Secure Data Exchange in Environmental Health Monitoring System through Wireless Sensor Network

Amang Sudarsono[1,*], Samsul Huda[3], Nurul Fahmi[3], M. Udin Harun Al-Rasyid[2], and Prima Kristalina[1]

[1]Department of Electrical Engineering, Electronic Engineering Polytechnic Institute of Surabaya, Indonesia.
[2]Department of Informatics and Computer Engineering, Electronic Engineering Polytechnic Institute of Surabaya, Indonesia.
[3]Graduate School of Informatics and Computer Engineering, Electronic Engineering Polytechnic Institute of Surabaya, Indonesia.

Received 26 January 2016; received in revised form 15 March 2016; accepted 15 March 2016

Abstract

Recently, disseminating latest sensory information regarding the status of environmental health in the surroundings of human life is one of very important circumstances which must be known by everyone. These circumstances should be accessible at anytime and anywhere by everyone through any type of end-user devices, both fixed and mobile devices, i.e., Desktop PCs, Laptop PCs, and Smartphones. Wireless Sensor Network (WSN) is one of the networks which deals with data sensors distribution from sensor nodes to the gateway node toward a Data Center Server. However, there is a big possibility for many adversaries to intercept and even manipulate data sensors crossing the network. Hence, a secure data sensor exchange in the system would be strongly desirable. In this research, we propose an environmental health conditions monitoring system through WSN and its implementation with considering secure data sensor exchange within the network and secure data sensor access. This work may contribute to support a part of smart cities and take in part the Internet of Thing (IoT) technology. In our proposed system, we collect some environmental health information such as temperature, humidity, luminosity, noise, carbon monoxide (CO) and carbon dioxide (CO_2) from sensor nodes. We keep the confidentiality and integrity of transmitted data sensors propagating through IEEE802.15.4-based communication toward a gateway node. Further, the collected data sensors in the gateway are synchronized to the Data Center Server through a secure TCP/IP connection for permanently storing. At anytime and anywhere, only legitimated users who successfully pass-through an attribute-based authentication system are able to access the data sensors.

Keywords: WSN, Internet of Thing, data sensor confidentiality and integrity, and attribute-based authentication

1. Introduction

For the past decade, Wireless Sensor Networks (WSNs) have become popular in the context awareness development for distributing very important information to everyone at anytime and anywhere. Because of its feature, in addition, increasingly it is becoming common issues and taking in a part of the Internet of Thing (IoT). Naturally, a sensor node in a WSN is simply formed as a small device that raises an electrical signal containing a particular data sensor and usually possesses limited resources such as low speed processor, small size memory and storage, low cost, and low performance. In most cases, the main goal of WSN development is to transmit and disseminate data sensors which refer to particular information should be known by everyone, especially a very critical information.

[*] Corresponding author. E-mail address: amang@pens.ac.id
Tel.: +62-31-5947280; Fax: +62-31-5946114

Due to the flexibility of WSN in term of its implementation, it may overwhelm a wide range of area and support a variety of applications such as disaster warning, medical, military, agricultural, forest fire, and other environmental monitoring [1, 18]. There also a real time system of monitoring environment circumstances in term of temperature, humidity, light intensity, soil components, etc. has been researched [2]. Another important monitoring system of our environment is gases monitoring [3, 5, 9], such as Carbon Monoxide (CO), Carbon Dioxide (CO_2), and Methane (CH_4), etc. By utilizing Arduino micro-controller system and ZigBee radio communication module, [3] introduced an environmental monitoring of greenhouse gases and visualized continuously the results in real time through a web-based application. Another system for monitoring atmospheric pollutants also has been researched to collect several types of atmosphere gases such as sulfur dioxide (SO_2), nitrogen dioxide (NO_2), suspended particulates (PM), CO, and ozone (O_3) as well as health-care spheres, disaster warning, location-based detection in military, parking-lot [5, 18], and the implementation of WSN for Wireless Body Area Network (WBAN) in human body monitoring [4, 8]. Currently, distributing latest information regarding to the status of environmental health in the surroundings of human life is one of very important circumstances which must be known by everyone at anytime and anywhere. WSNs deal with data sensors distributions from sensor nodes to the gateway node toward a Data Center Server.

In considering that the advantages of WSN in various applications and providing sensory information which generally carries very critical information, it has to be able to distribute data sensors to everyone. These data sensors usually are freely transmitted over wireless media transmission both in attended and un-attended environment. Moreover, to provide more sensory information distribution, sensor networks are essentially connected to the user networks through common use networks, such as Internet or any other public network connection. Hence, everyone is able to access the information easily. However, there is a big possibility for provoking many potential threats and attacks because naturally sensor networks are easily to be intercepted, eavesdropped, injected with unexpected information, and even altered into faked information by adversaries. Therefore, particular security mechanism is required to prevent such threats and attacks by concerning to the natural property of sensor nodes in WSN e.g., low power, low performance, low processor speed, limited memory and storage size. On the other hand, there is another possibility for illegally access, modification, and retransmission altered sensory information as well when data sensors are exchanged over the Internet and any other public connection by many sensory information based Service Providers in order to disseminate very important information to everyone as broadest as possible. Thus, a security system to overcome such illegally misuses is also desirable.

Currently, many researchers have taken in account the suitable security methods and systems in their WSN related researches with consideration to sensor nodes' constraint, i.e., by utilizing modern cryptographic algorithms both symmetric and asymmetric cryptosystems [13-14]. Generally, in wireless networks e.g., WSN, some security requirements should be fulfilled such as confidentiality, data integrity, availability, authentication and privacy [6, 18]. Confidentiality makes sure data sensors are transmitted in ciphertext when crossing the networks. Data integrity verifies and guarantees the originality of data sensors when propagating the networks and preventing the modification of transmitting data sensors. Availability keeps and maintains sensory information accessible by legitimated sensor nodes and users within the networks. Meanwhile, authentication permits only authenticated sensor nodes to exchange and disseminate data sensors within the networks, and privacy protects data sensors from the exposure of unauthorized sensor nodes or any other unauthorized entity. There has been proposed a secure protocols in WSN which deal with confidentiality, data integrity, and authentication based on the security library in WSN [18] for e-healthcare system [8]. The system utilized slightly complex combination between symmetric (i.e., AES 256-bit), asymmetric (i.e., RSA 1024-bit), and hash function (i.e., SHA 256-bit) cryptographic algorithms. However, the cost of computation cryptographic algorithms in [8] is slightly heavy. An implementation of symmetric cryptography for environmental health monitoring system [9] based on [18] is introduced with confidentiality and data integrity security requirement satisfaction.

The system also deals with sensor nodes' limitation because it provides a very light computation cryptographic algorithm. However, symmetric key has to be changed either periodically or incidentally to prevent the fragility of the system. Moreover, there is also much more various implementation, mechanisms, and scenarios of WSN w.r.t security requirements (i.e., authentication, confidentiality, and data integrity) using modern cryptographic algorithms, such as AES, RSA, MD5 and SHA algorithms presented and provided by Libelium technologies [18].

Secure data sensor transmission over the wireless networks in natural WSN is very important, but when data sensor is exchanged in the Internet or any other public connection, it also has to be considered its security. Data sensor is the core data in the sensory information systems and services stored in the data center server so that it is needed a restrictions on the right of data sensors access only for authorized users or entities. Recently, a technique to exchange data securely in the data center server such as Secure Electronic Medical Record system based on cloud computing using Elliptic Curve Cryptography (ECC) algorithm to encrypt data in the data center has been proposed [19]. Another proposed secure data access mechanism based on identity-based encryption and biometric authentication for cloud tenants [20] also has been proposed. However, the existing security systems are still based on user personal data authentication, such as a user account i.e., username and password or some other personal data. Cipher-based Policy Attribute Based Encryption (CP-ABE) [10] is one of the techniques that provide features to protect user's personal data by endowing insensitive user attributes as user identity. In CP-ABE, access policy is embedded on the ciphertext. Any user is able to decrypt the ciphertext if and only if his/her attributes match with access policy. Whereas, the access policy is determined in advanced by the manager for controlling user access to the system. CP-ABE is appropriate for most applications, such as data exchange over wireless medium [22] and secure content exchange in Delay Tolerant Networks (DTNs) [12], etc. To enable secure access and data sharing in an environmental health data center, we have presented a secure data sensor sharing using CP-ABE with introducing two protocols: registration and data sharing protocol, and various rules access policy for each sensor groups to ensure confidentiality, integrity, and user privacy aspects [11].

In this paper, we propose a secure data exchange in environmental health conditions monitoring system through WSN. In this work, we collect data sensors in term of temperature, humidity, luminosity, noise, CO and CO_2 from sensor nodes securely. We encrypt data sensors and propagate the encrypted data sensors through IEEE802.15.4-based communication toward a gateway for temporary storing. Here, we adopted a suitable symmetric encryption [9] to ensure the confidentiality and integrity of the data sensors from sensor nodes to the gateway. In addition, periodically and incidentally, we changed the symmetric key by distributing the new key to all sensor nodes through a key renewal mechanism. Key renewal mechanism is able to guarantee the freshness of symmetric key used in the secure data sensors transmission. Further, the encrypted data sensors in the gateway are synchronized to the Data Center Server through TCP/IP connection or other connections for permanently storing. Here, to ensure the security of data sensors, we synchronized data sensors between the gateway and Data Center Server through a secure channel over the TCP/IP connection, i.e., Internet or Local Area Networks (LANs). At anytime and anywhere, all legitimated users are able to access the data sensors through web-based and/or mobile applications from their end devices. In this case, we adopted our previous system [11] with slightly modification by omitting the role of manager for attributed based user authentication. Here, we embedded the set of user's attributes in his/her secret key when user joins to the system. On the other hand, collected data sensors in the Data Center Server are attribute-based encrypted w.r.t access policy which is defined in the Data Center Server and only if the users who have match possessed attributes with access policy are able to decrypt the encrypted data sensors.

The rest of this paper is organized as follows. In Section 2, we describe the common secure communication system in the WSN. Later on in Section 3, we explain our security requirements of proposed system. Then, we explain our adopted cryptographic primitives to construct security functions in our proposed system in Section 4. Furthermore, in detail, we explain our proposed secure environmental health monitoring system, its implementation and experimental measurements in Section 5 and Section 6, respectively. And finally, we express our conclusion and future works in Section 7.

2. Secure Communication System in WSN

Commonly, secure communication system in WSN should recover security in all tiers. Regarding the multi-tier architecture [7], there are three tiers in the architecture of WSN: base tier, interface tier, and highest tier as shown in Fig. 1. The basic tier comprises sensor nodes that usually transmit a set of particular data sensors such as temperature, noise level, luminosity, CO, CO_2, humidity, etc. The interface tier consists of the gateway or master or coordinator node which bridges sensor nodes and application/monitoring server. The gateway node has a responsibility to fetch all data sensors from all sensor nodes in its coverage area and forward to the application/monitoring server. The gateway may store data sensors either temporary or permanently depending on the size of its storage. Usually, a gateway node has a small size storage, thus the data sensors are stored temporary before forwarding to the application server. To carry out its functionalities, a gateway usually is equipped with several network interfaces such as IEEE 802.15.4 or ZigBee, WiFi, Ethernet, GPRS, 3G or 4G interfaces, or other interfaces to hook data sensors toward application server. Meanwhile, the highest tier consists of application server which stores permanently data sensors into database. This tier has a responsibility to provide data sensors to all users through any public connection such as Internet. However, the highest tier could be either low-end devices, i.e., smartphones or high-end devices, i.e., high performance servers which have connection to the public networks such as Internet. Thus, everyone is able to access sensory information at anytime and anywhere using their end devices (i.e., Desktop PCs, Laptop PCs, and Smartphones) through web-based and/or mobile applications.

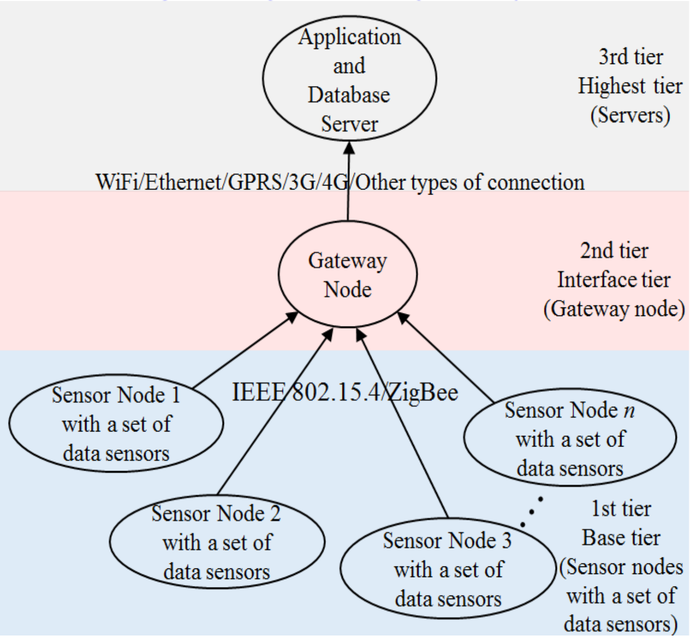
Application and Database Server
3rd tier
Highest tier
(Servers)
WiFi/Ethernet/GPRS/3G/4G/Other types of connection
Gateway Node
2nd tier
Interface tier
(Gateway node)
IEEE 802.15.4/ZigBee
Sensor Node 1 with a set of data sensors
Sensor Node n with a set of data sensors
Sensor Node 2 with a set of data sensors
Sensor Node 3 with a set of data sensors
1st tier
Base tier
(Sensor nodes with a set of data sensors)

Fig. 1 Multi-tier architecture in the WSN [7]

2.1. Secure Communication Layers

To obtain a perfect design of secure communication in the WSN, we have to consider the multi-tier architecture in WSN. The secure communication should be applied in the 1st tier, 2nd tier and 3rd tier. In the 1st tier, secure communication between sensor nodes and gateway node through IEEE 802.15.4 or ZigBee connection should be realized to transmit data sensors from sensor nodes to the gateway securely. In the 2nd tier, data sensors are forwarded to the server through TCP/IP connection or other connections. Hence, a secure connection should be applied to ensure the validity of the data sensors. Then, secure data access to all legitimated users in the 3rd tier should be applied as well as 1st and 2nd tiers. Based on [18], there are several mandatory security layers to protect sensory information in the WSN: confidentiality/encryption, authentication, HTTPS and SSH connection.

2.1.1. Confidentiality/Encryption

The first security layer in the WSN is confidentiality or encryption and generally used in the 1st tier. This requirement ensures that only the participating sensor nodes in the system who have a valid shared-key are able to encrypt the data sensor and transmit the encrypted data sensor to other sensor nodes or gateway node. On the other hand, only participating sensor nodes who have a valid shared-key are able to decrypt and recover the encrypted data sensors. Let assume that pre-shared-key is distributed in advanced to all participating nodes when the system is set up for the first time. By embedding pre-shared-key in the encryption algorithm or storing it in the sensor nodes' memory, sensor nodes which equipped with IEEE 802.15.4 or ZigBee radio device encrypt data sensor and transmit it either unicastly or broadcastly to other sensor nodes or gateway node. The common symmetric cryptography used in this scenario is AES 128-bit.

2.1.2. Authentication

Authentication is the second security layer that makes sure point-to-point encryption between participating nodes in the 1st tier and/or gateway node. Based on [18], standard public key cryptography RSA 1024-bit is utilized to permit authenticated sensor nodes transmitting and receiving data sensors within the network. When a sensor node or gateway node authenticates another sensor node, other sensor nodes are not able to intercept the data sensor exchange between the authenticating sensor nodes. To do so, in advanced let assume a sensor node transmit data sensor with authentication to the gateway, sensor node's secret key Sk_{N} and public key Pk_{N}, and gateway's secret key Sk_{G} and public key Pk_{G}. Before transmitting data sensor M to the gateway, sensor node generates a signature by using its secret key Sk_{N}, $S_{\mathrm{N}} = Sign_{\mathrm{RSA}}(M, Sk_{\mathrm{N}})$ and encrypts M using gateway public key Pk_{G}, $C = E_{\mathrm{RSA}}(M, Pk_{\mathrm{G}})$. Whereas S_{N}, $Sign_{\mathrm{RSA}}$, C, and E_{RSA} denote signature, RSA-based signature generation algorithm, ciphertext, and RSA-based encryption algorithm, respectively. Then, ciphertext C is transmitted to the gateway along with signature S_{N}. Upon receiving C and S_{N} from sensor node, the gateway decrypts ciphertext C using its secret key Sk_{G}, $M' = D_{\mathrm{RSA}}(C, Sk_{\mathrm{G}})$ and verifies the signature S_{N} by using sensor node's public key Pk_{N}, $v = Verify_{\mathrm{RSA}}(M', S_{\mathrm{N}}, Pk_{\mathrm{N}})$. The authentication is valid if and only if v is true, otherwise the authentication is invalid. Here, the gateway ensures that the data sensor is truly transmitted from legitimated sensor node, not from the other sensor nodes or adversaries. In this case, to encrypt data sensor, a standard symmetric cryptography algorithm AES 256-bit can be adopted, whereas in advance the gateway distributes pre-shared-key to the sensor node. However, allowing the use of same symmetric key for many times encryption process will open a big possibility to compromise the symmetric key, thus it decreases security level. To overcome the problem, symmetric key should be kept its freshness through key renewal mechanism either periodically or incidentally.

2.1.3. HTTPS and SSH Connection

The third security layer is HTTPS and SSH connection to protect the data sensors from illegally access when data sensors are exchange in the external networks of WSN, i.e., Internet. For example, when data sensors provided by Data Center Server in the 3rd tier of WSN architecture are distributed to everyone over the Internet or any other public connection, HTTPS and SSH connection could be one of solutions. Of course, there is another possibility to establish a confidential connection to the external networks by using public key for protecting data sensors during transmission.

2.2. Secure Data Sensor Exchange and Synchronization

According [18], there are two key points of security in securing data sensor exchange. The first point is when data sensor crosses the link layer; it is encapsulated by security header using AES 128-bit. To enable this link layer security, it is needed a configuration in the radio device. The encryption key of AES 128-bit is embedded in the radio hardware. Hence, only the sensor nodes that configured with the same encryption key are able to transmit successfully encrypted data sensors to the gateway or other sensor nodes and decrypt successfully the encrypted data sensors. The second key point is the use of AES 256-bit to encrypt data sensor in the application layer through an executing software in the sensor nodes such that encrypted data sensor can be transmitted point-to-point from sender node to destination node. On the other hand, the destination node successfully decrypts the encrypted data sensor received from sender node as long as the encryption key used for encryption by the sender node is the same as encryption key used for decryption by the destination node. Another important point of security in exchanging data sensors is data sensor synchronization. Data sensor synchronization is happened when exchanging data sensors from the gateway with equipped small size storage to the Data Center Server. Here, a secure connection between the gateway and Data Center Server is strongly desirable such as by utilizing Secure Socket Layer (SSL)/Transport Layer Security (TLS) which generally employing public key cryptography to establish a confidential connection and protect data sensors during transmission.

2.3. Key Renewal

The use of encryption key between two parties (i.e., sensor node and gateway) in AES 128-bit or 256-bit encryption algorithm for encrypting data sensor both in the link layer security header and application layer through a software running in each communicating sensor node should be kept its freshness. Firstly, encryption key distribution is done from the gateway to sensor nodes for ensuring the identically encryption key for encryption and decryption process. To ensure the freshness of the encryption key, periodically gateway has to renew the encryption key and redistribute the new key to the sensor nodes. The process of key renewal cyclically is performed by gateway using standard public key cryptography algorithm RSA 1024-bit or simply by utilizing symmetric key encryption algorithm, such as AES 128-bit or 256-bit. Another recommendation based on [18] in making sure the freshness of key renewal transmission, seed could be generated randomly and put it together with the new key during key renewal transmission process.

3. Security Requirements in WSN

Essentially, participating nodes in the WSN are fixed and/or randomly or frequently mobile, or even running out of the battery during sending, storing, and receiving data sensor over wireless connection which usually has unstable connectivity characteristic. Meanwhile, any sensor nodes including faked sensor nodes and adversaries have a big possibility to join the network freely and without getting permission from the network administrator. Hence, at anytime the adversaries illegally intercept sensory information crossing the network, transmit bad data sensor or even modify the original data sensors and retransmit them to other sensor nodes within the network. Another possibility for adversaries to illegally access and misuse data sensors from Data Center Server within the Internet or public connection. Based on [18] and our previous works [8-9][11], we define security requirements in our proposed system as follows:

3.1 Confidentiality

This security requirement ensures that no sensor node is able to receive the original data sensors, except the sensor nodes that have a valid encryption key to decrypt the encrypted data sensors when data sensors exchanging within wireless network. In case illegally access and misuse data sensors from Data Center Server within the Internet, the confidentiality ensures no users is able to access the original data sensors, except the users whose have a set of possessed attributes match with access policy of attributes to decrypt the encrypted data sensors.

3.2 Data Integrity

This security requirement ensures that no sensor node is able to alter the original data sensors and guarantees that received data sensors are kept originality during their transmission over wireless network. To do so, receiving sensor node verifies the received data sensors digest. If the verification is valid means that received data sensors are kept the originality and no alternation during transmission.

3.3 Authentication

This security requirement ensures only authorized gateway node is able to forward and synchronize data sensors to the Data Center Server through the Ethernet, WiFi, GPRS, 3G, 4G, or any other type of connections, and only authorized users are able to access data sensors provided by Data Center Server over the Internet or any other public connection.

4. Adopted Cryptographic Primitives

As well as our previous systems [8-9, 11], we utilize symmetric encryption algorithm AES 128-bit and hash function MD5 to satisfy confidentiality and data integrity, respectively. AES 128-bit is used for encrypting data sensors both in link layer header and application layer when data sensors transmitted over IEEE 802.15.4 connection. To check the integrity and originality of the received data sensors, MD5 is utilized to verify the validity of the data sensors. Meanwhile, Ciphertext Policy Attribute-Based Encryption (CP-ABE) scheme [10] is adopted as well as our previous system [11] which utilized CP-ABE as well to fit the security in the data sensors access from Data Center Server over the Internet or any other public connection.

4.1 Symmetric Encryption and Data Sensor Integrity

As well as our previous system [9], for the fastness of encryption and data sensors integrity with considering to the limitation of sensor nodes, we encrypt several types of data sensors which consists of temperature, humidity, noise level, luminosity, CO, CO_2, and accelerometer using AES 128-bit. Then, we transmit the encrypted data sensors along with MD5 data sensors digest. Upon receiving encrypted data sensors and its digest, the gateway extracts the original data sensors by decrypting the encrypted data sensors and compares the extracted original data sensors digest and the received data sensors digest. Data sensors are said valid if only if the result of comparison is exactly equals.

4.2 Attribute-Based Encryption Scheme

Let assume a message *M* in CP-ABE. To create a. encrypted message in CP-ABE, *M* is encrypted using public key and a set of access policy of attributes. Generally, access policy of attributes is determined to restrict the user access to the system. The access policy of attributes comprises a rule which expressed by a logical relation on attributes. Each user who registered in the system has a set of attributes possession, whereas this set of attributes is embedded initially into the secret key assigned to the user when registering him/her self to the trusted authority, called Key Generator Server (KGS). Later on, the secret key is used for decrypting the encrypted *M*. The decryption process returns the valid *M* or not depending on whether the set of user's attributes embedded in his/her secret key is matching with the access policy of attributes used in the encryption or not. In this case, if the users who have a set of attributes possession matches with access policy of attributes are able to successfully decrypt and recover the original message *M*.

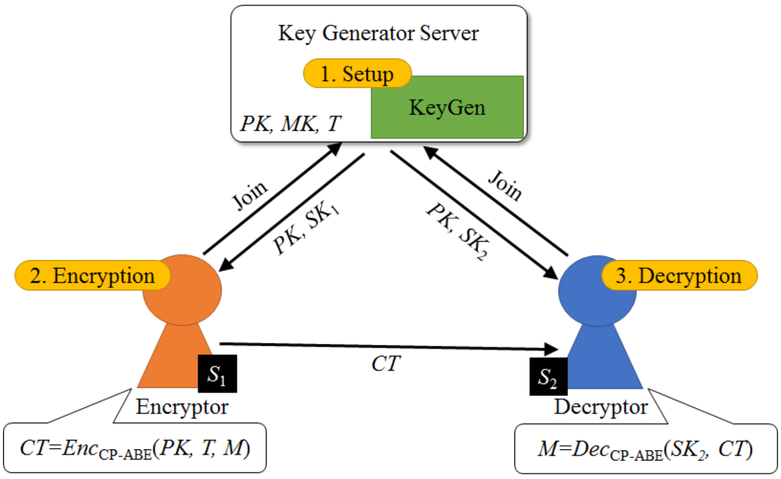

Fig. 2 Players and algorithms involved in CP-ABE scheme

In the CP-ABE scheme, basically there are three players: Key Generator Server (KGS), Encryptor, and Decryptor, and four algorithms: Setup, Encryption, KeyGen, and Decryption as shown in Fig. 2.

(a) **Setup**: KGS executes this algorithm to randomly generate public key parameters *PK* and a master key *MK* using a security parameter. Later on, *PK* is used for encrypting data sensors and recover encrypted data sensors into original data sensors. To do so, *PK* is distributed to all users in the joining/registration phase. Meanwhile, *MK* is used for creating users' secret keys. In the joining phase, a user endows his/her set of attributes possession S_i to KGS. Then, by using *MK*, KGS embeds S_i into his/her secret key SK_i. Together with *PK* and access policy of attributes *T*, KGS sends the joining user his/her secret key SK_i.

(b) **Encryption**: Let assume a data sensor *M*, access policy of attributes *T* obtained from KGS, and public key *PK* obtained from KGS in the Setup algorithm. All participating users in the system are able to encrypt *M* based on access policy of attributes *T* into a ciphertext *CT*, $CT = Enc_{\text{CP-ABE}}(PK, T, M)$, where $Enc_{\text{CP-ABE}}$ denotes CP-ABE based encryption algorithm.

(c) **KeyGen**: KeyGen stands for Key Generation. KGS executes this algorithm to randomly generate the users' secret keys SK_i on given a set of user-*i* (e.g., user-1, user-2, etc.) and master key *MK*. Here, the created SK_i is associated with S_i. Again, this algorithm is performed by KGS in the joining phase together with Setup algorithm.

(d) **Decryption**: All participating users in the system are able to act as decryptor user and execute this algorithm. On given *CT* from encryptor user and user-*i* secret key SK_i which associated to his/her set of attributes possession S_i. User-*i* successfully decrypts *CT* and recovers message *M*, if and only if his/her S_i embedded in the SK_i has matching rule with access policy of attribute *T* associated to the ciphertext *CT*, $M = Dec_{\text{CP-ABE}}(SK_i, CT)$, where $Dec_{\text{CP-ABE}}$ denotes CP-ABE based decryption algorithm.

5. Proposed Secure Data Sensor Exchange in Environmental Health Monitoring System

Our proposal of a secure environmental health conditions monitoring system and its implementation through WSN with considering secure data sensor exchange within IEEE 802.15.4 network and secure user data sensor access provided by Data Center Server over the Internet or any other public connection. This work may contribute to support a part of smart cities and take in part the Internet of Thing (IoT) technology. In our proposed system, the latest sensory information regarding the status of environmental health such as temperature, humidity, luminosity, noise level, carbon monoxide (CO) and carbon dioxide (CO_2) are transmitted by sensor nodes. We keep securely transmitted data sensors propagating through IEEE802.15.4-based communication toward a gateway node by encrypting data sensors and ensure their integrity such that receiving sensor nodes are able to recover the original data sensors without any corruption during transmission. Further, the collected data sensors in the gateway are synchronized to the Data Center Server through a secure TCP/IP connection for permanently storing by utilizing SSL/TLS and/or IP Security (i.e., IPSec) to construct a Virtual Private Network (VPN) between the gateway and Data Center Server. We provide an attributes-based authentication system to control the data sensors access. At anytime and anywhere, only legitimated users who successfully pass-through an attribute-based authentication system are able to access the data sensors. Fig. 3 shows our proposed secure data sensor exchange in environmental health monitoring system. Our proposed system consists of three sensor nodes connected to a gateway through IEEE 802.15.4 WSN connection. Then, through a secure IP-based connection, data sensors are synchronize from the gateway to Data Center Server.

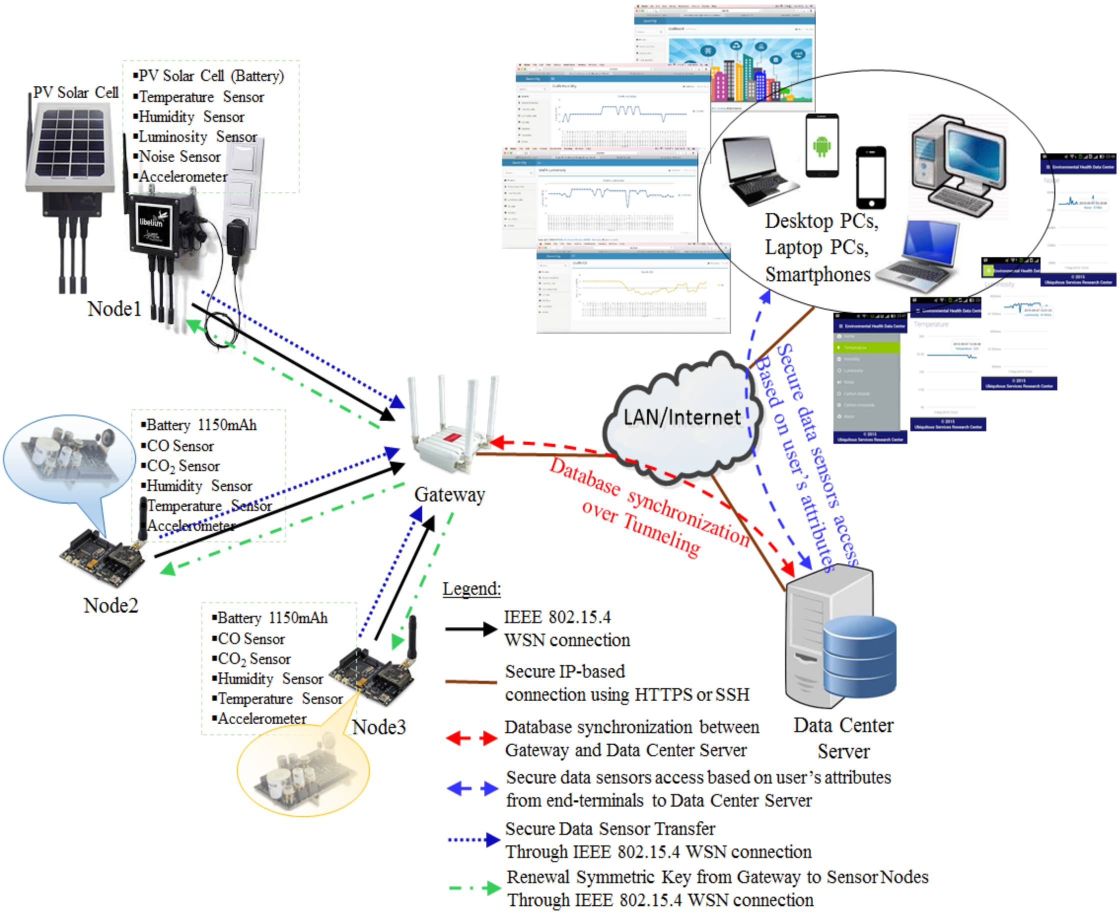
PV Solar Cell
▪PV Solar Cell (Battery)
▪Temperature Sensor
▪Humidity Sensor
▪Luminosity Sensor
▪Noise Sensor
▪Accelerometer
Node1
▪Battery 1150mAh
▪CO Sensor
▪CO_2 Sensor
▪Humidity Sensor
▪Temperature Sensor
▪Accelerometer
Node2
▪Battery 1150mAh
▪CO Sensor
▪CO_2 Sensor
▪Humidity Sensor
▪Temperature Sensor
▪Accelerometer
Node3
Gateway
LAN/Internet
Desktop PCs,
Laptop PCs,
Smartphones
Secure data sensors access Based on user's attributes
Database synchronization over Tunneling
Data Center Server
Legend:
→ IEEE 802.15.4 WSN connection
— Secure IP-based connection using HTTPS or SSH
↔ Database synchronization between Gateway and Data Center Server
↔ Secure data sensors access based on user's attributes from end-terminals to Data Center Server
→ Secure Data Sensor Transfer Through IEEE 802.15.4 WSN connection
→ Renewal Symmetric Key from Gateway to Sensor Nodes Through IEEE 802.15.4 WSN connection

Fig. 3 Proposed secure data sensor exchange in environmental health monitoring system

5.1 Our Approach of Secure Data Sensor Exchange

In this work, we consider on the IEEE 802.15.4 WSN, all three sensor nodes (i.e., Node1, Node2, and Node3) are located separately, but they are kept in the transmission coverage area with the gateway. We equipped all sensor nodes with the battery as their power supply to run their functionalities. We assume all sensor nodes are fixed and no mobility mechanism. In our construction of secure data exchange in environmental health monitoring system, we divide the security approach into three secure data sensor approaches: secure data transmission with key renewal, secure data sensor synchronization, and attribute-based authentication data sensor access. Shortly, to realize a secure data transmission, we utilize symmetric encryption to encrypt data sensors transmitted from sensor nodes to the gateway. To improve the security, we also perform key renewal mechanism to periodically renew the encryption key. We utilize OpenVPN - open source VPN software [21] to establish a tunnel between the gateway and Data Center Server to provide secure data sensors exchange through database synchronization, and CP-ABE scheme [10] with special scenario of access policy of attributes to control the user access to the data sensors in the Data Center Server as well as our previous system [11]. However, in the proposed attribute-based authentication data sensor access is slightly different from our previous system [11], whereas the role of manager is omitted to simplify and streamline the data sensor access system.

5.2 Construction of Our Proposed System

Again, in our construction system consists of three sensor nodes (i.e., Node1, Node2, and Node3) which have transmission range with the gateway and transmit data sensors over IEEE 802.15.4 WSN connection. Node1 is equipped with photo voltaic solar cell as the power supply to charge the battery. Node1 carries out temperature, humidity, luminosity, noise level, and accelerometer sensory information. Meanwhile, Node2 and Node3 carry out CO, CO_2, humidity, temperature, and accelerometer sensory information. The gateway is connected to Data Center Server through IP-based connection to forward data sensors from sensor nodes to Data Center Server.

5.2.1 Secure Data Sensor Transmission and Key Renewal

Our security construction to transmit data sensors from sensor nodes to the gateway is performed both in link layer and application layer. Fig. 4 shows the frame on layer stack of our proposed secure data sensor transmission from sensor nodes to the gateway. The first security approach is when the data sensors passing-through the link layer, data sensors are encapsulated by the security header using symmetric encryption algorithm AES 128-bit. To enable this functionality, in advanced, we configure in hardware the security setting onto the IEEE 802.15.4/ZigBee radio devices including the setup of encryption key. This mechanism establish a secure link between sensor nodes to the gateway. Only sensor nodes that configured the same encryption key with gateway are able to transmit data sensors to the gateway successfully.

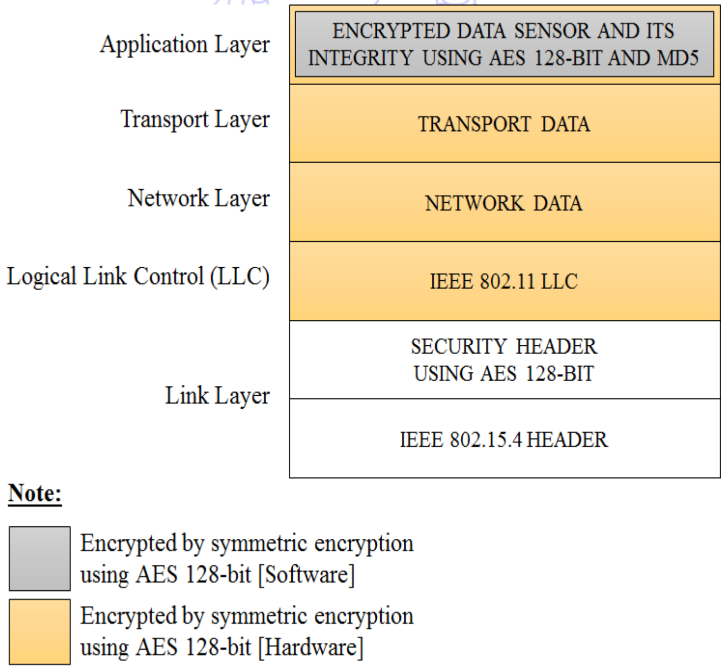
Application Layer
ENCRYPTED DATA SENSOR AND ITS INTEGRITY USING AES 128-BIT AND MD5
Transport Layer
TRANSPORT DATA
Network Layer
NETWORK DATA
Logical Link Control (LLC)
IEEE 802.11 LLC
SECURITY HEADER USING AES 128-BIT
Link Layer
IEEE 802.15.4 HEADER
Note:
Encrypted by symmetric encryption using AES 128-bit [Software]
Encrypted by symmetric encryption using AES 128-bit [Hardware]

Fig. 4 Frame on layer stack for proposed secure data sensor transmission

The second security is the use of AES 128-bit to encrypt data sensors in the application layer by activating the symmetric encryption algorithm AES 128-bit software which incorporated in the sensor nodes. This security mechanism creates a secure point-to-point data sensor transmission from sensor node to the gateway. In our design, we do not only enable data sensor encryption to convey confidentiality function, but also append data sensor integrity feature by utilizing a hash function MD5 algorithm. Thus, the gateway successfully decrypts the encrypted data sensors obtained from sensor nodes and checks the integrity of the recover data sensors whether data sensors are valid verified or not.

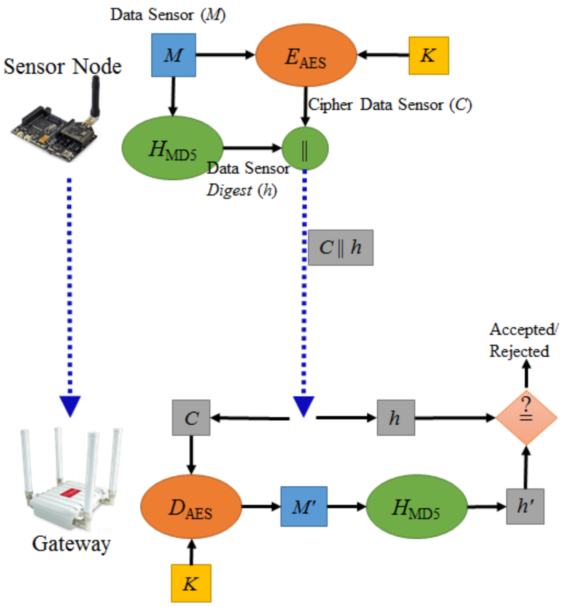

Fig. 5 Proposed secure data sensor transmission between sensor node and the gateway

Fig. 5 shows our proposed secure data sensor transmission from sensor node to the gateway which provides confidentiality and data sensor integrity simultaneously as well as our previous system [9]. Let M denotes a message of data sensor, $Enc_{\text{AES-128}}$ and $Dec_{\text{AES-128}}$ are AES 128-bit encryption and decryption algorithms, respectively. We employ MD5 hash function algorithm as the data sensor integrity function. K denotes a 128-bit valid encryption key between sensor nodes and the gateway which initially determined by the gateway and distributed to all participating sensor nodes. Meanwhile, || implies the concatenation of two or more string, text or data. Here, || is used for concatenating ciphertext of data sensor and data sensor digest h. Firstly, h is created by hashing the data sensor M with MD5 hash function, h = MD5(M). Then, data sensor M is encrypted using AES 128-bit encryption with encryption key K, $C = Enc_{\text{AES-128}}(M, K)$. Then, the result cipher data sensor C is concatenated with the data sensor digest h to create a tuple (C || h). Further, a tuple (C || h) is transmitted to the gateway over IEEE 802.15.4 WSN connection. Upon receiving a tuple (C || h), the gateway de-concatenates C and h. The ciphertext C is decrypted using gateway's valid encryption key K to recover a valid data sensor $M' = Dec_{\text{AES-128}}(C, K)$. Then, recovered data sensor M' is hashed into data sensor digest h'. The integrity of data sensor can be verified by comparing h and h'. If and only if h equals h', recovered data sensor is valid verified which means that data sensor is not altered during transmission. Otherwise, data sensor is discharged, which means data sensor is indicated not original anymore or has been modified during transmission. However, the use of encryption key many times increases the possibility of compromising the security of data sensors transmission. Therefore, to keep the freshness of encryption key K is expectable. To do so, there should be a mechanism to change the K either periodically or incidentally through a key renewal system.

In our construction of secure data sensor transmission from sensor nodes to the gateway, we also provide a simple key renewal system. Fig. 6 shows our key renewal system to change periodically the encryption key K. In our constructed system, we assume the gateway is the initiator and distributor of encrypted key K. In the setting up of the system, K is 128-bit key randomly chosen by the gateway and distributed to all participating sensor nodes. Then, periodically the gateway re-distributes a new 128-bit encryption key K_{NEW} to all participating sensor nodes in its transmission range of IEEE 802.15.4 WSN connection. In our system, we determine the periodic time of key renewal in a day. This means that every day the encryption key used by all participating nodes to encrypt data sensors is always changed, whereas the K_{NEW} is generated from the previous encryption key. K_{NEW} is distributed securely by the gateway to all participating sensor nodes broadcastly by simply encryption using AES 128-bit encryption algorithm. Let CK_{NEW} is the cipher of K_{NEW}, $CK_{\text{NEW}} = Enc_{\text{AES-128}}(K_{\text{NEW}}, K)$, whereas $Enc_{\text{AES-128}}$ is AES 128-bit encryption algorithm and K is the old encryption key. On the other words, $CK_i = Enc_{\text{AES-128}}(K_i, K_{i\text{-}1})$, whereas as K_i is the new encryption key, CK_i denotes the cipher of new encryption key, $K_{i\text{-}1}$ is the previous encryption key, and K_0 is the initial encryption key randomly determined by the gateway.

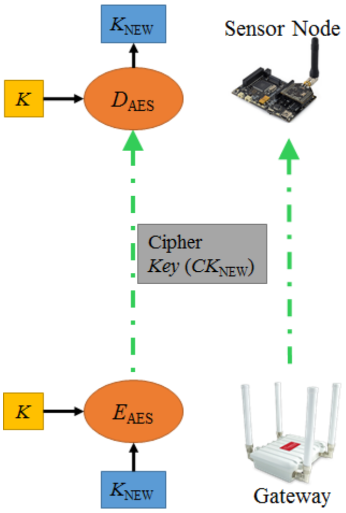

Fig. 6 Proposed simple encryption key renewal

The cipher of new encryption key CK_{NEW} is broadcastly distributed by the gateway to all participating sensor nodes. Upon receiving CK_{NEW}, each node recovers K_{NEW} by decrypting CK_{NEW} using the previous encryption key K, $K_{\text{NEW}} = Dec_{\text{AES-128}}(CK_{\text{NEW}}, K)$, whereas $D_{\text{AES-128}}$ is AES 128-bit decryption algorithm or $K_i = Dec_{\text{AES-128}}(CK_i, K_{i\text{-}1})$. Again, K_i is the new encryption key, CK_i denotes the cipher of new encryption key, and $K_{i\text{-}1}$ is the previous encryption key.

5.2.2 Secure Data Sensor Synchronization

We employ OpenVPN - open source VPN software [21] to create a secure tunnel lied between the gateway and Data Center Server over IP-based connection. Here, we configured Data Center Server as VPN server and the gateway acts as the VPN client. Security model of OpenVPN is designed on using SSL/TLS for creating a session authentication procedure and the IPSec Encapsulating Security Payload (ESP) protocol for establishing a secure tunnel transport over IP-based connection through User Datagram Protocol (UDP). Throughout VPN, data sensors store temporarily in the gateway could be synchronized securely to Data Center Server for storing permanently. We employed MySQL - database open source software to synchronize and update data sensors from sensor nodes to Data Center Server.

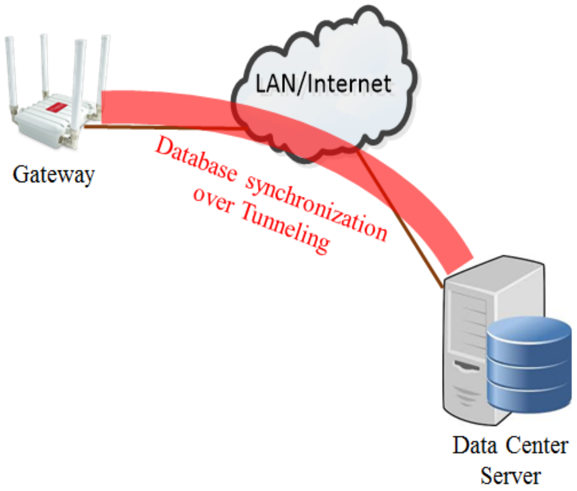

Fig. 7 Establishment VPN tunnelling using OpenVPN in secure database synchronization

Fig. 7 shows the establishment VPN tunnelling constructed using OpenVPN, whereas Data Center Server acts as a VPN server and the gateway acts as a VPN client.

5.2.3 Attribute-Based Authentication Data Sensor Access

To access sensory information provided by Data Center Server through public network, such as Internet, users have to pass attribute-based authentication system. Similar to common services access provided by service provider who offers specific services, participating users in this attribute-based authentication data sensor access system have to register themselves to the system by endowing their set of attributes possession S_i as shown in Fig. 8. In our proposed system, the role of KGS is taken over by Data Center Server that provides sensory information of environmental health conditions.

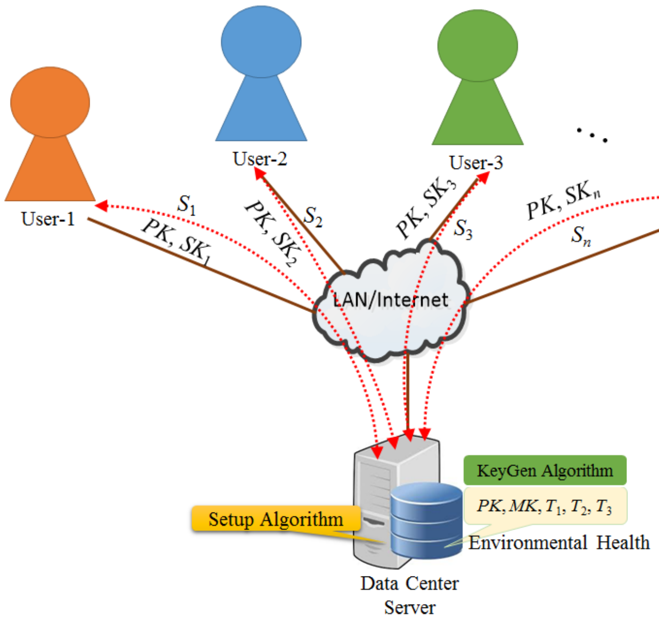

Fig. 8 Users joining to the attribute-based authentication data sensor access system

Firstly, Data Center Server executes Setup algorithm to generate public key *PK* and master key *MK*. In addition, Data Center Server also has a responsible to determine access policy of attributes T_1, T_2, and T_3. Let assume User-*i* (i.e., User-1, User-2, User-3, …, User-*n*) wants to join to the system. User-*i* endows his/her set of attributes possession S_i along with his/her account in the registration system. On given S_i, Data Center Server operates KeyGen algorithm to generate corresponding user secret key SK_i associated with User-*i*'s set of attributes possession S_i. Meanwhile, from user's account i.e., password is used for Message Authentication Code (MAC) key K_{HMAC} to provide data sensors integrity feature. In this goal, we utilize MAC using SHA 256-bit hash function, HMAC. Then, Data Center Server supplies the joining User-*i* public key PK and User-*i*'s secret key SK_i. Here, Data Center Server prepares set of access policy of attributes, T_1, T_2, and T_3 for later on encrypting data sensors. As well as previous system [11], we adopt three scenarios of access policy of attributes T_1, T_2, and T_3. The access policy of attributes relations are depicted in Fig. 9 to Fig. 11.

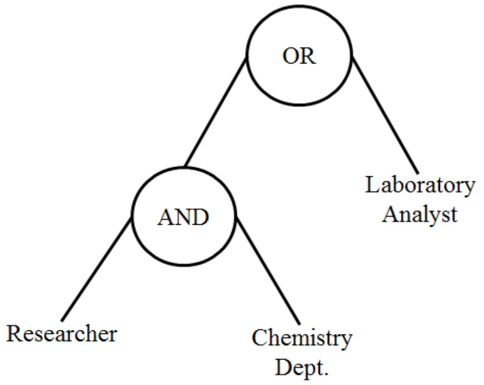

Fig. 9 Access policy of attributes T_1 for accessing gases sensory information (i.e., CO and CO_2)

Fig. 9 illustrates the access policy of attributes T_1 relation which is used for encryption data sensors for users' request on gases sensory information such as CO and CO_2. Here, we assume that Laboratory Analyst and Researcher in Chemistry Dept. are kind of users who need gases sensory information. The access policy of attributes relation shown in Fig. 9 can be represented as:

$$T_1 = (\text{“Laboratory Analyst”} \vee (\text{“Researcher”} \wedge \text{“Chemistry Dept.”})).$$

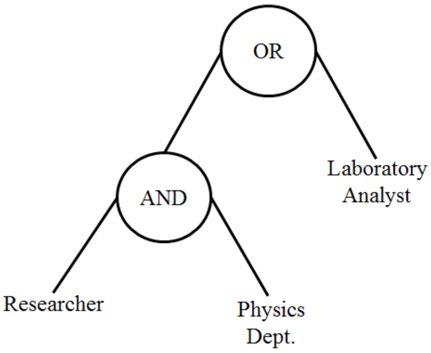

Fig. 10 Access policy of attributes T_2 for accessing environmental condition related sensory information (i.e., temperature, humidity, luminosity, and noise level)

Similarly, Fig 10 illustrates the access policy of attributes T_2 relation for response users' access data sensors request on sensory information related to environmental conditions such as temperature, humidity, luminosity, and noise level. In this case, we assume that Laboratory Analyst and Researcher in Physics Dept. are kind of users who need environmental conditions sensory information. Where T_2 can be expressed as:

$$T_2 = (\text{“Laboratory Analyst”} \vee (\text{“Researcher”} \wedge \text{“Physics Dept.”})). \quad (1)$$

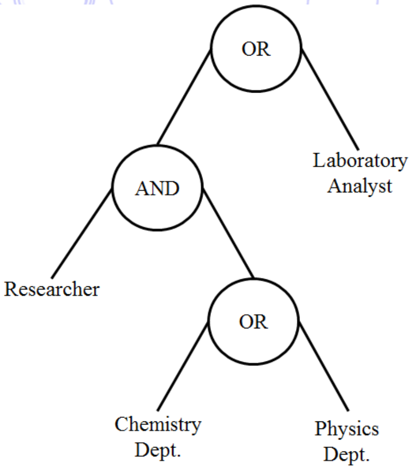

Fig. 11 Access policy of attributes T_3 for accessing the battery level sensory information

Meanwhile, access policy of attributes T_3 relation depicted in Fig. 11 is used for responding users' access data sensors request on sensory information of battery level because we assume that Laboratory Analyst, Researcher in the Chemistry Dept., and Physics Dept. are kind of users who need sensory information of battery level for monitoring the availability of sensor nodes. Where, T_3 can be expressed as:

$$T_3 = (\text{“Laboratory Analyst”} \vee (\text{“Researcher”} \wedge (\text{“Chemistry Dept.”} \vee \text{Physics Dept.}))). \quad (2)$$

For example, let User-1 who has a set of attributes possession S_1, "Researcher in the Chemistry Dept." associated with his/her secret key SK_1 requests on access data sensors related to gases sensory information Data Center Server. Further, Data

Center Server prepares the requested gases sensory information M and encrypts such information using T_1, $CT_M = Enc_{\text{CP-ABE}}(PK, T_1, M)$, then transmits the encrypted data sensors CT_M to User-1. In this case, User-1 is able to successfully decrypt the encrypted data sensors using his/her SK_1 and recover data sensors, due to his/her S_1 matches with access policy of attributes T_1, $M = Dec_{\text{CP-ABE}}(SK_1, CT_M)$.

Fig. 12 illustrates the mechanism of data sensors access in our previous system [11]. Among joining users, there exists a special user called manager who has a responsibility to encrypt data sensors requested by the users. In this system, whenever users request a specific data sensors access, Data Center Server commands the manager to encrypt the users' data sensors request and return back the result encrypted data sensors to Data Center Server such that Data Center Server forwards the encrypted data sensors obtained from the manager to the users. This mechanism is adequate complex in term of operational procedure for accessing data sensors.

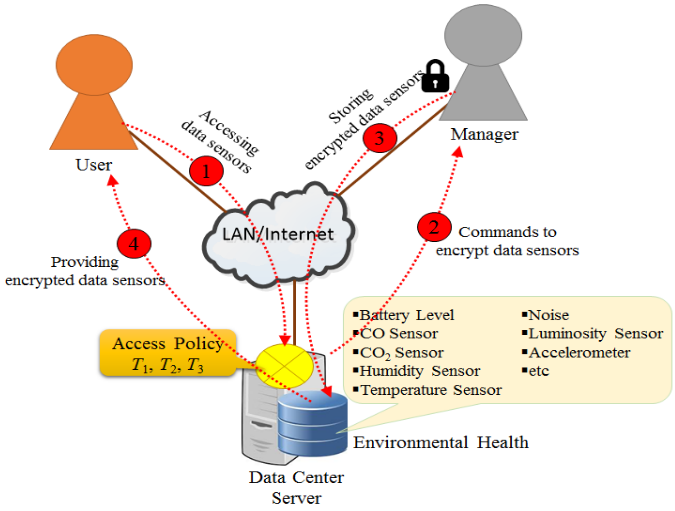

Fig. 12 Attribute-based encryption to access data sensors in the previous system [11]

To simplify the operational procedure of previous system [11], we propose a different procedure which much simpler and better than the previous one as shown in Fig. 13. In our proposed attribute-based encryption, we omitted the role of manager. Whenever users request an access of specific sensory information to Data Center Server, the Data Center Server immediately encrypts the requested data sensors using corresponding access policy of attributes either T_1, T_2 or T_3 and sends back the encrypted data sensors to the users. The users decrypt successfully the encrypted data sensors obtained from Data Center Server and recover data sensors if and only if their set of attributes possession matches with corresponding access policy of attributes.

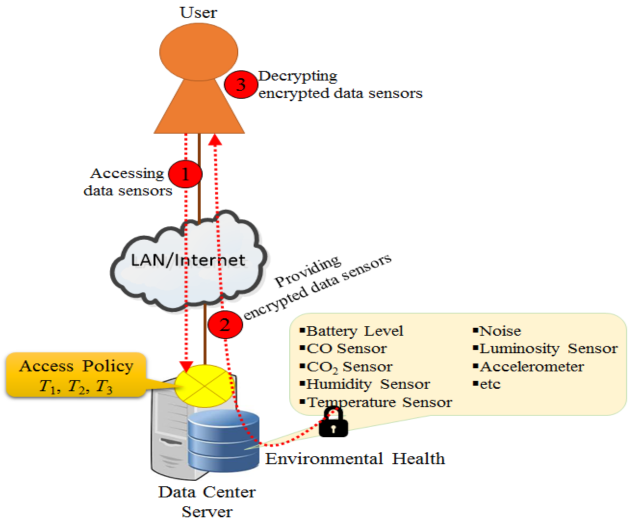

Fig. 13 Proposed attributed-based encryption to access data sensors from Data Center Server

6. Implementation and Experimental Measurements

In this Section, we describe the implementation and experimental results of our secure data sensor exchange in environmental health monitoring system through WSN with hardware and software specifications are described in Table 1. We combined both hardware security in the link layer as well as in [8-9, 18] and software security in application layer using proposed security scenario shown in Fig. 5. We employed MD5 as the hash function and AES-128 as the symmetric algorithm with operation mode Electronic Codebook (ECB) and PKCS5 padding as well as previous system [9]. The total time computations needed by sensor node to transmit encrypted data sensor frame is only about 312 ms including initialization and communication time and the total time to decrypt and recover received encrypted data sensor frame by the gateway is only about 144 ms, respectively. Here, the computation load of proposed system security comprises an AES-128 encryption and an MD5 hash function.

Table 1 Hardware and software specifications used in the experimental

Sensor Nodes (Node1~Node3)	Gateway	Data Center Server	End User
Microcontroller ATmega1281 14MHz, SRAM 8KB, EEPROM 4KB, FLASH 128KB, Clock RTC 32KHz, 802.15.4/ZigBee 2.4GHz	Geode Integrated AMD PCS x86 Processor 500MHz, cache memory 128KB, RAM 256MB, Disk 8GB, Linux Debian kernel-2.6.30, WiFi Atheros AR5213A 802.11b/g 100mW -20dBm, XBee Pro 802.15.4 2.4GHz 100mW, Ethernet Controller VIA VT6105M [Rhine III] and GNU C Compiler 4.3	Intel Xeon 3.2 GHz, RAM 4GB DDR3, Linux Debian kernel-3.5.0-17, gcc-4.7.2, gmp-5.1.1, pbc-lib-0.5.14, glib-2.34, openssl-1.0.1e, Java 1.8.060, apache-tomcat-8.0.15.	Intel Core i3 2.4 GHz, RAM 2GB DDR3, Wifi 802.11b/g/n, Linux Debian kernel-3.5.0-17 gcc-4.7.2, gmp-5.1.1, pbc-lib-0.5.14, glib-2.34, openssl-1.0.1e, Java 1.8.060, Mozilla firefox-40.0.3.

Meanwhile, in the implementation of key renewal, we inserted micro SD memory card for each sensor node to store the current encryption key. Whenever the gateway broadcastly retransmits the new encryption key, all sensor nodes save the new key into their micro SD memory for encrypting data sensors. We set the schedule for renew the encryption key every day. Of course, we can change this schedule based on demand, whereas for each key renewal process, it needs about 270 ms including the transmission time.

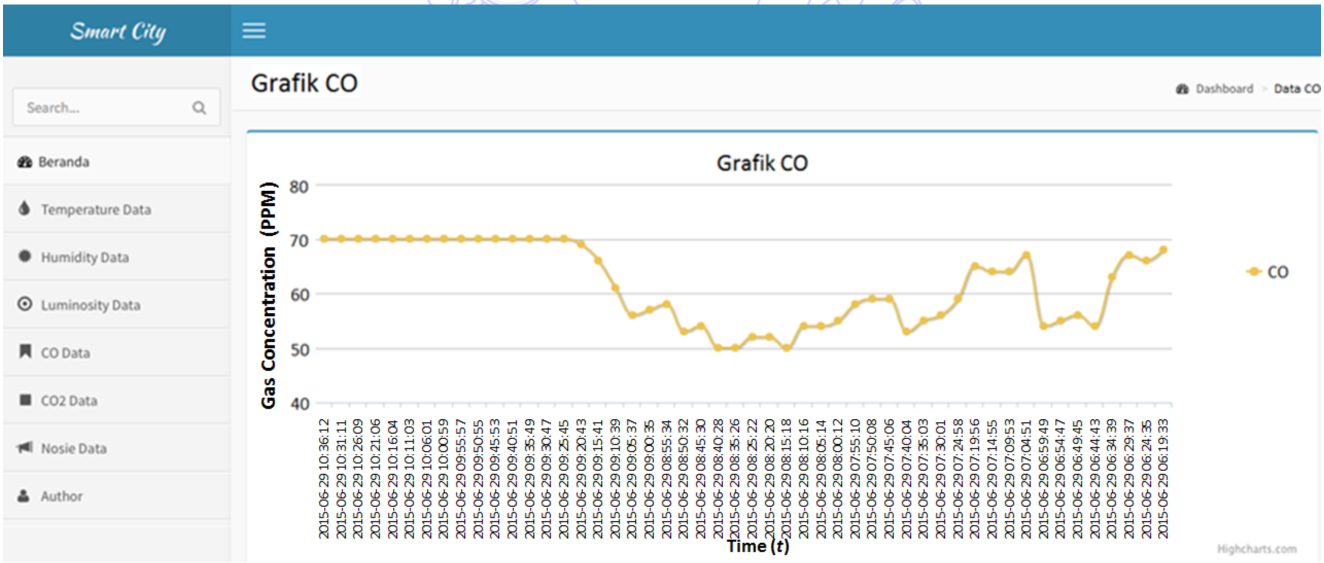

Fig. 14 Example of data sensor access from web-based application

Fig. 14 shows a web-based data sensor access example from the user end device (i.e., Laptop PC and Smartphone). As well as web-based application to access the collected data sensors stored in the Data Center Server, our proposed system also provides mobile application to monitor the current condition of environmental health. Fig. 15 displays temperature, humidity, and luminosity sensory information in the mobile device.

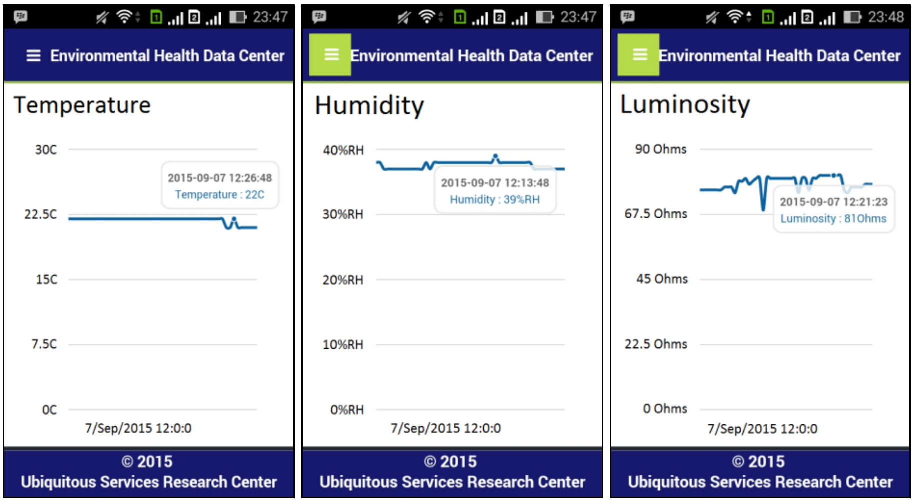

Fig. 15 Data sensors of temperature, humidity, and luminosity accessed through a mobile application

We implemented our attribute-based authentication system using Java through the Java Server Pages (JSP). The communication between the users, and Data Center Server is over IP-based connection through HTTP communication. We adopted a middleware [17] for CP-ABE scheme [10], which is implemented on the Pairing-based Cryptography (PBC) library [16] in C language, whereas PBC library is for pairing and the underlying ECC computations used in the CP-ABE. In the middleware, CP-ABE is hybrid applied of AES and CP-ABE. In this case, we used this hybrid version with insertion of HMAC algorithm to provide the integrity of data sensors. Fig. 16 illustrates the implementation of our CP-ABE based encryption for attribute-based authentication in accessing data sensors.

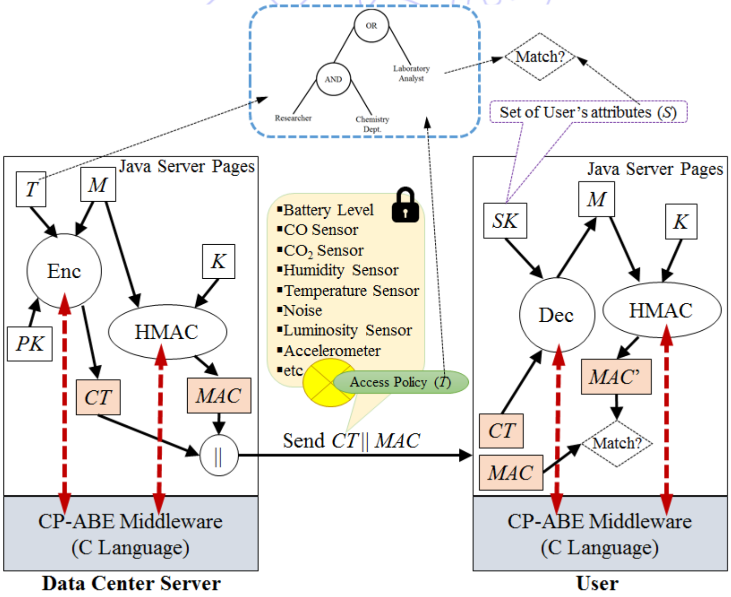

Fig. 16 Implementation of CP-ABE based encryption for accessing data sensors

In Fig. 16, K_{HMAC} of the users is derived from their password obtained in the registration phase. When a user request a specific sensory information, let say this user has a set of attributes possession S_i, “Researcher in the Chemistry Dept.” associated with his/her secret key SK_i requests on access data sensors of CO and CO_2 to Data Center Server. Here, Data Center Server prepares the data sensors of CO and CO_2, let say M is data sensors of CO and CO_2. Then, Data Center Server encrypts M using appropriate access policy of attributes with user request on data sensors of CO and CO_2, that is T_1, $CT_{\mathrm{M}} = Enc_{\text{CP-ABE}}(PK, T_1, M)$. In addition, Data Center Server generates $MAC = \mathrm{HMAC}(M, K_{\mathrm{HMAC}})$, concatenates CT_{M} and MAC, (CT_{M} || MAC), and sends a tuple (CT_{M} || MAC) to the user. Upon receiving a tuple (CT_{M} || MAC), the user de-concatenates the tuple, decrypts CT_{M},

M' = $Dec_{\text{CP-ABE}}(SK_i, CT_M)$, and computes MAC' = HMAC(M', K_{HMAC}). In this case, the user successfully recovers M, due to his/her S_i matches with access policy of attributes T_1. The user checks the integrity of recovered M' by comparing received MAC and computed MAC'. If and only if MAC' equals MAC, the user gets the original data sensors of CO and CO_2 without any modification or corruption during data sensors transmission.

Table 3 Total execution time of CP-ABE encryption based on access policy of attributes

Access policy of attributes	Encryption		Decryption	
	Computation time (ms)	Cipher size (Byte)	Computation time (ms)	Data sensor size (Byte)
T_1	60.36	8060	20.11	6837
T_2	60.43	8058	20.10	6837
T_3	80.32	8348	25.12	6837

Table 4 Total execution time of CP-ABE encryption based on user access data sensors request

Data sensors request	Encryption		Decryption	
	Computation time (ms)	Cipher size (Byte)	Computation time (ms)	Data sensor size (Byte)
CO || CO2	60.35	14714	10.10	13496
Temp || Hum || Lum || Noise	60.45	28394	10.11	27178
Battery level	70.27	8444	20.11	6932

Table 3 shows the CP-ABE based encryption time on 6837 Bytes data sensor of the last 100 data temperature. Encryption time when using access policy of attributes T_1 and T_2 is about 60 ms, meanwhile, when using T_3, it consumes about 80 ms. On the other hand, decryption time for T_1 and T_2 is about 20 ms, whereas decryption time for T_3 is about 25 ms.

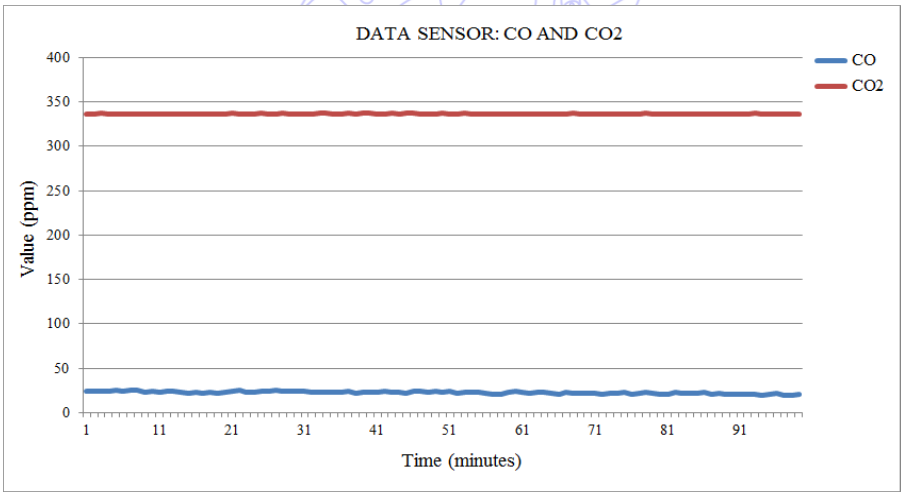

Fig. 17 Obtained recovered data sensors of gases CO and CO_2 w.r.t T_1

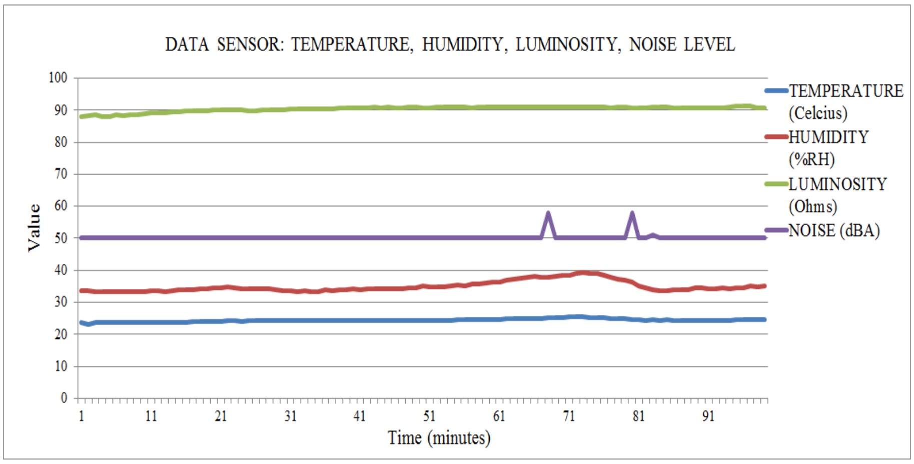

Fig. 18 Obtained recovered data sensors of temperature, humidity, luminosity, and noise level w.r.t T_2

Table 4 shows the CP-ABE based encryption time based on user access data sensors request. Encryption time when the user requests on 13496 Bytes of 100 last gases data CO and CO_2 w.r.t T_1 is about 60 ms, meanwhile, when accessing 27178 Bytes of 100 last data temperature, humidity, luminosity, and noise level w.r.t T_2, it consumes about 60 ms, and for accessing 6932 Bytes of last 100 battery level conditions w.r.t T_3 is about 70 ms. On the other hand, decryption time for access data sensors of gases (CO and CO_2) and environmental conditions (temperature, humidity, luminosity, noise level) is about 10 ms. Meanwhile for battery level, decryption time takes 20 ms.

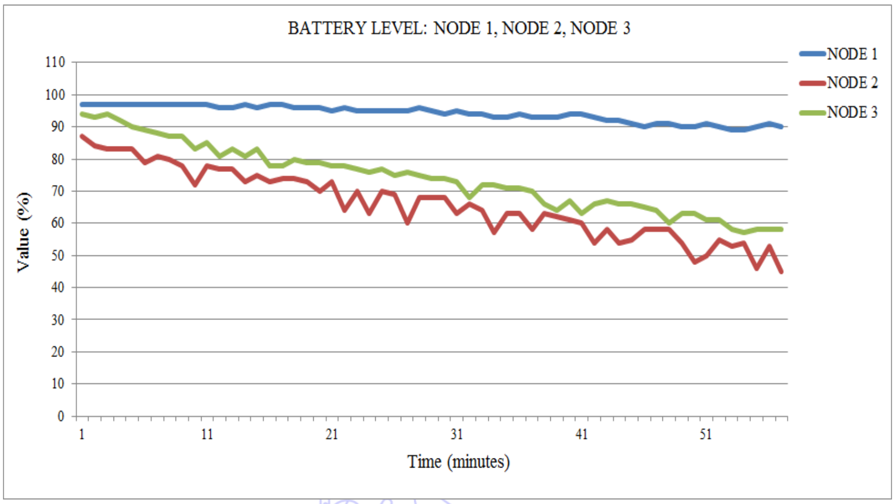

Fig. 19 Obtained recovered data sensors of battery level of all sensor nodes w.r.t T_3

Fig. 17 to Fig. 19 show the data sensors successfully obtained by the user when his/her set of attributes possession S_i matches with access policy of attributes T_1, T_2, or T_3. Fig. 17 shows data sensors of gases CO and CO_2 obtained by the user whose attribute possession of Laboratory Analyst or Researcher in the Chemistry Dept. which deals with T_1. CO and CO_2 values in average are about 23 ppm and 336 ppm, respectively. Fig. 18 shows data sensors of environmental health conditions, such as temperature, humidity, luminosity, and noise level obtained by the user whose attribute possession of Laboratory Analyst or Researcher in the Physics Dept. which deals with T_2. Temperature, humidity, luminosity, and noise level values in average are about 24^{o}C, 33 %RH, 89 Ohms, and 50 dBA. Fig. 19 shows the battery level conditions of Node1, Node2, and Node3 obtained by the user whose attribute possession of Laboratory Analyst or Researcher in the Chemistry Dept. or Researcher in the Physics Dept. which deals with T_3. Node1 is equipped with photo voltaic solar cell, hence the condition of its battery level is relatively stable in about 95%, due to the battery is always charged by the photo voltaic solar cell. Meanwhile, the battery level of Node 2 and Node3 time-based decreases gradually from 87% to 45%, and from 94% to 58%, respectively.

7. Conclusions

We have presented a secure data exchange in environmental health monitoring system through WSN and its implementation which offers secure data sensor transmission from sensor nodes to the gateway to keep the confidentiality and data sensor integrity simultaneously, secure data sensor synchronization between the gateway and Data Center Server, and attribute-based authentication user access data sensors using CP-ABE with HMAC. The experimental results show the practicality of the system in the 14 MHz Microcontroller and the current environmental of PCs.

Our future works include the adoption of more efficient security system in the WSN sensor nodes and CP-ABE in the attribute-based authentication for data sensor access with faster pairing-based library.

Acknowledgements

This work was partially supported by Penelitian Unggulan Perguruan Tinggi (PUPT), Ministry of Research, Technology, and Higher Education, Republic of Indonesia.

References

[1] M. F. Othman and K. Shazali, "Wireless sensor network applications: a study in environmental monitoring system," International Symposium on Robotics and Intelligent Sensors 2012 (IRIS ’12), Procedia Engineering 41, pp. 1204-1210, 2012.

[2] R. Mittal and M. P. S. Bhatia, "Wireless sensor networks for monitoring the environmental activities," International Conference on Computational Intelligent and Computing Research (ICCIC), pp. 1-5, 2010.

[3] S. Ferdoush and X. Li, "Wireless sensor network system design using raspberry pi and arduino for environmental monitoring applications," The 9th International Conference on Future Networks and Communications (FNC ’14), Procedia Computer Science 34, pp. 103-110, 2014.

[4] M. U. H. Al Rasyid, B. H. Lee, and A. Sudarsono, "Wireless body area network for monitoring body temperature, heart beat and oxygen in blood," International Seminar on Intelligent Technology and Its Applications (ISITIA), pp. 93-96, May, 2015.

[5] N. Fahmi and M. U. H. Al Rasyid, "A wireless sensor network for environmental monitoring gases," Knowledge Creation & Intelligent Computing (KCIC2015), pp. 56-61, March, 2015.

[6] P. Szczechowiak, Security in wireless sensor networks, Lap Lambert Academic Publishing, ISBN: 978-3-8443-9043-8, 2011.

[7] G. V. Crosby, T. Ghosh, R. Murimi, and C. A. Chin, “Wireless body area networks for healthcare: a survey,” International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), vol. 3, no. 3, June, 2012.

[8] A. Sudarsono, M. U. H. Al Rasyid, H. Hermawan, "An implementation of secure wireless sensor network for e-healthcare system", International Conference on Computer, Control, Informatics, and Its Application (IC3INA), pp. 75-80, 2014.

[9] A. Sudarsono, P. Kristalina, M. U. H. Al Rasyid, and R. Hermawan, “An implementation of secure data sensor transmission in wireless sensor network for monitoring environmental health,” International Conference on Computer, Control, Informatics and its Applications (IC3INA), pp. 94-99, 2015.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption", IEEE Symposium on Security and Privacy, pp.321-334, 2007.

[11] S. Huda, N. Fahmi, A. Sudarsono, and M. U. H. Al Rasyid, "Secure data sensor sharing on ubiquitous environmental health monitoring application," Recent Advancement in Informatics, Electrical and Electronics Engineering International Conference (RAIEIC ‘15), Dec. 10–12, 2015.

[12] A. Sudarsono and T. Nakanishi, “An implementation of secure data exchange in wireless delay tolerant network using attribute-based encryption,” 2nd International Symposium on Computing and Networking (CANDAR ‘14), pp. 536-542, Dec., 2014.

[13] W. Stalling, Network security essentials: applications and standards (4th edition), ISBN-13: 978-0136108054, Pearson, March 22, 2010.

[14] B. A. Forouzan, Cryptography and network security, ISBN-13: 978-0070702080, McGraw-Hill, 2010.

[15] G. V. Crosby, T. Ghosh, R. Murimi, and C. A. Chin, “Wireless body area networks for healthcare: a survey,” International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), vol. 3, no. 3, June, 2012.

[16] B. Lynn, PBC (Pairing-Based Cryptography) library, http://crypto.stanford.edu/pbc/ [accessed on October, 2015].

[17] J. Bethencourt, A. Sahai, and B. Waters, cpabe toolkit in Advanced Crypto Software Collection, http://hms.isi.jhu.edu/acsc/cpabe/ [accessed on October, 2015].

[18] Libelium - Connecting sensors to the cloud, http://www.libelium.com/ [accessed on August, 2015].

[19] K. Tsai, F. Leu, T. Wu, S. Chiou, Y. Liu, and H. Liu, "A secure ECC-based electronic medical record system", Journal of Internet Services and Information Security (JISIS ‘14), vol. 4, no. 1, pp. 47-57, 2014.

[20] C. Rong and H. Cheng, "A secure data access mechanism for cloud tenants," The 3rd International Conference on Cloud Computing, GRIDs, and Virtualization, pp. 113-119, 2012.

[21] OpenVPN - Open Source VPN, https://openvpn.net/ [accessed on October 2015].

[22] S. Huda, A. Sudarsono, and T. Harsono, “Secure data exchange using authenticated ciphertext-policy attributed-based encryption,” 2015 International Electronics Symposium (IES ‘15), pp. 140-145, 2015.