Design and Theoretical Analysis of the Application of the Certificateless Public Key Encryption Scheme for Home Monitoring System Security

Hadyan Radifan* and Amiruddin Amiruddin
Sekolah Tinggi Sandi Negara, Bogor, Indonesia
*hadyan.radifan@student.stsn-nci.ac.id

Abstract. Internet of Things (IOT) is becoming a trend in the field of information and technology today. IoT provides many benefits such as to turn on the lights, make temperature measurements, and measure heart rate. However, behind the benefits offered, there are also various security issues. Imagine if IoT is utilized in a strategic work environment and should have high security priorities but certain security mechanisms are not implemented, then the transmitted data can be interrupted and misused by unauthorized parties. Therefore, safeguarding the data transmitted through the system and technology is very necessary. One method that can be used for security is to implement a certificateless-based public key encryption scheme. In this study, to get the right security scheme, a literature study was conducted first, then a design was made for the application of the scheme for home monitoring system.

1. Introduction
Many benefits can be obtained if Internet of Thing (IoT) technology is applied in various human activities. IoT makes it easy to automate activities such as light bulb lighting [2] and temperature monitoring [3]. IoT also supports remote activities such as for heart rate measurement [4], home security monitoring [5], and access control [6]. However, behind the various benefits offered, IoT also raises security issues [7]. In communication between control devices with connected sensors or other supporting devices, if the data sent is still in the form of plaintext, there is a vulnerability by the presence of unauthorized parties who can intercept the data. If this happens then the communication process may be taken over and misused.

Suppose this happens in a home security monitoring system. By using IoT, homeowners can monitor the condition of their house through a smartphone or other smart device. When the homeowner is monitoring and at the same time someone else is eavesdropping it and obtaining a visual appearance as seen by the homeowner, then this is a vulnerability. The danger that arises from the description is that the eavesdroppers can monitor and study the characteristics of the house and its environment so that they can find out the vulnerabilities and can vent their bad intentions.

One of the security methods used in IoT is the application of public key encryption schemes [8] [9]. The disadvantage of the public key encryption scheme is the use of certificates that require considerable effort to distribute, verify, store, withdraw, and use which can become a computational burden for the system [10]. To overcome this problem, Shamir [11] proposed an identity-based public key cryptography scheme. However, this scheme arises a key storage problem at the third party. To overcome such a problem, Guo et al. [10] proposed a new method for public key cryptography without the use of digital certificate called certificateless public key cryptography. The question is how to get the right scheme?
In this study, a literature study was first conducted to choose a certificateless public key encryption scheme for home monitoring system. The next step was an initial design for implementing the selected scheme. The Certificateless Public Key Encryption (CL-PKE) scheme proposed by Guo et al. \cite{10} was chosen since it has the strongest security compared to other studied schemes. The security assumption is the difficulty of factoring the prime numbers in the RSA algorithm used by the scheme. The contribution of this study includes a literature review of certificateless public key encryption schemes, initial design, and security analysis of the implementation of a certificateless public key scheme for home monitoring systems.

2. Method and Materials

2.1. Research Method

The method used in this study consists of four stages: literature study, scheme selection, implementation design, and security analysis. A brief literature review was conducted to compare several certificateless public key encryption schemes. From the literature review, a certificateless public key encryption scheme has the highest advantage to be applied in a home monitoring system. Next, making the initial design for the implementation of the selected scheme. Finally, a theoretical security analysis was carried out on the implementation of the scheme for home monitoring systems.

2.2. Selection Method

From the results of the literature review conducted in the previous section, the scheme from Guo et al. \cite{10} was chosen to be implemented because the scheme has several advantages over the other three schemes. These advantages are: the scheme is claimed to guarantee the confidentiality and integrity of information in the IoT scenario; the setup stage of the probabilistic polynomial-time algorithm from the scheme is simpler and more effective than the other three schemes because it simply generates a random value that is used as the master secret key and can be used to calculate public key values and security parameters; the private key generator only generates part of the value of the private key so that the key generator does not have a private key in its entirety; and in the scheme there is an explanation of the general design of the application of the scheme on IoT, while other schemes do not explain the general description of its application.

Table 1 Characteristics of four certificateless-based public key encryption schemes

| Scheme        | Characteristics                                                                 |
|---------------|----------------------------------------------------------------------------------|
| Riyami et al.[12] | • The scheme is derived from Pairings on the Elliptical Curve.                   |
|               | • Security is based on the assumption of the difficulty in solving the Bilinear Diffie-Hellman Problems (BDHP). |
|               | • Using seven randomized / seven probabilistic polynomial-time (PPT) algorithm. |
|               | • The scheme is based on Elliptic Curve on the Ring.                            |
| Guo et al. [10]  | • Safety is based on the assumption of the difficulty in solving the Bilinear Diffie-Hellman Problems (BDHP) and the difficulty of factoring in prime numbers in the RSA. |
|               | • Using seven randomized / seven probabilistic polynomial-time (PPT) algorithm. |
|               | • Claimed to guarantee the confidentiality and integrity of information in the IoT scenario. |
|               | • The scheme is based on the Identity-Based Encryption scheme                    |
| Trinh [13]     | • Security is based on q-BDHI assumption and very simple static assumption.     |
|               | • Using the Bilinear Pairings algorithm.                                        |
|               | • Claimed to be resistant to weak selective chosen plaintext attacks            |
|               | • Using a non-certificate encryption scheme with Searchable Public Key using Multiple Keywords on Secure Channel free (SCF-MCLPEKS). |
| Ma et al. [14]  | • Security is based on the assumption of the difficulty in solving the Bilinear Diffie-Hellman Problems (BDHP). |
|               | • Using probabilistic eight polynomial-time algorithm.                         |
|               | • Claimed to have high efficiency in the computing process and low communication costs. |
2.3. Certificateless Public Key Authentication Schemes

In this section, the brief results of our literature review are presented. Four certificateless-based public key encryption schemes were compared. The four schemes are [10] [12] [13] [14]. To explain the difference between one scheme and another, an analysis of the certificateless public key encryption scheme is carried out. In this paper the algorithm compared is only a polynomial-time probabilistic algorithm, provided that it is the basic algorithm for a certificateless public key scheme that exists in the four studied schemes. Table 1 summarizes the characteristics of the four certificateless-based public key encryption schemes.

3. Results and Discussion

3.1 Design

In this section, the overview of the home monitoring system, devices requirement, flowchart diagram, and use case diagram are provided.

3.1.1 Overview of the system

This home monitoring system has a control panel, which is on the user's side, in the form of a multi-platform application. The control panel allows users to see events in the home environment, make an execution command, and get information. Users can do these things while doing their daily activities. This home monitoring system is a simple system with sensors and cameras that are integrated in such a way. The sensor works as a reader of environmental conditions, while the camera is an environmental watchdog. To save energy released, this system is made with the condition that the camera is not in the position of all-the-time recording. In this home monitoring system, for security, data will be encrypted before being sent by the sensor to the camera. When it arrives at the camera, the data is decrypted so that the camera can read it and then determine whether it remains idle or performs recording or shooting. However, if the sent data is not encrypted then the system will find it out and immediately turn itself off to prevent unauthorized people from seeing the home environment.

3.1.2 Devices Requirement

For implementing the CL-PKE scheme for home monitoring system, the following devices are required: wireless module of NodeMCU ESP8266, Passive infrared (PIR) sensor, Microcontroller board, and Web camera / CCTV / camera module as shown in Fig. 1.

![Fig.1 Required devices: (1) NodeMCU ESP8266 (2) Sensor of passive infrared (PIR) (3) Raspberry Pi 2 model B (4) Arduino Uno (5) Camera module](image)

3.1.3 Flow Diagram

The flow of our proposed monitoring security system is given in Fig. 2 (a) and the description is the following. The initial condition of the system is when the system gets electricity, all devices in the system that include the camera, microcontroller, wireless module, and PIR sensor, are active and in standby...
position. The microcontroller is connected to the camera wirelessly using a wireless module, which is connected to the PIR sensor. The PIR sensor in this system acts as a trigger maker for the camera to change its condition to active 'on' or standby. When the PIR sensor detects a movement, in this case in the form of analogue data, the analogue data is received by the wireless module. Then, the wireless module processes the received analogue data into a trigger for the camera. If the wireless module can read the analogue data then the data is considered as a value of "1" and this gives the camera a trigger to "ON", otherwise if it does not read any data it is assumed the value "0" and this gives a trigger for the camera "DO NOTHING".

The next process is to encrypt the trigger. Any triggers obtained will be encrypted and then sent to the microcontroller where the camera is connected to it. Next, the microcontroller decrypts the trigger to find out the contents whether to change the condition of the camera to be turned on or still on standby. If the microcontroller receives unencrypted data then the microcontroller automatically makes a notification and sends it to the wireless module, which will forward it to the user to inform that his home monitoring system is experiencing abnormal conditions. After the system has the trigger_Camera, the command obtained by the system will be encrypted so that if an interrupt occurs in this section, the attacker will not know the command the system has without making an attempt to decrypt the data packet.

![Flow diagram of the proposed system and (b) use case diagram](image)

After the system got the data from the trigger_Camera in the form of a statement to change the active condition which is then encrypted, then the data will flow to the next node, the microcontroller board. Before reaching the board, the system will check whether the data is encrypted or not. If it is not encrypted, the system will make a warning sent to the user who notifies the user that an error has occurred in the encryption process. If the data is encrypted then the data will flow to the board and then be decrypted to find out the contents of the statement which will then be sent to the camera. The camera will change the active condition according to the received statement. If it gets the statement "ON" then the camera will turn on, take a picture once, and do the recording. On the user side there will be a notification that the camera is active and he can see the situation around the house remotely.
3.1.4 Use Case Diagram

In this house monitoring system there are four entities i.e. users, camera, microcontroller, and wireless module, as depicted in Fig 2 (b). The proposed system has 9 use cases i.e. capture_image, encrypt, decrypt, live_view_video, login, logout, notification, turn_on, and turn_off. Each entity has different functions. Users can enter or exit the system (using login or logout use cases) and turn on or turn off the system, take_pictures, view_video, and view notifications from the system. The camera can take pictures or record videos. The microcontroller can perform the decryption function and make notification. The wireless module can send notification to users and perform encryption functions.

3.2 Theoretical Security Analysis

Security of the proposed system physically depends on the placement of the devices in it. It should be noted the location of the placement so as not to interfere with the system, especially the installation of cables or the installation of devices that require a wireless network. In the proposed house monitoring system, the biggest threat is related to electricity resources. If the main power source is off, the system does not work. To solve the problem, Uninterruptable Power Supply (UPS) can be used. Another threat is that an attacker can take over the system if the attacker gets the key pair value from the devices on the system. In addition, attackers can enter the system by doing social engineering to the homeowner. The attacker can also brute force attack or words list attack to get the user's account. This system can overcome the threat of vulnerability that commonly occurs in networks such as Denial of Service attack and Buffer Overflow attacks with encryption. The shortcomings of this system include the following. The system does not yet have a method or algorithm or protocol that can be applied to determine whether the data sent needs to be encrypted or not. This system also has not defined how to distribute keys between entities in the system. It is necessary to choose the right scheme to distribute the keys used to communicate to prevent Blackhole attacks.

4. Conclusion

In this study, a literature review has been carried out on several certificateless-based public key encryption schemes and the design of the application of the selected scheme has been conducted. The certificateless public key encryption scheme proposed by Guo et al. is chosen to be implemented in future work provided that it has the advantage that it is difficult for attackers to carry out attacks on this scheme. This is based on the difficulty of factoring prime numbers used in RSA algorithm, thus it can guarantee the confidentiality and integrity of information in an IoT scenario. Theoretically, the proposed system can overcome the threat of vulnerability that commonly occurs in networks such as Denial of Service attack and Buffer Overflow attacks. However, this system has not defined how to distribute keys between entities so that there is a possibility of Blackhole attack attacks. Future work of this study is to implement the proposed scheme based on the design conducted in this study, and also by adding security features.

5. References

[1] TechTarget. 2016. Networking and Communications: Internet of Things, (online, accessed on May 22, 2018), https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.
[2] A. Adriansyah and A. W. Dani, “Design of Small Smart Home System Based on Arduino,” Electrical Power, Electronics, Communications, Controls, and Informatics Seminar (EECCIS), 2014.
[3] M. Tellez, S. El-Tawab, and H.M. Heydari, “Improving The Security of Wireless Sensor Networks in an IoT Environmental Monitoring System,” IEEE Systems and Information Engineering Design Conference (SIEDS ’16), 2016.
[4] V. Goel, S. Srivastava, D. Pandit, D. Tripathi, and P. Goel, “Heart Rate Monitoring System Using Finger Tip through IOT,” International Research Journal of Engineering and Technology (IRJET), vol. 05, pp. 1114–1117, IRJET, 2018. (online accessed on August 02, 2018), https://www.irjet.net/archives/V5/i3/IRJET-V5I3254.pdf/.
[5] R. K. Kodali, V. Jain, S. Bose and L. Boppana, “IoT Based Smart Security and Home Automation System,” International Conference on Computing, Communication and Automation (ICCCA), 2016.

[6] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, “Access Control in IoT: Survey & State of The Art,” 2016 5th International Conference on Multimedia Computing and Systems (ICMCS). (online accessed on August 14, 2018), https://ieeexplore.ieee.org/document/7905662.

[7] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet of Things Journal, vol. 4, DOI 10.1109/JIOT.2017.2683200, 2017.

[8] A. B. Pawar and S. Ghumbre, “A Survey on IoT Applications Security Challenges and Counter Measures,” International Conference on Computing, Analytics and Security Trends (CAST), 2016.

[9] L. Yehia, A. Khedr, and A. Darwish, “Hybrid Security Techniques for Internet of Things Healthcare Applications,” Advances in Internet of Things, vol. 5, pp. 21-25, Scientific Research Publishing, 2015.

[10] R. Guo, Q. Wen, H. Shi, Z. Jin, and H. Zhang, “Certificateless Public Key Encryption Scheme with Hybrid Problems and Its Application to Internet of Things,” Research Article of Mathematical Problems in Engineering, vol. 2014, Article ID 980274, Hindawi Publishing Corp, 2014.

[11] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in Cryptology, vol. 196 of Lecture Notes in Computer Science, pp. 47–53, Springer, 1984.

[12] S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography,” in Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT’03), C.S. Laih, Ed., vol. 2894, Lecture Notes in Computer Science, pp.452–473, Springer, 2003.

[13] Viet Cuong Trinh, “Certificateless Public Key Encryption Made Practical,” 2017 4th NAFOSTED Conference on Information and Computer Science, IEEE 2017.

[14] M. Ma, D. He, N. Kumar, Kim-Kwang R. C., and J. Chen, “Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things,” IEEE Transaction on Industrial Informatics, 2016.