Securing Internet of Things Using RSA-OAEP encryption scheme

Yash Kumar and Amit Kumar

Abstract— In the past few years there has been a massive wave of IOT devices that has swept its consumers off their feet with its amazingly easy to use interface and left people awestruck with the advancement in technology today. However, with the exponential increase in the usage of internet in all such devices it is no surprise that the rate of cyber-crimes is increasing. Thus, the network of IOT devices is no longer secure. This insecurity brings risks to the privacy of data travelling through the connected devices. In today's technology, ever increasing number of electronics applications require secure communication, for example the Internet of things devices. RSA cryptosystem is widely used in various key exchange techniques that include the Diffie-Hellman Key agreement scheme. When contrasted with Optical Asymmetric Encryption Padding (OAEP), RSA offers equivalent security with smaller key sizes, which results in lower power consumption and data security. This is particularly valid and helpful for applications like IoT gadgets, which are regularly constrained regarding their CPU processing speed.

This work includes the software and hardware implementation of RSA-OAEP algorithm.

Keywords: Internet of Things, Architecture, Security, Encryption.

I. INTRODUCTION

The Internet of Things is one of the newest technologies that are being deployed to enhance the lifestyle of human race using Interconnected computing devices.

Recent development in relevant areas including embedded systems, wireless sensor networks, automation and electronics has accelerated the evolution of internet of things (IOT). Currently, IoT applications exist in nearly every field and are playing an increasingly important role in our daily life (e.g. healthcare systems, building and home automation, environmental monitoring, infrastructure management, energy management and transportation systems), which has led to the recent proliferation of IoT systems [1].

According to some researches, the global market size of IOT is expected to touch USD 3 trillion by 2020.

This work was in accordance to the requirements of a conference being held at Faculty of Engineering and Technology, Agra College, Agra.

Yash Kumar is an student of Bachelor of Technology, in The LNM Institute of Information Technology, Jaipur, in Communication and Computing Engineering. (e-mail: yashchaudhary830@gmail.com).

Amit Kumar, is an Assistant Professor in Computer Science and Engineering in Faculty of Engineering and Technolgy, Agra College, Agra. (e-mail: a1178mit@gmail.com).

In-order to connect these devices with each other there are technologies like Bluetooth, Z-wave, Zigbee, Wi-Fi (IEEE 802.11), RFID and many others. Today, almost every house, workplace, cafe, and university have a Wi-Fi network. Wi-Fi has become the de-facto term when referring to connecting to the Internet via a wireless access point. The widespread adoption of Wi-Fi makes it a first technology choice for many IoT applications [2]. Due to the highest adoption rate of Wi-Fi, we have concentrated on the security of Wi-Fi enabled IoT devices.

.

II. INTERNET OF THINGS

A. IOT Architecture

The Internet of Things is composed of 4 layers:

1. **Perception Layer**
2. **Network Layer**
3. **Management Layer**
4. **Application Layer**

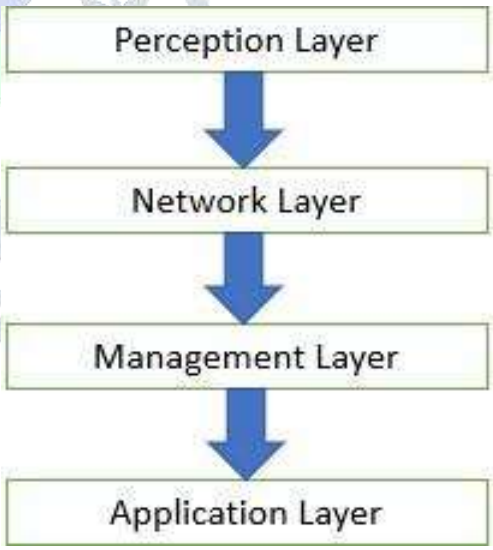

Figure 1

These layers are based on the Open System Interconnection (OSI) model. This section deals with the introduction of each layers of IoT and their security requirements.

1. Application Layer

The application layer is the topmost layer of the architecture and is the one to which user interacts to the IoT directly. This layer allows the user to interact with the services provided by the IoT system.

Depending on the application, the security issue of the layer is regarding data sharing. Sharing of data among different users with data privacy, information control and access-control is very necessary to make the IoT system secure and reliable. These issues can be achieved by proper Authentication and Key-agreement. This solution protects the data and IoT device by allowing the authenticated user to modify or access the data.

2. Management Layer

This layer is to Manage and control the data generated by the Perception layer and then transported by the Network layer. This layer works with both application layer and network layer.

To help with the security in the network layer this layer can do the mass data processing and make intelligent decision of what is suspicious behavior. Devices with limited resources could use this to generate keys for use in a secure authentication method.

3. Network Layer

The network layer handles the network communications and is responsible for securing the data transfer. It is involved with the transfer of data generated from the Perception Layer. The transfer of the information can use wireless technology such as Bluetooth, Infrared and Wi-Fi. Thus, securing the Wireless technology is very important for the privacy of data.

Since the nodes are connected to each other wirelessly and are movable, some nodes need to have the possibility to join and leave the system without prior authentication. This makes the network of nodes vulnerable. To prevent illegal nodes to connect to the network there should be a proper authentication process.

4. Perception Layer

This layer collects all kinds of information/data through sensing devices such as Radio Frequency Identification (RFID), GPS, Zigbee, Smart card and sensor networks. RFID technology uses microchips for wireless data communication which helps with automatic identification of the physical property they are attached to. The information that is gathered identifies the physical world in the digital world. The collected data is transmitted through Wireless Sensing Network.

In this research paper, we are going to implement the encryption scheme to encrypt the data collected from the Perception Layer and transmitted to Management Layer through Network Layer.

B. Security Requirements

IoT is constantly generating large amount of data which is processed and studied for future prospects. The protection of IoT means proper user authentication mechanisms and confidentiality about the generated data. There are five sets of functions required for ensuring security and privacy.

Five security features that are required for the security of IoT are:

i. Authentication The assurance that the communicating entity is the one that it claims to be.
ii. Access Control The prevention of unauthorized use of resources.
iii. Data Confidentiality The protection of data from unauthorized disclosure.
iv. Data Integrity The assurance that the data received is exactly as sent by authorized entity.
v. Non-Repudiation The validity of data cannot be denied by the entity involved in communication.

III. .SOLUTION – SECURE ARCHITECTURE OF IOT

All the security features can be achieved and implemented by use of some Cryptographic Algorithm. We need a solid encryption technique to secure the data flowing through the medium. Here the medium of transmission is taken as Wi-Fi (IEEE 802.11).

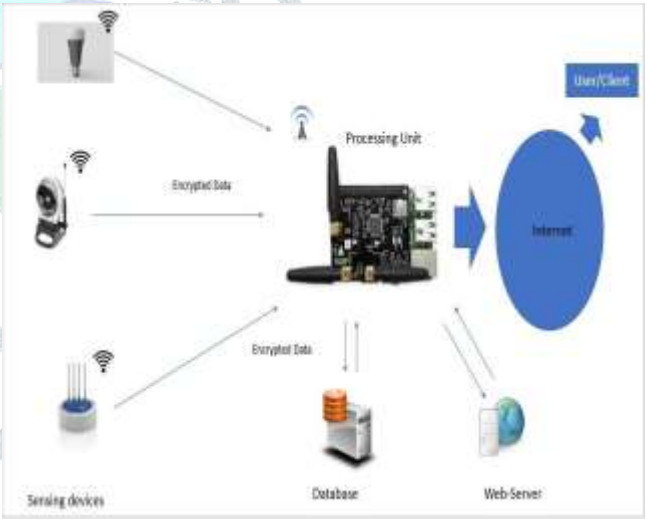

Figure 2: Architecture of IOT

The sensing devices are acting as the Perception Layer for collecting the real time data. The data is then encrypted using the RSA-OAEP[8] encryption scheme. This encrypted data will be then transmitted to the processing unit, where the data is collected and processed and made ready to be stored in the Database. Sometimes, the processing unit and the database can be a single unit collectively known as

Middleware Layer. To control the devices through internet, a dedicated web-application have to be deployed on the web-server so that the users can access the real time data through internet. The web-app is the application layer which is used to control the IoT devices or to access the data (from database).

Talking about the security, the application layer has to be made secure by end-to-end encryption of the data flowing between the client/user and the web-server. The SSL/TLS protocol used in the web-browsers provides HTTPs (http secure) to make an encrypted link between the client and the servers.

The need of encryption for security of IoT is within the IoT network itself. The data generated by the sensors is to be transmitted through the wireless network to the processing unit, which is again transmitted to the database for storage. Thus, encrypting this data (plain text) is our motive to gracefully secure the IoT devices.

Why RSA-OAEP?

There are certain flaws in RSA when it is being used for IoT specifically.

For the values of m=0 and m=1 the cipher text is 0,1 respectively. Since, IoT sensors generate mostly data in the form of 0's and 1's, the cipher text will be easily known.

When using small exponents (e.g., e = 3) and small values of the m, the (non-modular) result of m^e may be strictly less than the modulus n. In this case, ciphertexts may be easily decrypted by taking the eth root of the ciphertext with no regard to the modulus.

The RSA is a deterministic encryption algorithm. It has no random component. Therefore, an attacker can easily launch a Chosen Plaintext Attack against the cryptosystem.

The Optimal Asymmetric Encryption Padding (OAEP) is the most significant application of the random oracle model to date. It gives an efficient RSA encryption scheme with a strong security guarantee (semantic security against chosen-ciphertext attacks). After devastating attacks on RSA–PKCS #1 v1.5 in 1998, RSA–OAEP became the natural successor (RSA–PKCS #1 v2.0) and thus a de facto international standard [4].

An encryption scheme that is semantically secure under an adaptive chosen-ciphertext attack is said to be IND–CCA secure (IND stands for indistinguishability). IND–CCA security implies that even with full access to the decryption oracle, the attacker is not able to deduce one bit of information about the decryption of a given challenge ciphertext. The primitive RSA does not provide by itself an IND–CCA secure encryption scheme [4]. Thus, under a chosen cyphertext attack (CCA), the attacker can fully decrypt a challenge ciphertext.

RSA-OAEP Algorithm

Encryption Operation: -

RSAEP-OAEP-ENC ((n, e), M, P)

Input:
(n, e) - RSA public key
M - message to be encrypted
P – encoding parameters
Output:
C – cipher text of length k bytes

Steps:

1. Apply OAEP encoding to message M and encoding parameter P to produce an encoded message EM of length k-

1.
EM = EME-OAEP-ENCODE (M, P, k-1)
2. Convert the encoded message EM to an integer message m M = OS2IPC(EM)
3. Apply RSA encryption to the public key (n, e) and the message representation m to produce cipher text c
C = RSAEP ((n, e), m)
4. Convert cipher text c to C of length k
C = I2OSP (c, k)
5. OUTPUT – C Decryption

Operation: -

RSAES-OAEP-DECRYPT (K, C, P)
Input:
K - RSA private key
C – Cipher text to be decrypted
P – encoding parameter
Output:
M – Message

Steps:

1. Convert C to integer cipher text representation c c = OS2IP(C)
2. Decrypt using private key K
M = RSADP (K, C)
3. Convert message representation m to encoded message EM of length k-1
EM = I2OSP (m, k-1)
4. Applying decoding operation to EM
M **= EME-OAEP-DECODE (EM, P)**
5. OUTPUT – M

FUNCTIONS:

- **I2OSP – Converts a nonnegative integer to an octet string of a specific length.**
- **OS2IP – Converts octet string to non-negative integer.**
- **RSAEP – RSA-encryption.**
- **RSADP – RSA-decryption.**
- **EME-OAEP-ENCODE – OAEP encoding function.**
- **EME-OAEP-DECODE – OAEP decoding function.**

Implementation

The below, figure 3, shows the basic implementation of the algorithm in the IoT architecture.

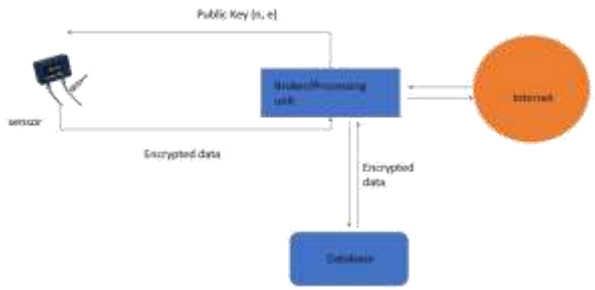

Figure 3

The main computational unit is the processing unit (also the broker of the information). The broker sends the RSA-public keys (n, e) to all the sensors of the system. Using this key-pair, the computational unit of the sensors encrypts the data produced by them. Therefore, the data that travels through the air is now a cipher text (C). This cipher text is then stored in the database for future use. Thus, the data in database is also kept secure by any attack as it is encrypted.

For accessing the real time information through internet, the users have to authenticate themselves on web-application. Only authenticated users can access the real time data from the processing unit (broker). The processing unit decrypts the data using the private key (K) which is not shared to anyone. Thus, the data that is transmitted throughout the system is a cipher text which cannot be read by the attacker anyhow.

IV. CONCLUSION

Security and privacy is the most imperative challenge to solve to maintain the trust of users in IoT. Pre-defined security solutions at each layer are still susceptible to attacks. To overcome RSA this simple CCA attack, practical RSA-based cryptosystems randomly pad the plaintext prior to encryption. This randomizes the ciphertext and eliminates the homomorphic property. According to the research done by Alfred Menezes [5], RSA-OAEP is both efficient and provably secure for short messages. Thus, RSA can be overtaken by RSA-OAEP in terms of security for the Internet of Things. One limitation of RSA-OAEP can be the computational power of the sensor devices. Since IoT devices are low power devices which have less energy and less computational units, implementation of RSA-OAEP in such cases may not be possible.

V. ACKNOWLEDGEMENTS

We wish to express our sincere gratitude to Dr. Anuj Kumar Parashar and Er. Pushkar Dixit, assistant professors at Faculty of Engineering and Technology, Agra College, Agra for providing us an opportunity and supporting us continuously for carrying out this research paper. We would also like to thank our family and friends for their understandings and support towards the completion for this paper.

VI. REFERENCES

1. Xiruo Liu , Meiyuan Zhao , Sugang Li, Feixiong Zhang and Wade Trappe , A Security Framework for the Internet of Things in the Future Internet Architecture ,28th June 2017.

2. Mahmoud Elkhodr , Seyed Shahrestani and Hon Cheung , EMERGING WIRELESS TECHNOLOGIES IN THE INTERNET OF THINGS: A COMPARATIVE STUDY,2016.

3. Eiichiro Fujisaki and Tatsuaki Okamoto, RSA–OAEP is Secure under the RSA Assumption,2001.

4. David Pointcheval, How to Encrypt Properly with RSA.2002.

5. Alfred Menezes, Evaluation of Security Level of Cryptography: RSA-OAEP, RSA-PSS, RSA Signature, 2001.

6. Isha and Ashish Kr. Luhach: Analysis of Lightweight Cryptographic Solutions for Internet of Things, July 2016.

7. Jacques Stern: Evaluation report on RSA-OAEP encryption scheme.

8. M. Bellare and P. Rogaway, Optimal Asymmetric Encryption - How to Encrypt with RSA. In Advances in Cryptology-Eurocrypt '94.1994.