

Internet Of Things (IOT) Cybersecurity based on the Hybrid Cryptosystem

Ming-Shen Jian*, Yu-En Cheng, Chen-Han Shen

Cloud Computing and Intelligent System Lab., Department of Computer Science and Information Engineering
National Formosa University, Taiwan

jianms@nfu.edu.tw*, f09789456123@gmail.com

Abstract— Since the Internet Of Things (IOT) are generally used, the data or information transferred between IOT devices and servers should be secured. In this research, hybrid cryptosystem based on the shared-key and asymmetric cryptography (or called Public-key cryptography) is proposed. According to the network communication, MAC address information of the IOT device is used for public-key querying and exchanging. Via asymmetric cryptography, the shared key can be automatically exchanged between IOT device and server. The implementation shows the feasibility of the proposed hybrid cryptosystem which could secure the data.

Keywords—Internet Of Things, Information Security, Network, Identity, Cryptography

I. INTRODUCTION

Internet Of Things (IOT) today is popular and generally used today [6]. By using various sensors with the network connection, the intelligent services, customized services, environment data collection, even the indoor location detection for the augmented reality [3,10] can be enhanced and developed. Due to the collected data from the various IOT sensors, all the corresponding information or data can be evaluated and further managed by the intelligent systems.

Suppose that the IOT elements can be divided into two partitions: sensor component and network component. The sensor component can be used to detect and collect the value of the environment parameters. The network component is used to transmit and exchange the data between the server and IOT element via network. Therefore, considering the various types of the sensors and the configuration of the network, to develop and implement the IOT system with network is not easy for general public. In other words, the cost and human resource will be needed and increased when the IOT system is deployed. It also means that the professional IT knowledge required for deploying the IOT system should be reduced then the IOT system can be more generally used.

Currently, the various types of sensor components which embedded with Arduino, Raspberry Pi, etc., are generally used. By programming the code of the tiny embedded system, different sensors such as ultrasonic sensor, infrared sensor, photosensitive sensor, etc., can be connected to the embedded system (ex. Arduino)[3]. The detected data or information can

be transmitted to the embedded system based on the on demand defined program. Then, based on the network component, this IOT element can be connected to the network. According to the framework of the network, each network component will equip the unique media access control (MAC) address. As people all know, the MAC address is the unique identifier assigned to individual network interface controllers. Therefore, based on this unique ID number (MAC address) which is similar to the Electronic Product Code (EPC), each IOT element can be identified [2] individually. According to the concept of the EPC Global, all the trade items or objects will be assigned the individual and unique ID number. Via the EPC network, this unique ID number can be used as the network URL link address. By tracing the unique ID number, the corresponding factory or manufacture of the object can be found. In other words, similar to the driver downloading or updating, by using the unique ID number, the driver or function can be found for each IOT element through querying the driver database of the manufacture. In other words, each IOT element can be identified. Individual IOT elements can be differentiated from each other.

However, considering the real implementation of the IOT systems, most IOT elements exchange or transmit the data by using the wireless network such as ZigBee, Bluetooth, Wi-Fi, LoRA, etc. All the detected data of the environment from the IOT elements will be sent via network. In other words, the data related to the privacy, local environment, even the secret, may be dangerous during the transmission. Furthermore, the IOT elements may be removed or re-located from one location to another. Not only the network transmission but also the valid network accessing should be considered [5,8]. One IOT element can access the network in one area but not in another. Therefore, to manage the corresponding area of IOT elements which are valid or not for the network accessing is also important for cybersecurity.

However, the IOT elements may connect to the network wirelessly. The security of wireless signal is not easy to maintain. The “eavesdrop,” “spoofing,” and “falsification” may happen when transmit the message via network [9].

In the past, various cryptosystems were proposed the secure and encrypt the wireless signal and data packets. Some cryptosystems require the assistance of complex computing.

Currently, the IOT elements can only provide the embedded computing system with low power consumption and limited computing performance. In other words, to implement complex cryptosystems for IOT elements is difficult. To embed the same cryptosystem into various IOT elements for different users is not safe, either. Hence, considering the differentiation of IOT elements, the cryptosystem or encrypt method based on the information of individual IOT element can be the possible. Since there is the network component of each IOT element, the cryptosystem based on the MAC address [4] of the network component and the information of sensor component can be the solution.

The contributions of this research are:

Based on the components of IOT element, the unique MAC address and the IOT sensor information can be used to implement the cryptosystem for the wireless or wire data transmission. Each IOT element can be identified and differentiated. Therefore,

- 1) Even the same type of IOT elements can be differentiated and distinguished according to the corresponding network MAC address and the information from the manufacture. The IOT element related information can be traced also based on the MAC address. In other words, the identification of individual IOT device and corresponding information obtaining can be achieved.
- 2) According to the identification information of individual IOT element, the encryption method of the cryptosystem can be defined independently and individually. In other words, different IOT elements can be assigned different encryption key based on the same cryptosystem. The security of data transmission can be enhanced.
- 3) Due to the unique MAC address, the information exchanging between the local IOT element management server and remote manufacture can be done automatically similar to the EPC Global network. Hence, the network managers or system users only need to decide the valid network accessing area of the IOT elements. The workload and cost for managing the IOT elements and maintaining the cryptosystem can be reduced.

The rest of this research is organized as follows. Chapter 2 will introduce the related technologies used in this research. The whole proposed infrastructure and system is presented in Chapter 3. The conclusion will be given in Chapter 4.

II. RELATED WORK

A. Identification for Internet Of Things (IOT) elements

Today, most IOT elements equip two components: sensor component and network component. Network component is used for the network connection. Then, the data or information can be exchanged between IOT elements and hosts [6]. However, the network configuration such as IP address should be on demand given to the individual equipment before connecting to the network.

In the past, the network administrator or manager should identify individual equipment first. Then, according to the identification results, network manager can configure and arrange each network equipment or device individually such as IP address assignment, network environment configuration, etc. Considering the real implementation of IOT system, there will be huge amount of various IOT elements deployed in the environment. The cost and time consumption will be increased very quickly. Therefore, to automatically identify individual IOT element when arranging the network configuration is important.

Suppose that the IOT elements are connected to the embedded system such as Raspberry Pi. The sensor component of the IOT element with the limited memory may provide the device description similar to the description of USB device. In other words, according to the device description, the IOT element can be the "Plug & Play" device for the IOT systems or services. However, considering the physical system implement, to deploy the IOT elements and systems with the wire line including USB connection [2], power line connection, network connection, etc., is not easy. In other words, the network will be the wireless connection. To obtain the corresponding information from the IOT elements automatically for identification becomes an important issue.

Today, electronic product code (EPC) is generally used in supply chain application [1]. By assigning the unique EPC number to individual object or trade item, this unique EPC number can be used instead of the object itself. The EPC number includes the manufacture number (EPC manager number), classification number, and serial number to indicate individual object. In other words, according to the EPC number, the manufacture or type of each object can be differentiated. In addition, based on the EPC number, the corresponding information can be traced and tracked through the EPC network. In other words, by using the EPC identification number, the object can be identified according to the information through the EPC network. Therefore, different members of the supply chain can share the information with each other.

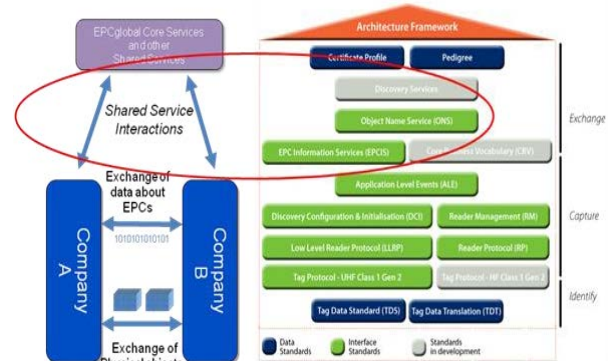


Figure 1. EPCGlobal Architecture Framework [1]

Since the IOT element includes the network component with the unique MAC address, if the network component is not separable, this unique MAC address of the network component can be used similar to the EPC number to indicate the individual IOT element itself.

In addition to the MAC address, the sensor component of IOT device can record the device information such as device description file. Currently, the Universal Serial Bus (USB) is also a world popular connection standard for the communications between devices. Different devices can exchange the device related information and obtain power via USB connection. Therefore, the plug-in USB electronic devices can provide the corresponding information such as device description driver, data, etc., to the connected master host or device. Finally, the master host or device can identify individual USB device and active (control) the corresponding device.

B. Security

Today, considering the information protection, many security algorithm and methods are proposed. To secure the information, the content of the message can be encrypted when the information sender and receiver use the same security code (key) to encrypt and decrypt the same message or information, the content can be secured and obtained between sender and receiver. Considering the implementation and using of IOT, huge amount of information will be exchanged between sensors through the Internet [8]. To secure the messages with less computing power or less power consumption of each IOT device becomes an important issue [11].

If the information is exchanged and transmitted directly through the network, the malicious third party can eavesdrop the packet or message transmitted. Without encryption, all the content of the message can be known by the malicious third party. Therefore, to encrypt the information or content of the message packer is needed. Hash functions such as Message Digest Algorithm 5 (MD5), Secure Hash Algorithm (SHA-2), etc., for encryption are the generally used. By using the same hash function, different terminals with the same input value can obtain the same hash code. In addition, the malicious third party cannot recover the original content according to the hash code.

Considering the real implementation, the most types of network used IOT environment is wireless network. In other words, the spoofing and falsification security issues may happen. Therefore, digital signature was proposed for the information exchanging related to the spoofing and falsification security issues. Shared-key encryption such as advanced encryption standard (AES), or data encryption standard (DES) can be the possible to secure the data content of the message packet. However, using the shared-key encryption, the encryption key should be exchanged between sender and receiver. It means that the shared key may be peeked by the malicious third party. To enhance the security, the public-key cryptosystem, also called asymmetric cryptosystem, was proposed. By using the public key for

message packet encryption, receiver can use the secret-key to decrypt. For example, the RAS cryptosystem is the popular encryption method. However, if the malicious third party can send the malicious third party made public key instead of the original public key of receiver. Then, the sender would use the wrong public key to encrypt the message packet. In other words, by "man-in-the-middle attack" method, the malicious third party can peek all the content from the data sender.

Today, to quickly obtain the content of message packet with better security is important. By using the shared-key cryptosystem, sender and receiver would use the same encryption key for message packet security. In addition, the performance of the message decryption can be faster. To transfer the shared key, the public key cryptosystem can be used to protect the information of shared key.

III. PROPOSED SYSTEM

According to the Internet of Things implementation, most sensors would be located at the fixed positions or area and exchange the messages wirelessly. However, the wireless signal would be transmitted in all directions. In other words, other invalid receivers may have the messages sent from the IOT devices. Therefore, secure the messages and transmit the data through the valid network via configuring the network is an important issue. Considering the real verification, the Internet Of Things (IOT) Cybersecurity Based on the integration of Self-identification with Cryptosystem and Software Defined Network is proposed which includes Self-identification Procedure and Cryptosystem and Cybersecurity of IOT. The flowchart of initial configuration corresponding to individual IOT device can be shown as follows.

A. Self-identification Procedure

In the beginning, each IOT device will check its network configuration. If there is no network configuration information, it means that the IOT device may be new connected to the local area network. Therefore, this new added IOT device should registered itself. First, considering the development of IOT device, the network module will be embedded as the part of IOT component. In other words, there will be a MAC address assigned to the network module. Since the MAC address should not be repeatedly used, it means that this MAC address can be used to identify the IOT device itself. Similar to the EPCglobal network, this MAC address can be also used to find and trace the original manufacture. Considering the possible tapping, in this research, two different MAC addresses are assumed and supposed to be assigned to one IOT device: broadcasted MAC address and network address. The broadcasted MAC address will be used during initialization for network configuration exchanging and the identification.

If the broadcasted MAC address received from the IOT device is correct, the proposed local service server or system can query the public key from the database of the manufacture. In opposition, the unique private key is already recorded in individual IOT device.

When the client management system or third party system queries the public key related to the broadcasted MAC address of the IOT device, the information server of manufacture can reply the corresponding public key to the client management system or third party system. Furthermore, since the broadcasted MAC address of the IOT device (or the corresponding public key) is queried, the server of manufacture will mark the public key as used. In other words, the public key cannot be repeatedly used.

In other words, according to the broadcasted MAC address, each IOT device can be individually identified. The administrator can differentiate each IOT device according to the individual broadcasted MAC address. It also means that every IOT device can be also identified due to the broadcasted MAC address. Furthermore, the corresponding public key can be also managed according to the query which comes from the client system.

In addition to the corresponding public key, the type and function of the specific IOT device can be also identified. The driver or configuration data can be also exchanged between the client management system or third party system and the manufacture server. Therefore, the information updating or upgrading corresponding to the individual IOT device can be achieved according to the result of self-identification.

B. Cryptosystem and Cybersecurity of IOT

Considering the cybersecurity of each IOT device, two step security methods, same encryption key (Shared Key Cybersecurity) and public-key cryptosystem (Asymmetric Cryptosystem), are both used in this research. According to the self-identification procedure result, the public key from the manufacture server can be obtained. In addition, each IOT device was already assigned a private key by the manufacture. In other words,

Therefore, in the beginning, the service server cannot obtain the information except the MAC address. Based on the Asymmetric Cryptosystem, the on demand embedded private key of the individual IOT device can be used to transmit the encrypted ~~shared key~~ between IOT device and the service server. In other words, without the public key, the ~~shared key~~ cannot be obtained at the client side. Therefore, based on the self-identification result, the public key can be obtained for the IOT device. Therefore, the ~~shared key~~ which is encrypted by the private key can be transmitted to the service server with security. In opposition, the invalid users cannot obtain the public key since the information packet is secured. To reduce the risk of tapping, the time limitation of the MAC address broadcasting and network configuration can be on demand given. In other words, the network administrator should assign the IP related information to the IOT device within the limited time. Otherwise, additional time period delay will be required for another MAC address broadcasting and network configuration. Since additional time period delay can be assigned randomly or manually (presented in the guide book, etc.), the risk of tapping can be reduced.

After the configuration of network and the public key querying, the ~~shared key~~ which is on demand embedded in

the IOT device can be exchanged to the service server. At last, all the information can be secured and exchanged based on the ~~shared key~~. In other words, based on the proposed Cryptosystem and Cybersecurity of IOT, the Shared Key Cybersecurity and Asymmetric Cryptosystem are both used for security. Only the MAC address information in the beginning will be transmitted without encryption. Therefore, all the information packets exchanged between the IOT devices and service server will be secured according to the corresponding ~~shared key~~. The security of the IOT implementation can be enhanced.

Instead of the Asymmetric Cryptosystem based on the private key and public key, the common ~~shared key~~ is used to transmit the data between IOT device and the service server. Based on the Shared Key Cybersecurity, the same encryption key can be both used in IOT device and service server. Without the private and public key pair, the encryption and decryption of the transmitted packet can be faster. In other words, the time delayed can be reduced.

The proposed Cryptosystem and Cybersecurity of IOT can be shown as follows. During the Self-identification procedure, the local service server can obtain the on demand defined public key stored in remote manufacture server. Based on this obtained public key, the secured ~~shared key~~ can be decrypted and recorded in the local service server. In addition, since the network of the IOT device is also configured, the MAC address and the encrypted ~~shared key~~ will be no longer transmitted. In opposition, only the data which is secured and encrypted by the shared key will be transmitted through the network.

In other words, there will be three steps of security method for the IOT devices: 1) Asymmetric Cryptosystem based on the private key and public key will be used to protect the common ~~shared key~~. In addition, only the broadcasted MAC address can be used to find the corresponding public key. 2) Shared Key Cybersecurity based on the individual ~~shared key~~ will be used to secure the information or data transmitted between IOT devices and service server. In other words, each IOT device can be assigned an individual ~~shared key~~ for enhancing the security. Especially, this ~~shared key~~ is already secured and not public due to the symmetric Cryptosystem. 3) Manual operation of the network configuration. When an IOT device is new added into the local network, the IP corresponding to the correct sub-network will be assigned. In other words, the broadcasted MAC address will be only transmitted within the manual operation time. After network configuration, the broadcasted MAC address will no longer broadcasted. It means that the invalid user cannot have the chance to gain the public key.

Figure 2 presents the sequence between IOT device, service server, and manufacture server. In the beginning, the IOT device should broadcast its own MAC address to the local area network manager (such as router or service server). By receiving the MAC address, the service server can query the related data from the manufacture server through the Internet similar to the EPCIS and object name service (ONS) defined by the EPC Global [1]. In addition to querying the

corresponding information, the IP can be assigned to the IOT device via local area network (LAN). The time for MAC address broadcasting can IP assignment will be on demand limited. After querying, the service server and obtain the public-key from the manufacture server based on the Internet. Therefore, when the IOT device send the shared-key which is secured by the private key through the local areas network, the service server obtained the shared key. Finally, the data encrypted by the shared key can be transferred to service server via local network with less encryption time delay.

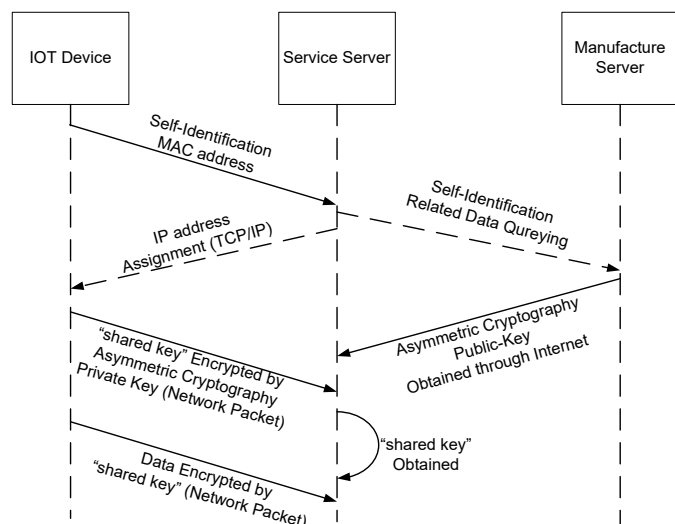


Figure 2. Sequence between IOT device, service server, and manufacture server.

C. Implementation

To verify the Cryptosystem and Cybersecurity of IOT device, Arduino with sensors and Raspberry Pi are used. There will be two on demand given security keys: private key and the shared key. After receiving the MAC address from the Arduino, the corresponding public key can be obtained from third server (emulating the server of manufacture). Then, the encrypted common key can be obtained at the service server. Finally, the data exchanging between the IOT device and local service server can be secured.

In addition, to enhance the security of the data exchanging between IOT devices and local service server, additional procedures for data encryption will be needed. In the beginning, the Asymmetric Cryptosystem based on private key for the shared key encryption will require about 0.198 seconds for public key decryption. This time delay will happen only once when IOT device and local service server exchange the shared key. In other words, by using the Asymmetric Cryptosystem for the shared key (command key) protection, only the addition time delay will be needed once.

In the implementation, the private key of Asymmetric Cryptosystem is 751 Bytes. The public key of Asymmetric Cryptosystem is 498 Bytes. The length of the shared key is 154Bytes.

```
Config HostName:
192.168.1.106
Config PortNumber:
54321
===== Key Pair Checker and Repairer =====
---- Key Not Found and Ready to Fix ----
*****GENERATE PUBLIC/PRIVATE KEY*****
Public Key - Sun RSA public key, 2048 bits
Modulus: 2243386628049382619484200064858343100719931942102170820046432045294011128544390028
41647765358600181713075368522286205709751459650880012372943094401956654892475903736162476899
055186513331655156478128563304322759253180145873280407482519523000268656765347341315450901542
576928375775662788972073514972960580260348976965363708424011516769564833266128174910092772683
102643172160686027736602281940947861810037150061614067758360628270773317280674996024959809872
8245741290153584165865824369
Private Key - sun.security.rsa.RSAPrivateCrtKeyImpl@ffe60290
public exponent: 65537
*****SOME PARAMETERS ABOUT KEYPAIR*****
Public Key Modulus: 2243386628049382619484200064858343100719931942102170820046432045294011128544
46316236416477653586001817130753685222862057097514596508800123729430944019566548924759037361
575161410551865133316551564781285633043227592531801458732804074825195230002686567653473413154
847840365769283757756627889720735149729605802603489769653637084240115167695648332661281749100
228775311026431721606860277366022819409478618100371500616140677583606282707733172806749960249
692546418245741290153584165865824369
Private Exponent: 65537
Private Modulus: 2243386628049382619484200064858343100719931942102170820046432045294011128544
316236416477653586001817130753685222862057097514596508800123729430944019566548924759037361
516141055186513331655156478128563304322759253180145873280407482519523000268656765347341315450
784036576928375775662788972073514972960580260348976965363708424011516769564833266128174910092
877531102643172160686027736602281940947861810037150061614067758360628270773317280674996024959
2546418245741290153584165865824369
Private Exponent: 881991849769144034265070095841128955142129887242390303940008973237186486077
091797725055579631306328031356324724236137802684912242637654882166060960355450660840962138425
96836734101249221818860737927370130001648252006408042130312616071223933998963077588824867660
0563416620503869734008972160979386207671654127390970352948223484695368570023825667528008126241
128394455775027740609082027042015957740624095319367618879302349025346184879275987204030491303
1037466938229566333934302460252065
*****SAVING KEY INTO FILE*****
```

Figure 3. A example of Asymmetric Cryptosystem for encrypting Shared Key Cybersecurity

IV. CONCLUSIONS

According to the proposed system, the exchanged data from the IOT devices can be hiding and secured by the two steps of Cryptosystem methods. Although the addition tiny time will be required for encryption, the information can be secured with less manual operation. By using the self-identification method, the security and key can be automatically exchanged. Only the corresponding network address will be assigned by the router or according to the manual operation. The IOT devices and security system can be managed with higher security.

ACKNOWLEDGMENT

Thanks for the support of Cloud Computing and Intelligent System Lab. of National Formosa University.

REFERENCES

- [1] EPCGlobal website. [Online]. Available: <https://www.gs1.org/epcglobal>
- [2] M.-S. Jian, J.-Y. Wu, J.-Y. Chen, Y.-J. Li, Y.-C. Wang, H.-Y. Xu, "IoT base Smart Home Appliances by using Cloud Intelligent Tetris Switch," *ICACT*, pp.589-592, Feb. 2017.
- [3] A. S. Ali, Z. Zanzinger, D. Debose, B. Stephens, "Open Source Building Science Sensors (OSBSS): A low-cost Arduino-based platform for long-term indoor environmental data collection," *Building and Environment*. Vol. 100: 114-126. 2016
- [4] C. B. Westphall, C. M. Westphall, J. Werner, Daniel Ricardo dos Santos, "Security in the Context of Internet of Things, Cloud, Fog, and Edge," *IWCSS 2017*, Dec. 2017. (DOI: 10.13140/RG.2.2.20008.67841)
- [5] Z. Yan, P. Zhang, A.V. Vasilakos, "A survey on trust management for internet of things," *J. Netw. Comput. Appl.*, Vol. 42, pp. 120-134, 2014, DOI: 10.1016/j.jnca.2014.01.014.

- [6] L. Xu, W. He, S. Li, "Internet of things in industries: a survey." *IEEE Trans. Ind. Inf.*, Vol. 10(4), pp. 2233–2243, 2014, DOI: 10.1109/TII.2014.2300753.
- [7] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.
- [8] T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar, K. Wehrle, "Security challenges in the IP-based internet of things." *J. Wirel. Pers. Communic.*, Vol. 61(3), pp. 527–542, 2011, DOI: 10.1007/s11277-011-0385-5.
- [9] B. Kamal, et al. "Software-defined networking (SDN): a survey," *Security and Communication Networks*, vol. 9 no. 18, pp. 5803-5833, Dec. 2016.
- [10] M.-S. Jian, Y.-C. Wang, B.-H. Wu, Y.-E. Cheng, "Hybrid Cloud Computing for User Location-aware Augmented Reality Construction," *ICACT*, pp.190-194, Feb. 2018.
- [11] M.-S. Jian, Y.-L. Chen, S.-J. Li, "Wireless Power Charger with Dynamic Pivoting Antenna Module for Various Wireless Sensor," *13th EHAC'15*, Sept. 2015.



Ming-Shen Jian was born in Kaohsiung City, Taiwan in 1978. He received the B.S. from the National Chiao Tung University, HsinChu, and Ph.D degrees in Computer Science and Engineering from the National Sun Yat-sen University, Kaohsiung, Taiwan in 2007.

From 2009, he was a Assistant Professor and director with the National Formosa University Cloud Computing and Intelligent System Laboratory. Since 2009, he has been an Assistant Professor with the Computer Science and Information Engineering Department, National Formosa University. He is the author of four books, more than 50 articles, and at least 15 invention patents. His research interests include IOT development and application, Big Data, Optimal Solution, Intelligent System, and Cloud Computing. He was a Secretary of the Taiwan Association of Cloud Computing. Dr. Jian was a recipient of the IEEE sponsored international conference Paper Award in 2016, 2017, and 2018.



Yu-En Cheng is a master degree student of Dept. Computer Science and Information Engineering at National Formosa University. Her current research interests are in the area related to IOT and Information security. She received B.S. degree at Computer Science and Information Engineering at I-Shou University, 2017. Her current research interests include Internet Of Things and Cryptography.



Chen-Han Shen is a master degree student of Dept. Computer Science and Information Engineering at National Formosa University. His current research interests are in the area related to the integration of IOT system and Cloud Computing. He received B.S. degree at Computer Science and Information Engineering at National Formosa University, 2018. His current research interests include Cloud Computing, and Intelligent System.