disasters. Sensitive data can be leaked by intruders and information can be revealed. It is thus necessary to ensure that alleged data are received from intended sensors only.
6. Vulnerability exploitation [8]
   Every software has its vulnerabilities. Depending upon the type of vulnerability such as code injection, cross site scripting (XSS) [5], Buffer overflows etc., they are used to exploit in various ways.

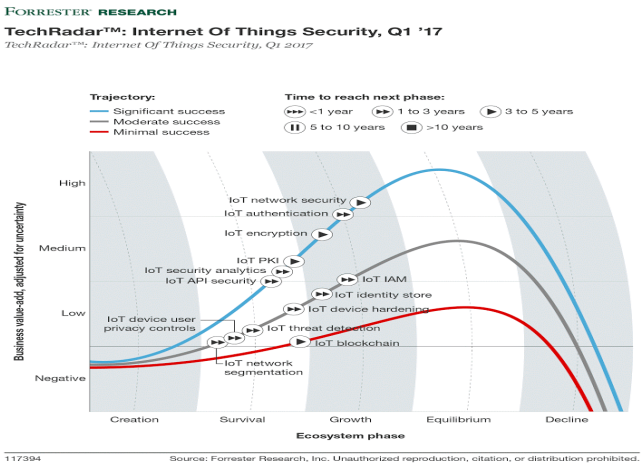

Figure 2: Forrester research for IoT Security

In the figure 2, the recently-released TechRadar report for security and risk professionals is highlighted in which Forrester Research discusses the outlook for the 13 most relevant and important IoT security technologies, warning that "there is no single, magic security bullet that can easily fix all IoT security issues."

3.2 Implementation of Security in IoMT Healthcare

Medical equipment utilized in the advanced technology in recent days also see the internet integration. Such equipment used with Internet of Things are termed as Internet of Medical things (IOMT). IoMT is transforming healthcare industry by providing large scale connectivity for medical devices, patients, physicians, clinical and nursing staff who use them and facilitate real-time monitoring supported the knowledge gathered from the connected things. Security constraints for IoMT [11] can be provided in terms of confidentiality, integrity and authentication (CIA).

Basic record of medical health of patient is stored in Personal Health Records (PHR). Several methods are employed to make sure the privacy of the PHRs stored on the cloud servers. The privacy preserving approaches confirm confidentiality, integrity, authenticity, countability, and audit trial. Confidentiality ensures that the health information is completely obscured to the unauthorized parties, whereas integrity deals with maintaining the originality of the information, whether in transit or in cloud storage. Authenticity ensures that the health related is accessed by authorized entities only, while responsibility refers that the information access policies must suits the recommended methods. The proposed framework empowers the patients to securely store and share their PHR within the cloud server (for example, to their care-givers), and furthermore the treating doctors can refer the patients' medical history to specialists for research purposes, whenever they're required, while ensuring that the patients' information remain private.

4. PROPOSED METHODOLOGY

In the proposed system architecture, we have the following

4.1 Phases of IoMT healthcare

1) Phase I: Data Collection, Data Acquisition
The proposed system consists of data acquisition of the patient data i.e., PHRs from the IoMT sensors nodes and once they are gathered in real time, they are encrypted and stored on the cloud These devices collect, analyze and send the data and have inherent accuracy, intelligence, reliability, capability, small size and low power consumption.

2) Phase II: Storage
The data collected the medical devices is stored the data collected from in the storage devices. Usually, IoT components are connected with low memory and have low processing capabilities. Thus, the cloud is the best possible solution which takes over the responsibility for storing the data in the case of stateless devices.

3) Phase III: Data encryption
The IoT analyses the data stored in the cloud DCs and provides intelligent services for work and life in hard real time. The confidentiality of the patient information is prior requirement of our IoT security. The data which is collected from the sensors is encrypted and stored.

4) Phase IV: Data Transmission
The encrypted data is then sent to the server, where data is stored in the encrypted form only. Data Transmission usually occurs through all parts, from cloud to user. The user could be doctor, medical attendant, pharma and patient himself.

5) Phase V: User authentication and data delivery
The user, in order to view their data, have to register themselves and then are authenticates to the server. Only authorized users can access the data which is decrypted once authenticated. Delivery of information is carried out through user interface which may be mobile, desktop or tablet.

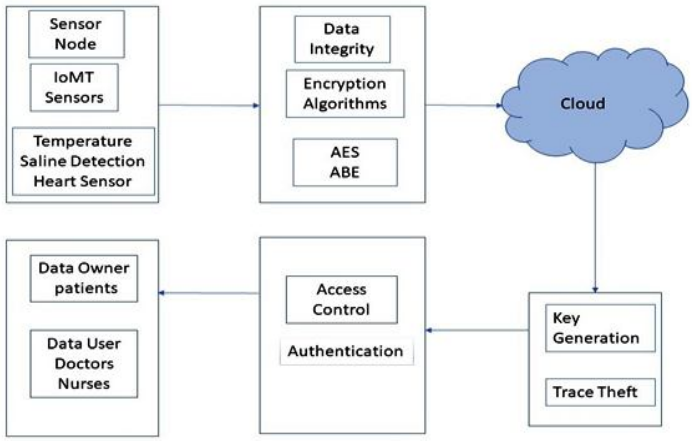

Figure 3 : IoMT proposed Framework

The figure 3 shows the proposed framework of IoMT which includes the design modules for IoMT sensors such as Temperature sensors, heart sensors, saline detection sensors etc. In this, the sensors data of the patients will be recorded and then stores on the cloud after encryption using AES cipher. Each user (patients, nurses) will be registered with username and password and will be given OTP on his mobile through SMS in order to view the data, this OTP will be verified with the server and then he will be provided with access to the data. Thus, the users are authenticated initially before fetching the data and also access control services can be achieved. In the proposed implementation, in order to encrypt the data received from the healthcare sensors, we are using the Advanced Encryption Standard - AES, a symmetric block cipher to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES encompasses three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256-bits, respectively.

Table1: Key size and Number of rounds of AES

No.	Key Size	Number of rounds
1	128 bits	10
2	192 bits	12
3	256 bits	14

The table1 shows the Key sizes and number of rounds of AES ciphers. Depending upon the number of rounds the key sizes are determined. If we are using AES with 10 rounds, it utilizes key size of 128 bits. We have used the AES-256 symmetric encryption algorithm, which is the most efficient symmetric block cipher. AES is extensively adopted and supported in the hardware and software. Till date, there are no practical cryptanalytic attacks against AES which have been discovered. Furthermore, AES has built-in flexibility of key length, which allows a degree of future-proofing against progress in the ability to perform exhaustive key searches.

4.2 Experimental Setup

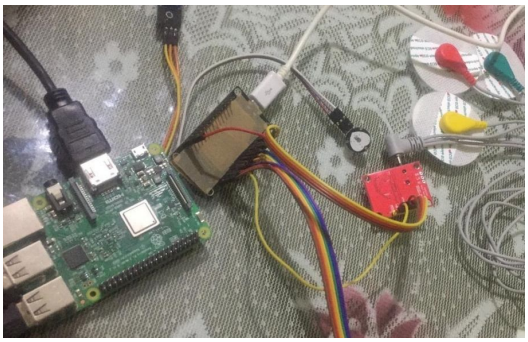

Figure 4. a) : Snapshot of sensors through Raspbery-pi3 module

In the figure 4a) and 4b), we have shown the experimental set up of IoMT sensors using Raspbery-pi3 and how the data is collected from the sensors. In the figure 4 c) , snapshot of ECG data collected from heart sensors is shown.

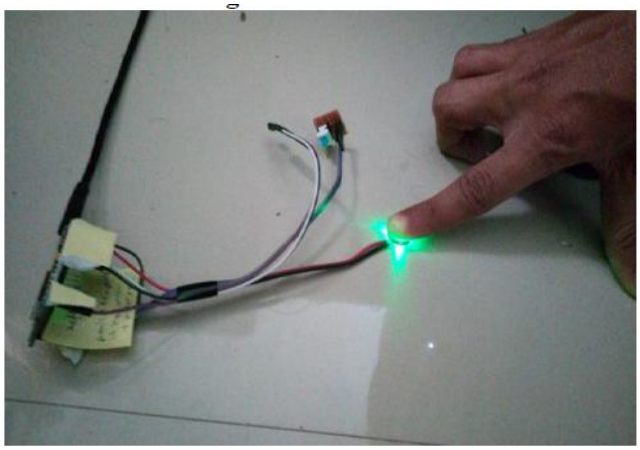

Figure 4.b): Snapshot of data collection from sensors

Figure 4. c) : Snapshot of ECG data collected from heart sensor

The sensors data is stored is the encrypted form which can be further decrypted after user authentication and key generation.

5. RESULT ANALYSIS

5.1 Time analysis of File uploads on cloud

In proposed system, data is stored on cloud. Before uploading files on cloud, files encrypted and then stores on cloud. While storing files on cloud, it will take some time to write files on cloud. In the figure 5 , the time analysis of file uploading is shown . In the experiment, file size considered in kb, as file

size increase required time to uploading increases exponentially

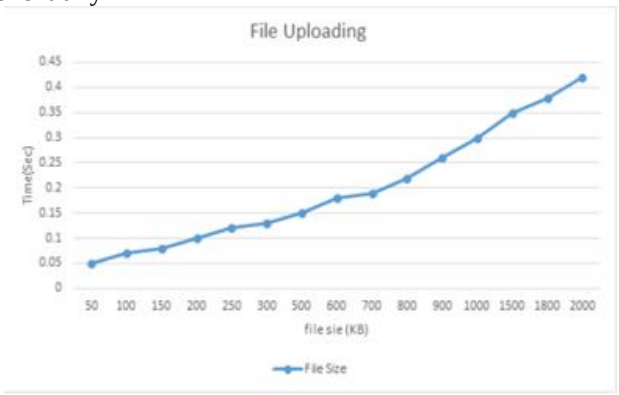

Figure 5: Time analysis – File uploading

5.2 Analysis on the basis of Comparison of Algorithms

First, the performance of the AES-256 symmetric encryption algorithm has been compared to algorithms like AES-128, DES, RSA with respect to encryption/decryption times, and security analysis. In the case of cryptographic algorithms, tradeoff is considered between speed and security.

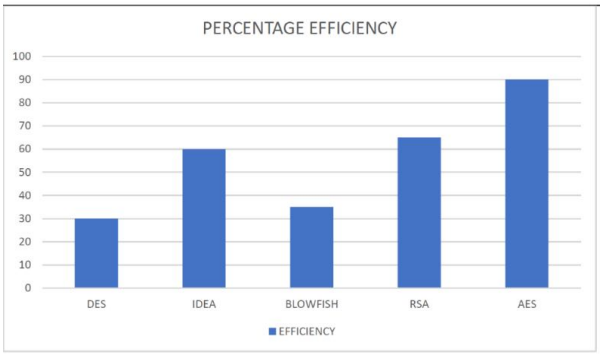

Figure 6: Comparison of algorithms

In the figure 6, it shows that the performance of AES algorithm is more efficient than other cryptographic algorithms in terms of security than speed because of its complexity. Also, it allows you various key lengths 128-bit, 192-bit and 256-bit making it strong encryption algorithm. It is mathematically efficient and more secure cryptographic algorithm.

6. CONCLUSION

In this paper, we have highlighted the key challenges and security issues in IoT. Also, the safety countermeasures of IoT in terms of authentication, encryption and IoT PKI are provided. This paper further covers the privacy preserving cryptographic and non- cryptographic methods which are employed within the e-Health clouds. In this research, a secure framework for authentication and encryption using AES-256 in IoT-based medical sensor data is proposed. The proposed authentication scheme also combines biometric parameters in addition to user credentials. To improve the security of IoMT sensors data, an additional level of security i.e. user authentication is used which enhances the system's security. Thus, we can ensure access control and privacy of the IoMT healthcare data.

ACKNOWLEDGEMENT

Authors acknowledge the support provided by Shivaji University, Kolhapur, Maharashtra, India for sponsoring this research work and helping us to find out the required resources in order to complete this research project.

We also thank institute, KIT's College of Engineering, Kolhapur for the constant support in making the project efficient.

REFERENCES

1. Jin-cui YANG, Bin-xing FANG, Security model and key technologies for the Internet of things, The Journal of China Universities of Posts and Telecommunications, Volume 18, Supplement 2,2011, Pages 109-112, ISSN 1005-8885, https://doi.org/10.1016/S1005-8885(10)60159-8
2. Mayuri A. Bhabad, Sudhir Bagade Internet of Things: Architecture, Security Issues and Countermeasures in International Journal of Computer Applications (0975 – 8887) Volume 125 – No.14, September 2015
3. "Evaluating Critical Security Issues of the IoT World: Present and Future" in IEEE Internet Of Things Journal, Vol. 5, No. 4 (2018).
4. Daniel Minoli, Kazem Sohraby and Jacob Kohns, "IoT Security (IoTSec) Considerations, requirements, and Architectures" (2017) 14th IEEE Annual Consumer Communications & Networking Conference (CCNC) 978-1-5090-6196-9/17/$31.00 ©2017 IEEE.
5. Syed Rizvi, Joseph Pfeffer III, Andrew Kurtz, Mohammad Rizvi "Securing the Internet of Things (IoT): A Security Taxonomy for IoT" 2018 17th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science
6. S. Sridhar and Dr. S. Smys, "Intelligent Security Framework for IoT Devices" Cryptography based End – To- End security Architecture in International Conference on Inventive Systems and Control (ICISC-2017).
7. Sumitra B, Pethuru CR &Misbahuddin M, "A survey of cloud authentication attacks and solution approaches", International journal of innovative research in computer and communication engineering, Vol.2, No.10, (2014), pp.6245-6253.
8. Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, *IEEE Fellow* "IoT Security: Ongoing Challenges and

Research Opportunities" in 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications 978-1-4799-6833-6/14 $31.00 © 2014 IEEE DOI 10.1109/SOCA.2014.58.

9. Trusit Shah and S. Venkatesan Authentication of IoT Device and IoT Server Using Secure Vaults 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering 2324-9013/18/31.00 ©2018 IEEE DOI 10.1109/TrustCom/BigDataSE.2018.00117.
10. Fei Hu, Security and Privacy in Internet of Things (IoT). Models Algorithms and Implementations, CRC Press, 2016.
11. Swatee S. Nikam, Jyoti P. Kshirsagar "Implementation of secure sharing of PHR's with IoMT cloud" in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, (2019).
12. Arjona, R.; Prada-Delgado, M.Á.; Arcenegui, J.; Baturone, I. A PUF- and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes. *Sensors* (**2018**,) *18*, 2429.
13. V. Alagar, A. Alsaig, O. Ormandjiva and K. Wan, "Context-Based Security and Privacy for Healthcare IoT," 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi'an, 2018, pp. 122- 128.doi: 10.1109/SmartIoT.2018.00-14
14. S. Venugopalan," Attribute Based Cryptology," PhD Dissertation Indian Institute Of Technology Madras, (2011).
15. Sankar Mukherjee, G.P. Biswas,Networking for IoT and applications using existing communication technology,Egyptian Informatics Journal,Volume 19,Issue 2,2018,Pages 107-127,ISSN 1110-8665,https://doi.org/10.1016/j.eij.2017.11.002.
16. https://www.controlcase.com/services/log-monitoring/
17. Weber, Rolf. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review. 26. 23-30. 10.1016/j.clsr.2009.11.008.
18. "Cyber Vulnerabilities on Smart Healthcare, Review and Solutions" **,** Nov 2018 DOI: 10.1109/CR.2018.8626826 Conference: 2018 Cyber Resilience Conference (CRC)
19. Abdulatif Alabdulatif, Ibrahim Khalil, Xun Yi, and Mohsen Guizan "Secure Edge of Things for Smart healthcare Surveillance Framework" IEEE access, 2019
20. A. A. Diro *et al.*: Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication
21. Kun-Lin Tsai, Yi-Li Huang, Fang-Yie Leu, Ilsun You, Yu-Ling Huang,Cheng-Han Tsai "AES-128 based Secure Low Power Communication for LoRaWAN IoT Environments" IEEE access, 2018