Device Protocol Design for Security on Internet of Things based Smart Home

https://doi.org/10.3991/ijoe.v14i07.7306

Trio Adiono(✉), Bryan Tandiawan, Syifaul Fuada
Institut Teknologi Bandung, Bandung City, West Java, Indonesia
tadiono@stei.itb.ac.id, tadiono@gmail.com

Abstract—One of the major challenges that arise in the internet of things (IoT) based smart home systems is security issue. It is still relatively low in which the exchange of data between devices can easily be stolen by outsiders since it is connected to the internet. In this work, we present the details of the protocol messages in smart home appliances that are encrypted by RSA algorithm and AES in which the RSA key was regenerated in every turnover of the day (exactly at 00:00:00 or 1 x 24 hours) since the last key generation by mobile. The performance test is done by sending an error command and a correct command to the RGB lamp device. The results show that the designed protocol works well as expected. Given the security mechanism in the designed protocol, data exchange between devices in the smart home will be hard to break by outsiders. Thus, the users can enjoy their smart home privacy without worrying the intruders (hacker).

Keywords—Internet of things, Privacy control, Secure protocols, Security, Smart home system

1 Introduction

The applications of an IoT at smart home systems are based on the convenience to access home appliances everywhere and anytime, not only limited to whether users are inside or outside of their home. The main problem that emerges in the smart home system is network security where all devices connected to the internet are very vulnerable to hacker attacks [1]. Hackers can break (illegitimately snoops) into the server and retrieve important information (*e.g.* home address, information about home devices, and damage the intelligent home system). A good security aspect and adequate comfort of an IoT based smart home are certainly important and extremely needed [2], it is legitimate to be implemented in order to allow a fully "privacy control" to the users [3-4]. In the other hand, an efficient mechanism for securing the home appliances connected to the internet is also concerned [5].

H. Suo *et al* summarize the security requirement in each layer that consists: application layer, support layer, network layer, and perceptual layer [6]. The application layer is related to the client's privacy protection that includes access control (password management and key agreement) and data authentication to

resilience against the attackers. In this work, we concentrate in an application layer, exactly in a secure data payload protocol design on the internet of things (IoT) based smart home devices for verifying the data communication in the home intelligent indoor system. It is employed as the only communication path among devices.

Compared to existing protocol for IoT which are *Message Queuing Telemetry Transport* (MQTT) and *Constrained Application Protocol* (CoAP), our proposed protocol has several advantages over those two protocols with several similar properties. In terms of advantage gathered from [7], several parameters are considered:

- **Communication Model**: similar as MQTT, our proposed protocol also has a highly decoupled publisher and subscriber model. While compared to CoAP, it only has an asynchronous communication model.
- **Packet Size**: Compared to MQTT & CoAP, the packet size of our proposed protocol offers more size for modifying the protocol format as we want.
- **Header**: Different with MQTT header that has 2 Bytes and CoAP header with 4 bytes, our protocol has 3 Bytes.
- **A number of Message Types**: While MQTT allows sixteen different types of messages and CoAP allows only four types, our protocol allows lots of message for any customization.
- **Security**: MQTT is un-encrypted yet, whereas CoAP works with Data Transport Layer Security (DTLS). Our protocol is fully flexible, with a double-verification as a foundation. In MQTT, the problems will arise in open networks because of there will be no information about how it is encoded. [8].
- **Quality of Service (QoS)**: Similar as MQTT, our protocol ensure three types of the QoS, which are: 1) At most once; 2) At least once; 3) Exactly once [9].

In Section II, we described briefly the smart home system that used in this work. The detailed scenarios of secure protocol message will be explained in Section III. Our smart home system allows anyone intercepting the messages cannot open as well as find the structure of the message with hard effort. The result and analysis is brought to Section IV.

2 Previous Research

In this work, we used the smart home full-system in which the block diagram is illustrated in Fig. 1 (the illustration is reproduced from T. Adiono, *et al.* [17]). The system consists of four elements: i) users, ii) cloud server and iii) access point as a home gateway, the last part is iii) home devices (nodes) that are coordinated by a host [10-11]. These devices communicate to each other via ZigBee® protocol and controlled by a Raspberry® host. There are three types of the developed devices that represent the common home appliances: *mechanical-based* (horizontal curtain, fan, and door lock), *electronic-based* (Red-Green-Blue lamp, generic switches, lamp switches, and temperature sensor monitoring) [12-13] and Infra-red based (television, air conditioner, LCD projectors) [14]. The users grant access to the home appliances

through an Android application, namely MINDS-app, in which this app is installed on the user's mobile phone [15-16]. It is the main tool that connects the users to the whole system. Whereas to control the IR-based devices, we incorporated the IR remote.

Our smart home system offers the benefit to the users, because we have equipped a dynamic key validation system which will be discussed detail in this paper. The security scenario consists of RSA algorithm, advanced encryption standard (AES), and also self-made protocol messages. This protocol can only be accessed after successful connection with the server, which is encrypted with RSA and AES method. The public key will change daily at every 00:00:00 or 1 x 24 hours. This complicated technique can realize the secure data exchange among devices that cannot be stolen easily by the outsiders. However, in this paper, we only study on designing a secure communication protocol between the devices in which the detailed scheme is presented in Section II. To ensure the designed protocol is working properly, we used our smart home miniature, namely meshed-internet networked system (MINDS®) as tester device (Fig. 2). Every nodes contained: XBee module, Microcontroller STM32L100 minimum kit, electronic drivers, power supply circuit, and LED or actuator (in form DC motor for fan, stepper motor for curtain, solenoid for door lock, relay for lamp switch) as a final part.

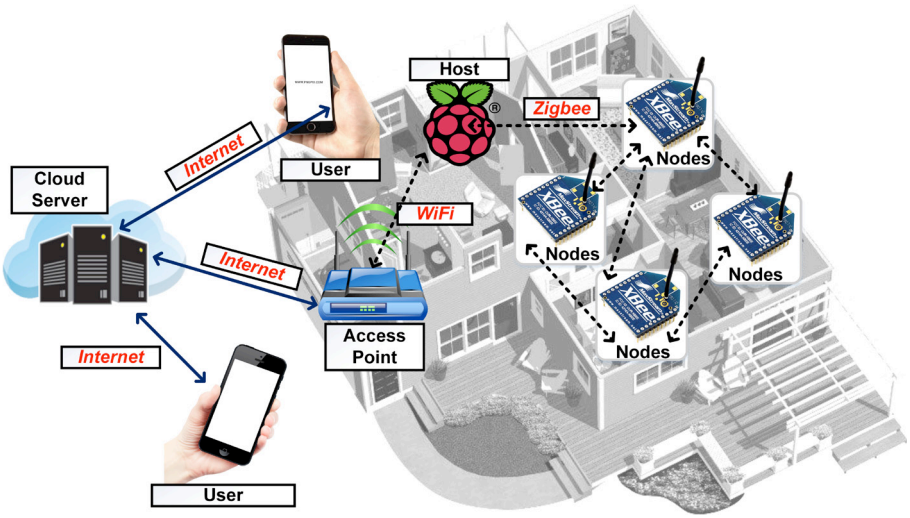

Fig. 1. Block diagram of developed smart home system

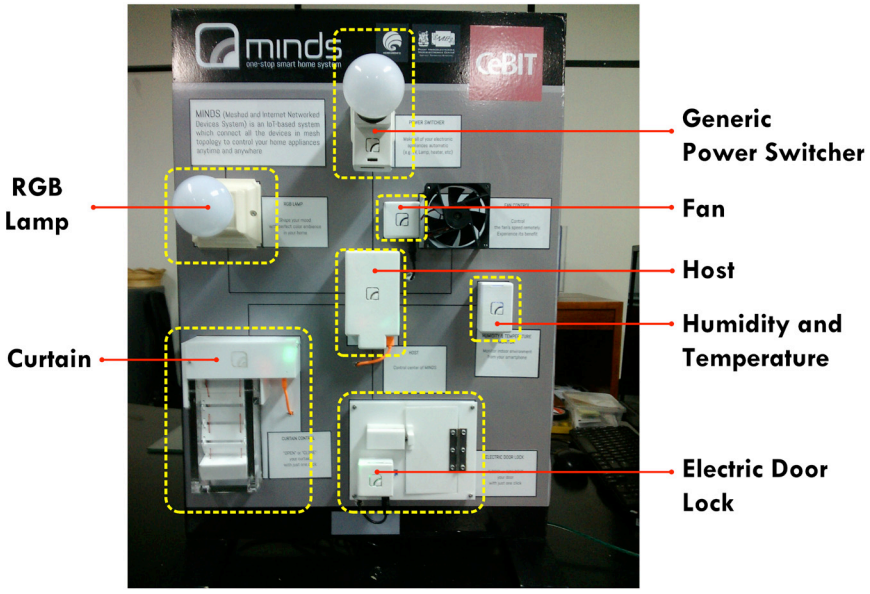

Fig. 2. A photograph of smart home panel: MINDS platform that consists of Raspberry® host packaged in the white box and six devices (nodes)

3 Methods

The security scenario of the communication is depicted in Fig. 3 Before connecting access to the home appliances that located in the indoor environment, the first step is the user should verify it by sending a message to the server in which the key is shifted periodically using RSA algorithm and AES. In other words, before the user sends a protocol messages, the communication between user and server have to pass the security verification. Thus, to control the smart home devices shouldn't be breached its procedures (e.g. bypassed directly from the host). The server as the only way that links the user to the host.

All communication processes are encrypted with AES standards, except when the user wants to "login" to the system in which the security of communication employing the combination of AES and RSA as appropriate with the efficient mechanism depicted in Fig. 3. In short description, the combination between RSA and AES are performed merely for the login (sign-in) process. When the user has successfully signed-in, the RSA is no longer needed and it will be processed straight-forward using AES only. But on the next day, the RSA keys will be activated automatically and so the user should request again in which the procedure is similar as the previous day. In this work, the RSA key will be updated once in a day (1 x 24 hours) and continuously consistent throughout the year.

The mechanism of communication encryption using RSA and AES has already been discussed in [18]. The technical chronology of the process as follows: 1) the server generates RSA public and private keys; 2) the client generates AES key when

intending to sign-in and sends requests; 3) the server sends public key; 4) the client forms sign-in message (containing AES key) encrypted using RSA; 5) the client sends sign-in message; 6) the server decrypts the message using private key; 7) the server send sign-in reply encrypted using AES; 8) the client receives the reply and the subsequent communications are encrypted using AES.

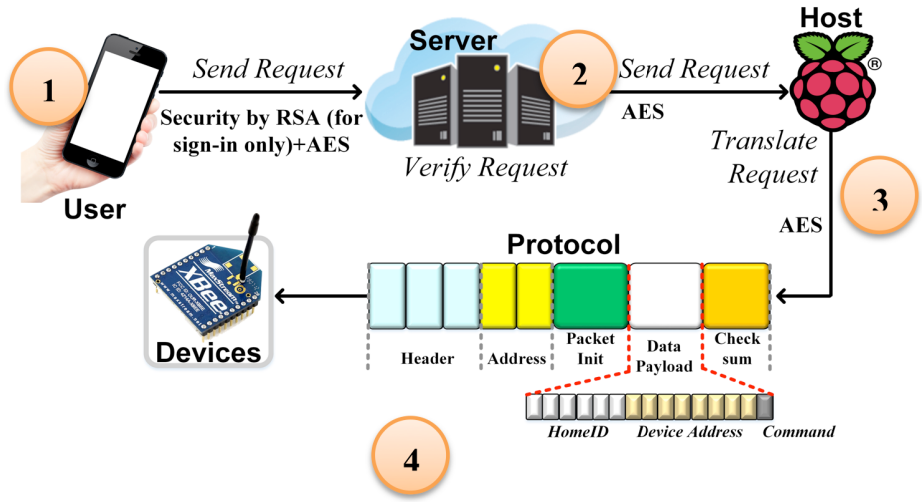

Fig. 3. Encrypted communication mechanism of sign-in process using RSA and AES

As an overview, the RSA itself is run by following step [19]:

a) Select two different prime numbers randomly, p and q, preferably is ($p \neq q$) because if $p = q$ then the value of n will be squared.
b) Calculate $n = p * q$
c) Calculate $\varphi = (p\text{-}1)*(q\text{-}1)$.
d) Select a public key e, where $1 < e < \varphi(n)$, $\gcd(e, \varphi(n)) = 1$
e) Generate a private key by using the equation $d = e^{-1} \bmod \varphi(n)$.
f) The results of the calculation are: public key = $[e, n]$, private key = $[d, n]$
g) For "encryption" use the equation below: $C = m_t^e \bmod n$, where m_t is a transmitted message and e is the key of the received message.
h) For "decryption" use the equation below: $m_r = C_d \bmod n$, where m_r is a received message and d is the key of the sent message.

As stated in Section II, we focus on the protocol design. They indicated in fourth step process of Fig. 3. We refer to the research on paper [20] where the data exchange protocol among devices used in our smart home system are shown in Table 1. In this work, we discuss on the *Data Payload* section due to its infinite capacity so that it can be applied as additional security system for smart home system. The *Data Payload* protocol proposed in this paper is shown in Table 2.

Table 1. Indoor smart home communication protocol

Header	Address	Packet Init	Data Payload	Check Sum
3 bytes	2 bytes	1 bytes	n bytes	1 byte

Table 2. Proposed of the data payload protocol

HomeID	Device Address	Command
6 bytes	8 bytes	n bytes

In this protocol, two verifications are required that a combination of *HomeID* and *Device Address* data before controlling the device. *HomeID* is a 6-bytes information which is a combination of numbers from 0-9 and is highly confidential and is known only to home owner. The selection of 6 bytes is due to fulfill great capacity for smart home users, covering up to 10^{48} houses. The *Device Address* is the 8 bytes information printed on the device in the form of QR code that has been encrypted using RSA algorithm and AES. These 8 bytes are selected because the production code for each item is 8 combinations of letters and numbers printed on Xbee module. These 14 bytes will then be merged and implemented as a verification system to perform device control. After the messages sent in accordance with this verification, the device will be ready to receive *Command* of *n* bytes (depending on device) which is the information in the form of control device desired by user.

Suppose a home has *HomeID* = XXXXXX, and *Device Address* RGB lamp = YYYYYYYY, whereas the main verification to be sent by the host will be XXXXXXYYYYYYYY. Afterward, the RGB lamp is ready to accept the control command and the host will send a color command which is the value of R, G and B. The *Delivery Command* with format of (0, 0, 255) sequentially, will produce a bright blue color on RGB lamp.

4 Results and Analysis

This protocol testing is done to the RGB lamp device in our smart home system and the flowchart is shown in Fig. 4. In the flowchart shown, it is to be noted that the conditional blocks of *Statereceive* == 6 and *Statereceive* == 14 is not implemented in the real code. Those blocks are put to help explain better of the flowchart system, which *Statereceive* == 6 means it is done reading and verifying *HomeID*; *Statereceive* == 14 means it is done reading and verifying *Device Address*, and is ready to read RGB values.

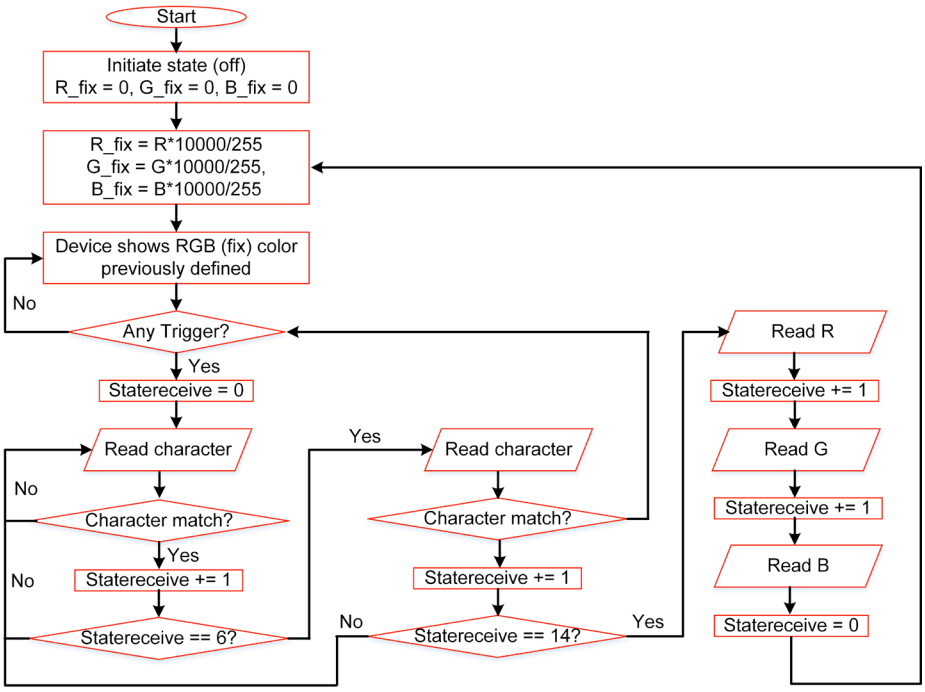

Fig. 4. Flowchart of how the RGB lamp works

(a) (b) (c)

Fig. 5. Functional test results: (a) RGB lamp does not turn on due to wrong protocol sent; (b) RGB lamp turns with blue colour with the Command = 0, 0, 255; (c) RGB lamp turns with red colour with the Command = 255, 0, 0. The test aims to ensure whether the system can perform well or not.

The sending of data is done by Raspberry® host and data is sent to each device for control on two scenarios. If the data sent does not confirm to the designed protocol, then the device will not perform the desired command as shown in Fig 5(a). If the correct command is sent, thus the RGB lamp device will respond as visualized in Fig. 5(b). In case of this functional test, we bypassed directly from the host to the nodes via designed protocol. It means, the security mechanism is not involved. In this implementation, the simply protocol used is sequence number, that is 123456 for

HomeID and then plus 40A88BB2 and plus the value of Red color (0-255) + value of Green color (0-255) + value of Blue color (0-255).

From Fig. 5(b) and Fig. 5(c), it can be seen that the RGB lamp works in accordance with the *Command* sent after passing the *HomeID* and *Device Address* verification. The RGB lamp controlled with data transmission of 12345640A88BB200255 (*HomeID* = 123456, *Device Address* = 40A88BB2, *Command* = RGB (0, 0, 255)). Whereas for red colour, the data transmission is 12345640A88BB225500 (*HomeID* = 123456 + *Device address* = 40A88BB2 + *Command* = RGB (255, 0, 0)).

5 Conclusion

We have carried out a security implementation on *Data Payload* protocol that includes initial verification of combination from the *HomeID* and *Device Address* data in which they are encrypted with RSA algorithm and AES. It is very important to ensure a secure communication among devices in smart home system, so it can serve the privacy control to the users. With this scheme, each device in the smart home has a different process and verification. Certainly, it will be able to make hard for outsiders to find out the data packets or even grabbing/breaking the transmitted information.

In the case of protocol security, it is expected to be more optimized again thus the number of bits employed is not too much. Certainly, it will take high power consumption of the system if the designed protocol has very long of bits. In addition, the payload data is recommended to be encrypted for a more secure smart home system. Furthermore, the updated simultaneously of RSA key in every hours of the day is also considered to be realized.

6 Acknowledgment

This research is one part of the big project entitled "*Perangkat Internet-of-Things untuk Sistem Rumah Cerdas*" that was supported by Decentralization scheme. This program is funded by the Ministry of Research, Technology and Higher Education of the Republic Indonesia (Kemenristekdikti) with Number of grant: 009/SP2H/LT/DRPM/IV/2017. We would like to grateful to our friends: Revie Marthensa, Maulana Yusuf Fathany, and Rahmat Muttaqin who help us indirectly.

7 References

[1] U. Saxena, J.S. Sodhi, and Y. Singh, "Analysis of Security Attacks in a Smart Home Networks," *Proc. of the 7th Int. Conf. on Cloud Computing, Data Science & Engineering – Confluence, January 2017,* https://doi.org/10.1109/CONFLUENCE.2017.7943189

[2] R.J. Robes and T-H. Kim, "A Review on Security in Smart Home Development," *Int. J. of Advanced Science and Technology,* Vol. 15, pp. 13-21, February 2010.

[3] V. Sivaraman, *et al.*, "Network-level security and privacy control for smart-home IoT devices," *Proc. of the 8th Int. Workshop on Selected Topics in Mobile and Wireless Computing,* pp. 163-167, 2015. https://doi.org/10.1109/WiMOB.2015.7347956
[4] M.A. Razzaq, *et al.,* "Security Issues in the Internet of Things (IoT): A Comprehensive Study," *Int. J. of Advanced Computer Science and Applications,* Vol. 8(6), pp. 383-388, 2017.
[5] R.M. Vrooman, "Enchancing Privacy in Smart Home Ecosystems using Cryptographic Primitives and a Decentralized Cloud Entity," M.Sc thesis in Delft University of Technology, Netherland, 2017.
[6] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *Proc. of the Int. Conf. on Computer Science and Electronics Engineering,* pp. 648-651, 2012. https://doi.org/10.1109/ICCSEE.2012.373
[7] Fastreamtech, "MQTT and CoAP: IoT Developers dilemma," [Online] Available at: https://www.faststreamtech.com/blog/mqtt-coap-iot-developers-dilemma/s
[8] M. Anusha, et al. "Performance Analysis of Data Protocols of Internet of Things: A Qualitative Review" *Int. J. of Pure and Applied Mathematics*, Vol. 115(6), pp. 37-47, 2017.
[9] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," *Proc. of IEEE Int. Syst. Engineering Symp.,* pp. 1-7, October 2017. https://doi.org/10.1109/SysEng.2017.8088251
[10] T. Adiono, R.V.W. Putra, M.Y. Fathany, B.L. Lawu, K. Afifah, M.H. Santriaji, S. Fuada, "Rapid prototyping methodology of lightweight electronic drivers for smart home appliances," *Int. J. of Electrical and Computer Engineering* (IJECE), Vol. 6(5), October 2016.
[11] T. Adiono, R.V.W. Putra, M.Y. Fathany, W. Adijarto, "Design of Smart Home System based on Mesh Topology and Efficient Wireless Sensor Network Protocol," *J. Informatika, Sistem Kendali dan Komputer (INKOM)*, Vol. 9(2), pp. 65-72, November 2015.
[12] T. Adiono, R.V.W. Putra, M.Y. Fathany, K. Afifah, M.H. Santriaji, B.L. Lawu, S. Fuada, "Prototyping design of electronic end-devices for smart home applications," *Proc. of The IEEE Region 10 Symposium (TENSYMP)*, pp. 261-265, July 2016. https://doi.org/10.1109/TENCONSpring.2016.7519415
[13] B.L. Lawu, M.Y. Fathany, K. Afifah, M.H. Santriaji, R.V.W. Putra, S. Fuada, T. Adiono, "Prototyping design of mechanical based end-devices for smart home applications," *Proc. of 2016 4th Int. Conf. on Information and Communication Technology (ICoICT)*, September 2016. https://doi.org/10.1109/ICoICT.2016.7571927
[14] T. Adiono, B. Tandiawan, M.Y. Fathany, W. Adijarto, and S. Fuada, "Prototyping Design of IR Remote Controller for Smart Home Applications," *Proc. of IEEE Region 10 Conf.* (TENCON), pp. 1304-1308, November 2017. https://doi.org/10.1109/TENCON.2017.8228059
[15] K. Afifah, S. Fuada, R.V.W. Putra, T. Adiono, M.Y. Fathany, "Design of Low Power Mobile Application for Smart Home," *Proc. of Int. Symposium on Electronics and Smart Devices* (ISESD), pp. 127-131, November 2016. https://doi.org/10.1109/ISESD.2016.7886705
[16] T. Adiono, S.F. Anindya S. Fuada, K. Afifah, I.G. Purwanda, "Efficient Android Software Development using MIT App Inventor 2 for Bluetooth-based Smart Home," *Unpublished.*
[17] T. Adiono, M.Y. Fathany, R.V.W. Putra, K. Afifah, M.H. Santriaji, B.L. Lawu, S. Fuada, "Live Demonstration: MINDS-Meshed and Internet Networked Devices System for Smart Home," *Proc. of the 13th IEEE Asia Pacific Conference on Circuits and Systems* (APCCAS), pp. 736-737, October 2016. https://doi.org/10.1109/APCCAS.2016.7804031
[18] T. Adiono, R. Marthensa, R. Muttaqin, S. Fuada, S. Harimurti, and W. Adijarto, "Design of database and secure communication protocols for internet-of-things-based smart home

system," *Proc. of IEEE Region 10 Conf.* (TENCON), pp. 1273-1278, November 2017. https://doi.org/10.1109/TENCON.2017.8228053

[19] S. Fuada, "Kajian Aspek *Security* Pada Jaringan Informasi dan Komunikasi Berbasis Visible Light Communication," *J. Informatika – Telekomunikasi – Elektronika* (INFOTEL), Vol. 9(1), pp. 108 – 121, February 2017. https://doi.org/10.20895/infotel.v9i1.163

[20] M.Y. Fathany, T. Adiono, "Wireless protocol design for smart home on mesh wireless sensor network," *Proc. of Int. Symp. On Intelligent Signal Processing and Communication Systems*, pp.462-467, November 2015. https://doi.org/10.1109/ISPACS.2015.7432816

8 Authors

Assoc. Prof. Trio Adiono, Ph.D received a B.Eng. in electrical engineering and an M.Eng. in microelectronics from Institut Teknologi Bandung, Indonesia, in 1994 and 1996, respectively. He obtained his Ph.D. in VLSI Design from the Tokyo Institute of Technology, Japan, in 2002. He holds a Japanese Patent on a High Quality Video Compression System. He is now a lecturer at the School of Electrical Engineering and Informatics, and also serves as the Head of the Microelectronics Center, Institut Teknologi Bandung. His research interests include VLSI design, signal and image processing, VLC, smart cards, and electronics solution design and integration (Address: Gd. Pusat Antar Universitas (PAU), Lt. IV, Integrated Circuit design laboratory, ITB Campus, Jln. Tamansari No. 126, Bandung City (40132) West Java, Indonesia.

Bryan Tandiawan is with the School of Electrical Engineering and Informatics, Institut Teknologi Bandung. He was born on 9th July 1995 in Medan, Indonesia. He received the B.Eng. degree (with honors) in electrical and electronic engineering from Bandung Institute of Technology, Bandung, Indonesia, in 2017.His research interests cover the area business, technology, engineering, Internet of Things, especially smart home system and security system. Currently, he is a Product Manager Associate in a well-known e-commerce in Indonesia, Blibli.com.

Syifaul Fuada received a B.Ed. in Electrical Engineering Education from Universitas Negeri Malang (UM), Indonesia, in 2014/2015 and an M.Sc. in Microelectronics Engineering from the School of Electrical Engineering and Informatics, Institut Teknologi Bandung (ITB), Indonesia, in 2016/2017. Now, he is with the University Center of Excellence at Microelectronics ITB. He has several achievements, such as receiving one of the 106 Indonesia Innovation by BIC-RISTEK DIKTI awards in 2014, a top of 10–student travel grant to the IEEE Asia Pacific Conference and Systems (APCCAS) 2016 that was held in Jeju, South Korea, and receiving one of 108 Indonesia Innovation by BIC-LIPI awards in 2016. He is a member of IAENG and an associate editor of Jurnal INFOTEL. His research interests include analog circuit design, circuit simulation, VLSI design, DSP, engineering education, multimedia learning development and VLC.

Article submitted 16 June 2017. Resubmitted 05 November 2017 and 13 April 2018. Final acceptance 13 April 2018. Final version published as submitted by the authors.