International Journal on Advanced Science Engineering Information Technology

Vol.7 (2017) No. 2
ISSN: 2088-5334

Secure Data Sensor In Environmental Monitoring System Using Attribute-Based Encryption With Revocation

Munsyi[#], Amang Sudarsono[#], M. Udin Harun Al Rasyid[#]

[#] *Department of Information and Computer Engineering, Magister Program of Engineering Technology*
Electronics Engineering Polytecnic Institute of Surabaya
Kampus PENS, Jalan Raya ITS, Sukolilo 60111, Surabaya, Indonesia
E-mail: munsyi@pasca.student.pens.ac.id, {amang, udinharun}@pens.ac.id

***Abstract*— Wireless sensor networks in internet of thing era have many applications, one of them for environment system, in environmental monitoring system everybody can access data anytime and anywhere. Information was collected using wireless sensor network, all of the data will be sent and stored in the data center. All of data in the data center can be accessed by users through HTTP protocol using a laptop, smartphone and Personal computer. The data in the data center must be secured and the data should be protected from the illegal access by the users from the environment monitoring. To secure the data from the illegal access by the user then the environment monitoring required a security with revocation aspect and encryption the data. CP-ABE (Ciphertext-Policy Attribute-Based Encryption) becomes a solution for this issue, to protect the sensor data and revoke the user. We propose a secure system using CP-ABE with user revocation for protecting the data in data center. Our system is not only encrypting the data sensor, but also revoke to the user. Our experiments system using CP-ABE showed the result for secure the sensor data and revoked the user who does not have the access rights. there are only 2 second processing time for revocation check users.**

***Keywords*— wireless sensor networks; environment monitoring; CP-ABE; user revocation.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have many applications in the internet of things era. One of them is an application for environment monitoring [2][3][4][5]. The environmental monitoring system uses WSN technology to obtain information such as carbon dioxide, carbon monoxide, temperature, humidity, luminosity, and noise. The data obtained from WSN will be sent to a data center that can be accessed by the users who want to get information from the environmental system. In the end, that data can be used for a research, a business planning, and to find out the quality of an area. The collected data in the data center should be easily read by the user. The data center without security can be intercepted, tracked and even modified by the user without the access rights [1]. The system requires an encryption for the data sensor in the data center to protect the data from the illegal user.

To protect the sensor data in the data center, there are so many methods from previous researchers in contexts of data security, for example, a system that performs an encryption for the sensor data with Ciphertext-Policy Attribute-Based Encryption with authentication using HMAC [3]. This method is the best to protect data from the user who did not have the access right. But this method has a problem, that it cannot protect the data center if the user with the access right did an illegal access. Because of the importance of the existing data, in the data center, then the system requires a data security and restriction on the accessing aspect. Only registered users and the ones who have access rights can view the data. In this case, there will be a problem, if there are users who perform the illegal access. To answer these problems, then the revocation of access is required. One of the cryptographic solutions for secure and revoke the user is the use of CP-ABE with Revocation schemes [10].

ABE (Attribute Based Encryption) [11] is a new approach for encrypted access control. It offers security and access control. CP-ABE (Ciphertext-Policy Attribute-Based Encryption) [3] is one of the variant of ABE algorithm. CP-ABE is an asymmetric encryption mechanism that provides features using the user attributes as rule of policy in the ciphertext. In CP-ABE, the ciphertext will be decrypted if and only if the attribute set of user's private key appropriate with the rule policy in the ciphertext. CP-ABE is appropriate for most applications, like for data exchange over wireless medium [3].

In this paper, we propose a secure system to protect the data center from illegal access user using web-based

communication applied java server page with HTTP protocol for IoT in environmental monitoring system case study. In this research, we consider for constructing a security system in web-based for the environmental monitoring system. We adopt the CP-ABE algorithm for secure data sensor in the data center and revoke the user.

The contribution of this paper, we implement CP-ABE applied HTTP protocol for communication using java server pages including the revocation for the user with the access right if the user did the illegal access. The system will be secured all of the data in the data center with encrypted before sending to the user. The system can be accessed by the user anywhere and anytime use their end devices such a smartphone, laptop and personal computer.

II. MATERIAL AND METHOD

Recently, many researchers has been researched about the environmental monitoring system. Fahmi, et al. [5] proposed a fuzzy logic for implementation of environmental health monitoring system based on WSN. The communication between the sensor node and the gateway use ZigBee 802.15.4 standard protocol. This research is applied real hardware using Microcontroller ATMega 1281 and Gases Sensor Board developed by Waspmote.

An environmental system without security will be affected to the original data where the user can intercept, tracked and even modified the data. The research for secure data has many methods for protecting the original data from illegal access, for example. Sudarsono, et al. [1] proposed a security method use the authentication system using pairing-based verifier-local revocation group signature scheme to authenticate wireless node of a particular privilege group to the gateway node in transmission data. The researchers used VLR group signature to reduce the revocation mechanism in the user and omit some procedures in Registration phase and Authentication phase of previous VLR group signature scheme. This research was applied in the real hardware using Raspberry Pi2 for sensor and gateway node, PC with Intel Core i7 2.60 GHz and Broadcom BCM43xx 1.0 for data center with 4 GB RAM, 1.80 Ghz with 2 GB RAM and Intel Dual Band Wireless-N 7260 IEEE802.11 a/b/g/n for User and for communication using TP-Link TL-WN722N 150 Mbps IEEE802.11b/g/n..

The secure system for protecting the data is very growing very rapidly. In the previous research [1], the researcher implemented the pairing-based verifier-local revocation group signature scheme for secure the transmission data. but in this research data in the data center is not secure because data was still in the form of the original data. The user with access right can directly read data. the only user in revocation list can't read the data because his transmission will be rejected by the system. There are many method to protect the data [3][6], where they analyzed the secure data with encryption. Make a palintext become a ciphertext with Ciphertext Policy Attribute-Based Encryption (CP-ABE). They are using the wireless and mobile protocol for communication not using the HTTP Protocol. In their research, they are just secure the data, but they not do the revocation for the user. The system not protecting the data center if the user with access right do the illegal access. The system from researcher only use in limitted area, user cannot access anywhere and anytime.

The previous researcher Huda, et al. [3] combined the method using Ciphertext-Policy Attribute-Based Encryption with Hash Message Authentication Code (HMAC) for integrity the data. The researcher uses the scheme for the military environment in the battlefield with the communication between soldier and captain using Mobile Ad-Hoc Network (MANET). The system is secured the information exchange protocol between all soldier. Using CP-ABE for secure the data and HMAC for integrity the data. All of the data will be encrypt using AES method before send to the other soldier. The only soldier with access right can read the original data.

Roy, et al. [10] proposed a security method using Ciphertext Attribute-Based Encryption for Disruption Tolerant Network. The researcher is applied CP-ABE with combining AES method for secure the data. the system handling the static and dynamic attributes the DTN Users where static attributes whose value remain unchanged for a long time and dynamic attributes which need to be updated periodically. This method is also using revocation technique where each message to be encrypted with a modified access policy, which is constructed by augmenting the original access policy with an additional list of revoked user ID. Formally, the new access policy (T) structure is as follows: T' = (T AND ((NOT X1) AND (NOT X2) AND (NOT Xn))), where users X1, X2, Xn have been revoked.

The previous researcher Huda, et al. [10] combined the method using Ciphertext-Policy Attribute-Based Encryption with Hash Message Authentication Code (HMAC) for integrity the data. The researcher uses the scheme for ubiquitous environmental health monitoring with HTTP protocol communication. The system is secure the data center with encrypting the data sensor use the CP-ABE and HMAC for integrity the data.

L. Touati, et. Al. [19] using the method Cooperative Ciphertext Policy Attribute-Based Encryption (C-CP-ABE) for the Internet of Things. The researcher compares the original CP-ABE method with their method C-CP-ABE. The researcher using C-CP-ABE to secure the communication between node in the IoT but the problem in this method is not able to secure data in the data center. Users with the access right can access anything. In our scheme, we need the system to protect all of data in the data center from illegal access user with the access right and only user with the access right can access the data.

We propose our scheme for environment monitoring with secure data and revoke user from previous researcher[3][9][10][19]. To secure data sensor in the data center we using the method from previous researcher [11] for encrypting the data sensor in the data center but the problem is we cannot revoke user with the access right if the user did the illegal access. The previous researcher proposes the method can revoke user with include NOT logic in the policy of ciphertext[9]. All of the users can make policy for encrypting the data with NOT logic to revoke user. We cannot apply this method to our scheme. From this method we combine and modified this method using web-based for revoke user who did the illegal access. The only user with access right can read the original data sensor.

In this section, we describe the different method between original CP-ABE and our proposed CP-ABE.

A. Original Scheme Ciphertext Attribute-Base Encryption

In the original CP-ABE scheme [6], a message M will be encrypt using the public key (PK) and access policy that associated with user attributes. The access policy is expressed by a logical on attributes from the user. Each user has a set of attributes which expressed information like shown in Fig. 1.

The secret key (SK) will generate by trusted party such as Key Distribution Center (KDC). After the KDC Generated the key, the key will be sent to the user. The user uses the Public Key and attributes for encrypting the original message to be a ciphertext. The only user has attributes matched with the access policy can successfully decrypt and read the original message

.

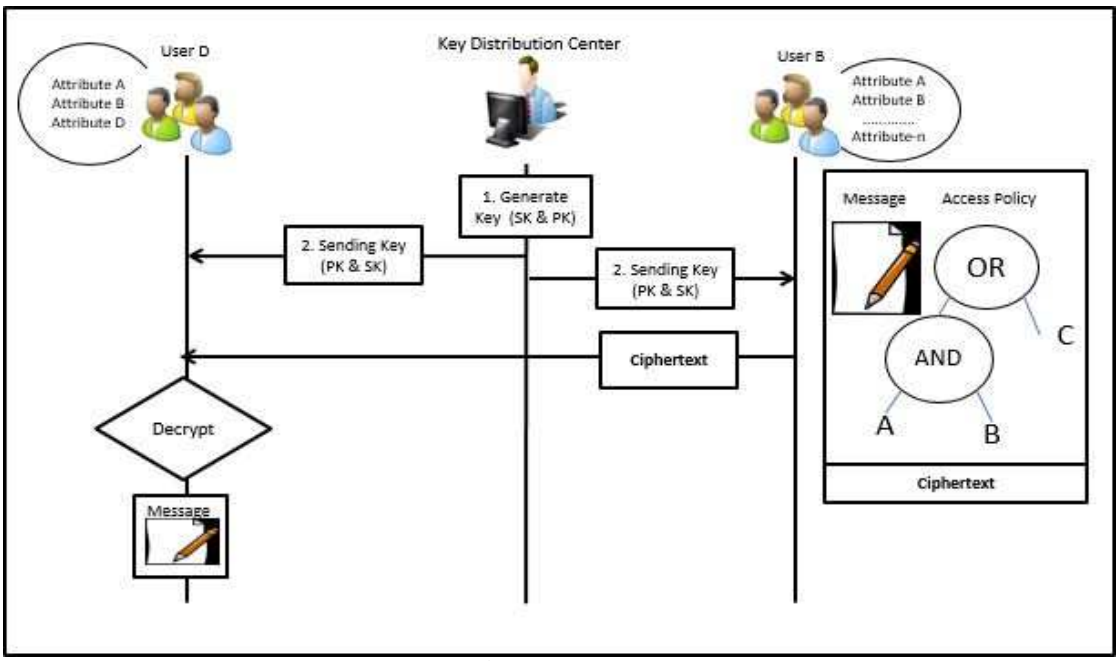


Fig. 1. Scheme of the original CP-ABE system.

B. Ciphertext Attribute-Base Encryption with Revocation Scheme

In scheme of CP-ABE with revocation, the system same with the original CP-ABE but the different is system add NOT logical in the rule of access policy. If the user in a revocation list, the attribute will be add NOT Logical in ciphertext like shown on Fig. 2 and Fig. 3. only user is not in revocation list can decrypt the original message.

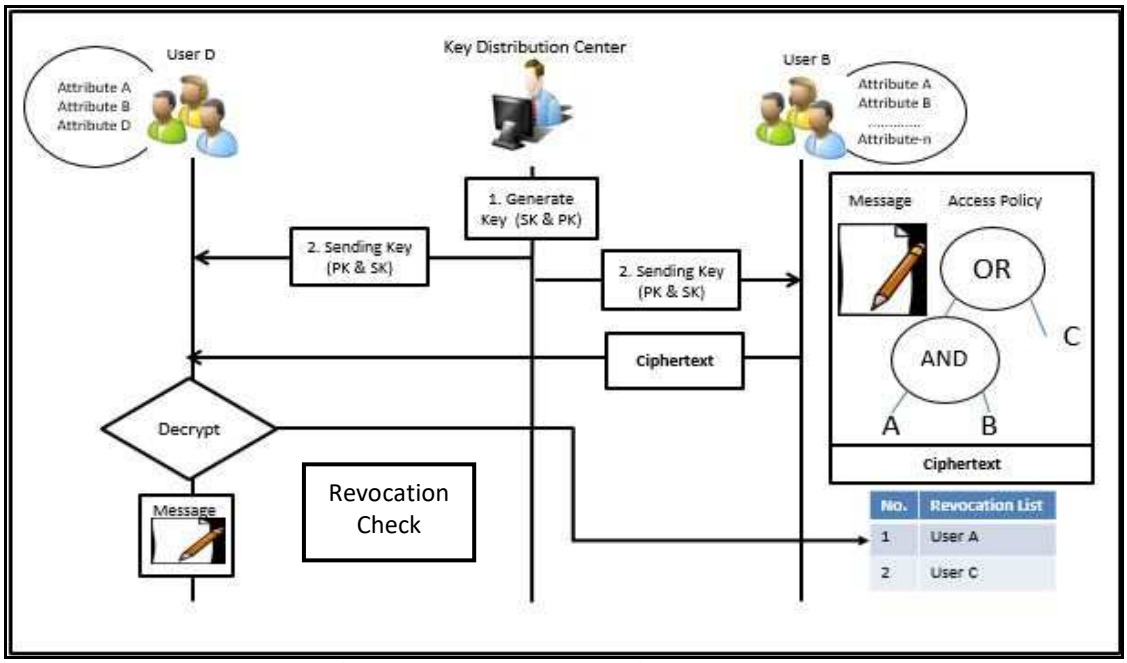


Fig. 2. Scheme of CP-ABE with revocation system for user is not in revocation list.

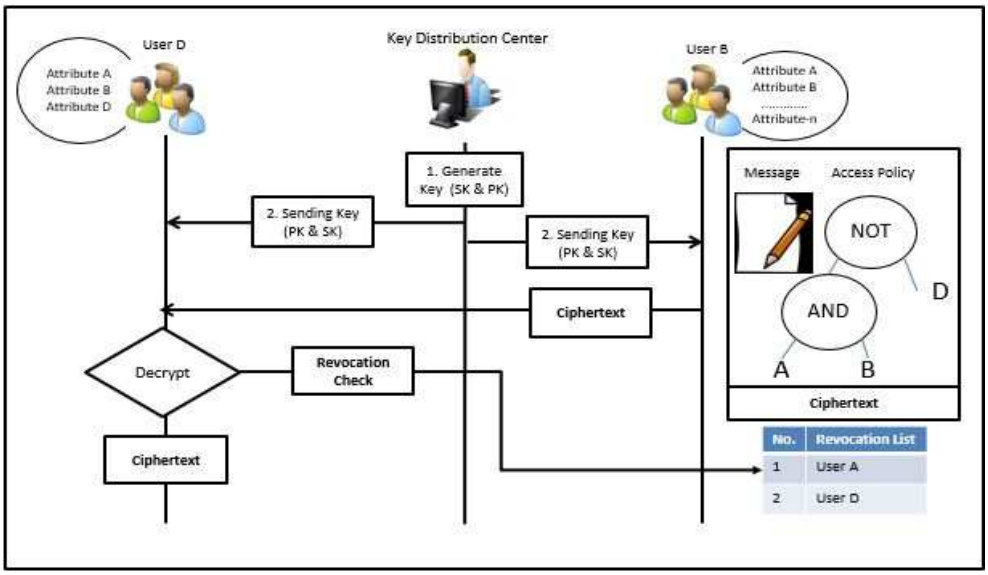


Fig. 3. . Scheme of CP-ABE with revocation system for user in revocation list.

In the CP-ABE scheme, there is four steps system such as: **Setup:** The system generate randomly output the master key (MK) and public key (PK) where MK is kept private. PK was sent to all user for encryption and decryption mechanism.

Keygen: The system generate the secret key (SK) use MK and PK and attributes of the user. The user requests to KDC by issued their attributes. KDC executed the system and generated SK and PK for the user.

Encryption: The system creates an original message (M) become a ciphertext (CT) using PK with user's parameters attribute. The system is performed by all participating users as an encryptor.

Decryption: On given CT and a secret key (SK) with the attributes of user, user who has matching to the attribute policy (T) associated with CT is able to recover the original message (M)proposed method cp-abe with user illegal access

We proposed our secure system in the scenario for the environmental monitoring system. We using 1 node with six sensors there is carbon monoxide, carbon dioxide, temperature, humidity, luminosity, and noise. Node sensor sends the sensor data using ZigBee to the meshlium, all of the data will be receipt by meshlium. Data in database meshlium we synchronize to the data center. In the data center, all of the data will be stored. To control the users who access the data, and secure the sensor data with illegal access to the data center of the environment monitoring system. We applied ciphertext policy attribute-based encryption with revocation to guarantee the confidentiality of the data, integrity, and user access rights. The system using HTTP protocol for all communication. The user can request data in the data center using end device such a smart phone, laptop and personal computer. The only user with access right can read the original data. the user without access right and in revocation list cannot read the original data from the data center. Fig 4. shows the proposed our system.

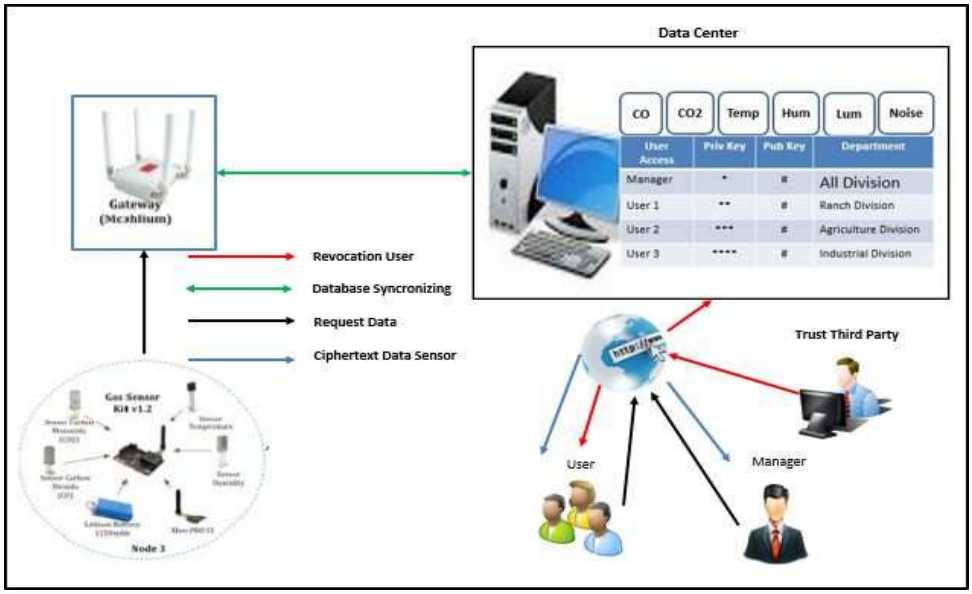


Fig. 4. system design secure data sensor in environmental monitoring using attribute-based encryption with revocation mechanism

User and manager make a registration with sending their identity, only to users, they select the attributes according to the field. Registered users and manager can request data to the data center through the HTTP protocol. The data center respond user's request before the original data send to the user. The data will be encrypted, after the data center finish encrypt the data, the ciphertext directly sends to the user's request. Trusted third party conducted a survey of users accessing illegally. If the trusted third party found the user conduct the illegal access, the trusted third party directly include in the revocation list. Users in the revocation list will never be able read the original data from the data center. We propose a CP-ABE to encrypt the data sensor in the data center. There are storing data such as temperature, humidity, CO, CO2, humidity, noise, and also the data from manager and users. User and manager can access the data from the data center through the web, where the data can be decrypted with the private key and the attributes that appropriate with access policies. We proposed the system with three actors such as Fig. 4.

Manager: a person who can decrypt all data. The manager is different from the users. The manager can access all data according to their access rights and send a message report to the third trust party for removing the user from revocation list.

User: a person who can only access the data according to their access right. The user only decrypts the data with the same policies with their attribute. The user who conducts the illegal access will be included in the revocation list.

Trust Third Party: a person trusted by the manager and user to confirm and enter the user into the revocation list.

Data Center: the storage media where the data sensor, user, and manager are stored. The other functions of the data center are doing the generation of the master, private, and public keys, where the private key and public key will be distributed to registered managers and users.

we design three protocols, those are a registration protocol, a sharing data protocol, and a revocation protocol:

1) *Registration Protocol*: Fig. 5 shows the flow of user registration, where the data center is generating master keys and public keys. Manager and user make registration by entering a username, password, and attribute. Registration is validated by a trust third party to be stored in the data center. Then, the data center will generate the key there is private key and public key. The key is distributed to the manager and users who have already done the registration. Registered users can use the key to decrypt the ciphertext form data center to read the original sensor data

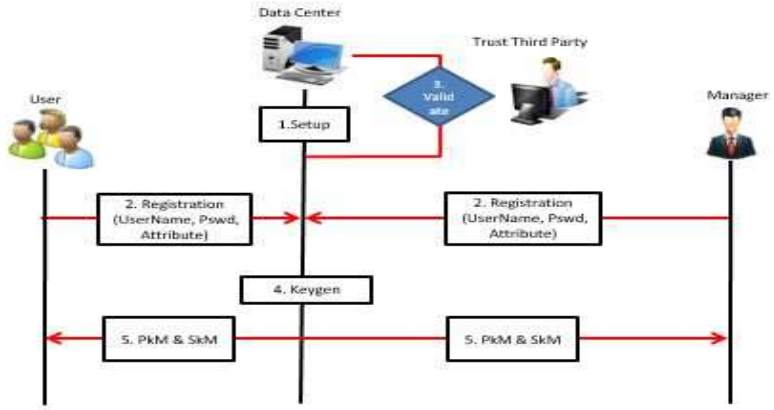


Fig. 5. Registration Protocol.

2) Data Sharing Protocol: Fig. 6 shows the flow of data sharing. The sensor data that is stored in the data center of the environment health monitoring are already encrypted before. The private key is needed to decrypt the data. In the previous registration protocol, we describe the mechanism how to get the key. After the manager and users get the key, they can download the ciphertext from data center and decrypt the ciphertext to read the original data sensor.

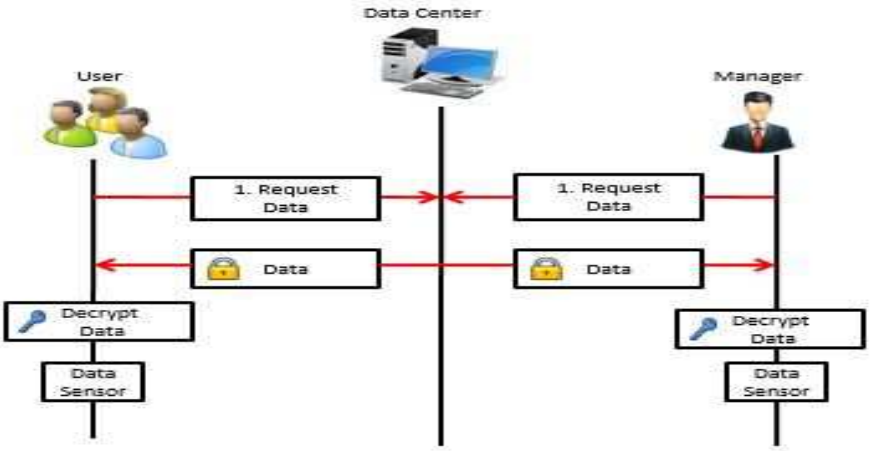


Fig. 6. Data Sharing Protocol.

3) *Revocation Protocol:* Fig. 7 shows the flow of user revocation who conducts illegal access. All the sensor data in the data center, that is previously encrypted, must be decrypted to completion in order to get the original data. To decrypt the data, the system requires the private key and attribute of the user. The user request to the data center, the data center responds and send the ciphertext sensor to download by users. User decrypts the ciphertext to read the original sensor data if the user cannot decrypt the ciphertext. The system will be saved that users conduct the illegal access. Data from the user who conducts illegal access will be stored in the data center to be revoked. The user, who has entered the list of revocation, will not be able to decrypt the data, that they request from the data center. All the sensor data in the data center, that is previously encrypted, must be decrypted to completion in order to get the original data. To decrypt the data, the system requires the private key and attribute of the user.

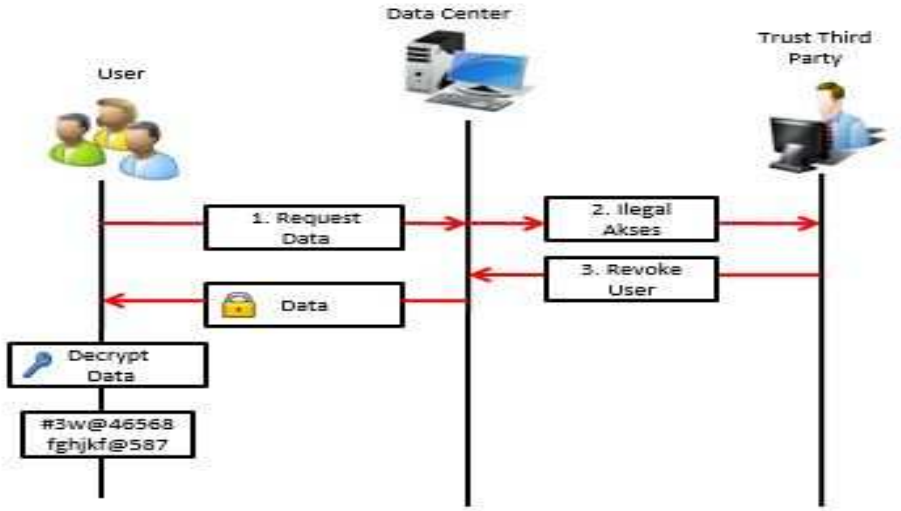


Fig. 7. Revocation Protocol.

The data center of environment health monitoring has many sensor data like temperature, humidity, CO and CO2, and noise. To perform a decryption, we create an access rule into four groups, which its attributes (T) are adjusted from data access requirements in the data center. The groups are a Manager (D0), Ranch Division (D1), Agriculture Division (D2), and Industrial Division (D3). Whereas, the data access right group is divided into three. Those groups will be used for monitoring the illegal access by users, such as the C1 Division for CO and CO2, C2 for temperature and humidity, and C3 for luminosity and noise. We choose attributes from the user department to perform the data decryption. The group 1 with T1 can decrypt all data (manager). The group 2 with T2 only decrypts the data of C2 and C3. The group 3 with T3 only decrypts the data of C1 and C2. To revoke an access of users, we add "NOT" to the policy rule to remove the user access for data decryption. We combine attribute from user division and sensor data to create rule of policy from ciphertext to ensure that only users with appropriate attributes that can decrypt. The base of access policy permission is defined as fig. 5.

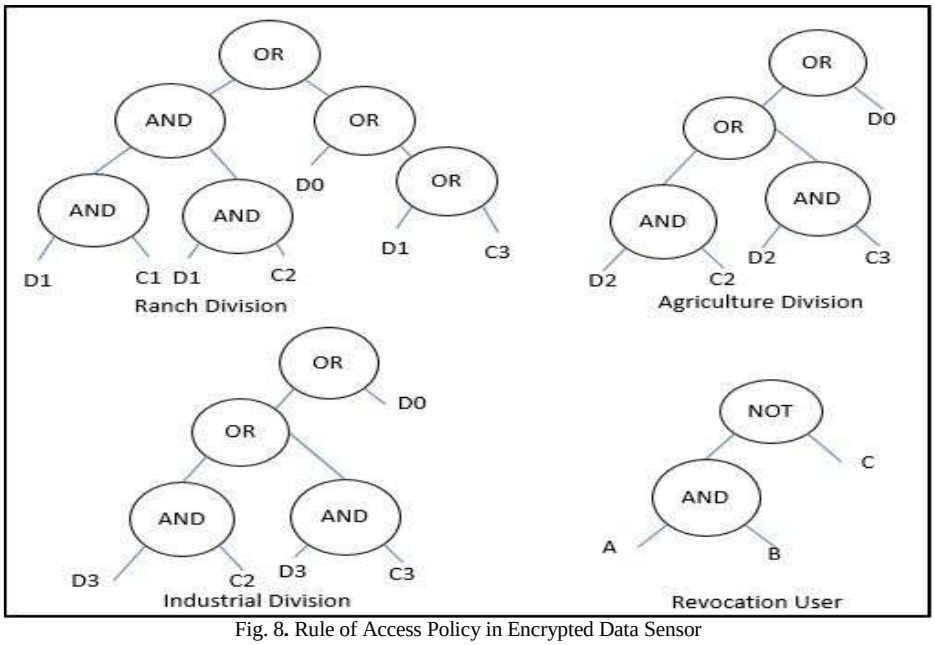


Fig. 8. Rule of Access Policy in Encrypted Data Sensor

We implement our system using Java server pages, where the communication between users, manager, and the data center uses HTTP with local area connection using wireless communication. For this system, we use a hardware device as seen in TABLE I below.

TABLE I
SPECIFICATION OF HARDWARE AND SOFTWARE

Actor	Details Hardware
Data Center	Intel Xeon CPU E3-1225 3.20GHz,4 GB DDR3, Dell Precision T1650
	Operating System
	Ubuntu Linux 16 kernel 4.4.0-22
	Software
	GMP-5.1.1, pbc-lib-0.5.14, glib-2.34, openssl-1.0.1e, net beans java 8, apache-tomcat-8.0.15. Mysql.
	Access Point TP-Link TL-WR740N IEEE 802.11n
Manager, User, and Trust Third Party	**Details Hardware**
	Intel core i3-3110M 2.4GHz, 4GB DDR3, Lenovo G400s
	Operating System
	Windows 10 64-bit
	Software
	Mozilla Firefox Browser-47

The data sensor, which previously stored as an encryption in the data center, will be downloaded by the user, and if it is downloaded by users who have the access right, then it will be decrypted. The data is downloaded by the users according to their access rights, if the existing rules in the policy are not appropriate with the user's attributes, then the ciphertext cannot be decrypted and its data is not readable. This makes the user be included in conducting illegal access, in which the data retrieval in the data center is not appropriate with their access right. The illegal access will be monitored by the third trust party. The user will directly be included in the revocation list.

The encrypted data can only be decrypted if only if the ciphertext qualifies with the already made rules and the owner's permission is appropriate. If the user accesses the data beyond their authority, the system will be saved that user did the illegal access, then the third trust party will directly put the user into the list of revocation as seen in Fig. 10. The data that has been encrypted before, called as a ciphertext (CT), only readable by decrypting it first, by using the private key and public key as well as the attributes of the user. The encrypted data is downloaded by the user by entering the private key if the rules are appropriate with the policies, and the user access is not included in the list of revocation, then the user can read the sensor data. In this system, the data is encrypted by using the access policy as seen in Fig. 9.

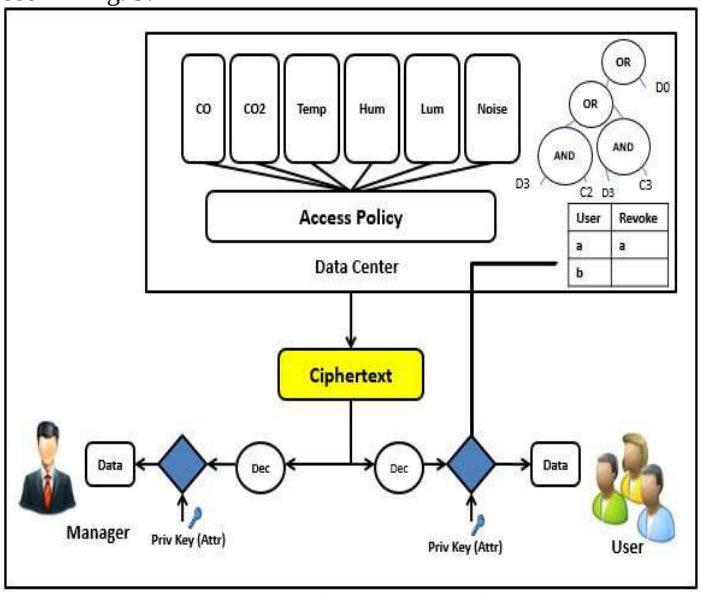


Fig. 9. Decryption process of ciphertext obtain from data center

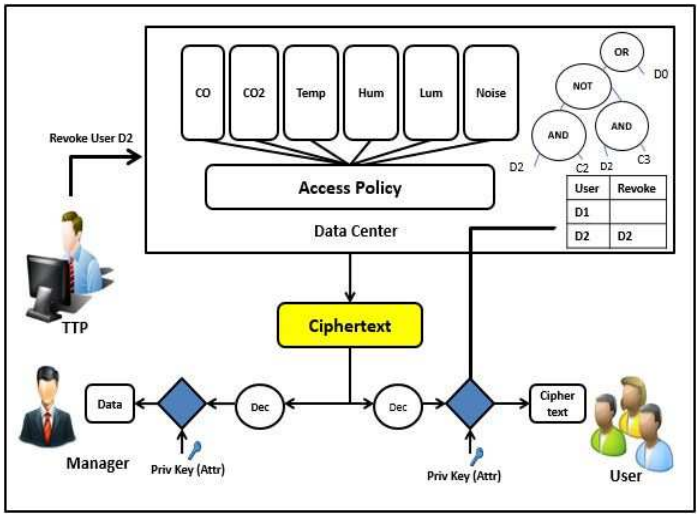


Fig. 10. Illegal access user process of data sensor stored in the data center

In Fig. 10 shows, the user did the illegal access, the user cannot decrypt and read the original data. the attribute from the user is not matched with the rule of policy from the ciphertext. What has been done by the user will be saved in databases from the data center? The trust third party will check users who did the illegal access to the system. If the trust third-party find the user performs the illegal access, the users will be saved in the revocation list, their attributes will be updated so that users will unable to decrypt the ciphertext. The user in revocation list cannot get the original data, if the user wants to get the original data, their id must be deleted from revocation list. The user in the revocation list can report their id to the manager if their id stored in the revocation list, the user can report their access by sending an information report (id.user) to the manager. The manager accepts the report from the user and sends it to the trust third party to remove the user from the revocation list. Then, the trust third party will perform a validation for messages from the manager. After trust third party did the validation, the trust third party removes the user from the revocation list.

Then, data center sends a message report to the user and then the user can access the data center and decrypt the ciphertext from the data center. Fig. 11 shows the flow of removing the user from revocation list.

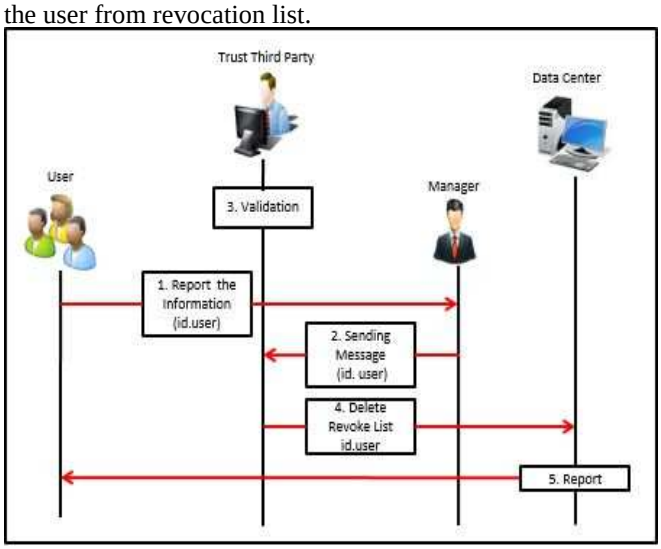


Fig. 11. User deletion process through revocation list

III. RESULTS AND DISCUSSION

The proposed system design is shown in Fig. 5. Where the manager and all users must register first, then the inputted data will be verified by the trust third party, after that the trust third party will generate the key (private key and public key). The key generated by the trust third party will be immediately sent to all users who was verified, we provide the link to register the user data and the link to download sensor data from data center, as seen in Fig. 12. Unregistered users can access the system but only view the current data from data center through the HTTP protocol using end device, they cannot download sensor data from the data center.

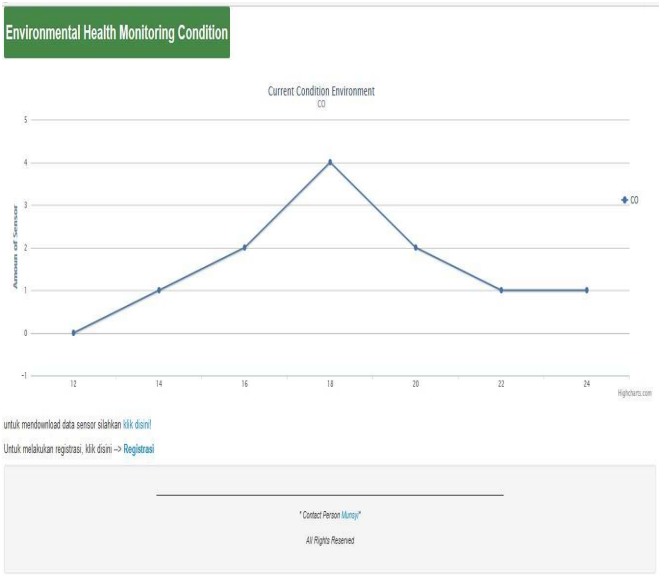


Fig. 12. initial appearance environmental conditions for users

In Fig. 13, for the user, we build the system by using laptop and for the data center, we use Linux Ubuntu. We use local area network transmission with a communication over an ethernet. The information of the user who already registered is stored in the data center and will be revoked if doing an illegal access.

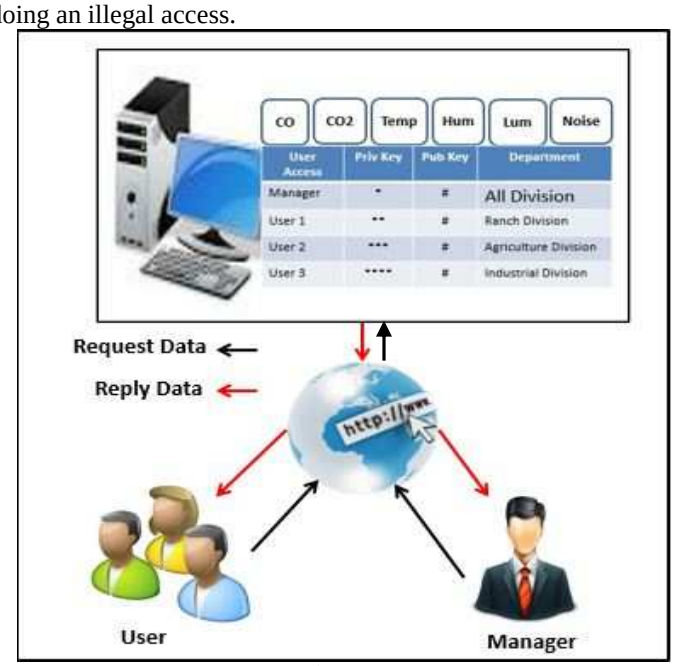


Fig. 13. Data sensor transmission from data center to user and managaer

In Fig. 14, we show how the user can get the sensor data, users enter the date for sensor data to be acquired, after the user entering the sensor data. the system will be process the user's request and provide a link to download the data. the sensor data will be encrypted by data center before user download the data, after the encrypt finished, the user can download the data in the form of ciphertext. The system of data encryption is using public key and attributes in accordance with the rule of policy from the user.

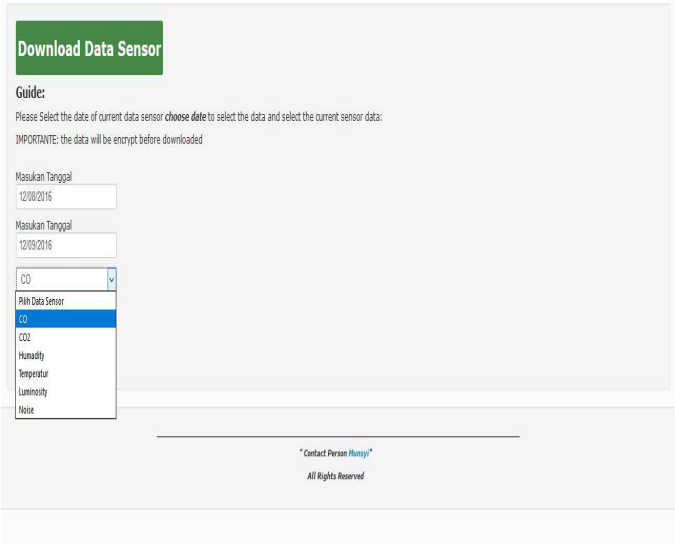


Fig. 14. Downloaded the encrypted data sensor

After the user downloads ciphertext of the data sensor from the data center, the user can access the system to get the plaintext of data sensor. The user can choose decryption menu in our system and then do the decryption. The user uploads a ciphertext to the system for decrypt ciphertext using their private key. If the attributes of user match with the access policies from the ciphertext, then the ciphertext

can be decrypted into a plaintext of the data sensor. In Fig. 15, we shows how to decrypt the ciphertext of the data sensor.

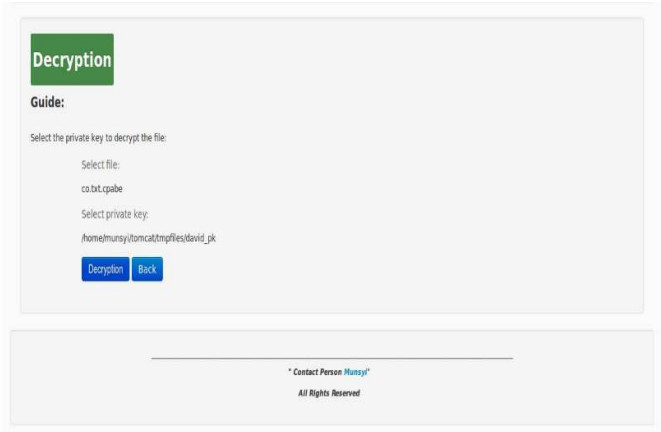


Fig. 15. Decryption of ciphertext data sensor

In Fig. 16, we show the user who conducts illegal access that will be directly included in the revocation list. Users who are included in the revocation list cannot decrypt the data, this is because the attributes of the user were updated by the trust third party, and the attribute from the user is not same with the rule of access policy of the ciphertext. The users who are not included in the revocation list can directly decrypt the ciphertext. In Fig. 17, the user with the access right can decrypt and get the sensor data. After the decryption is a success, the user can view the sensor data and get information from the data center.

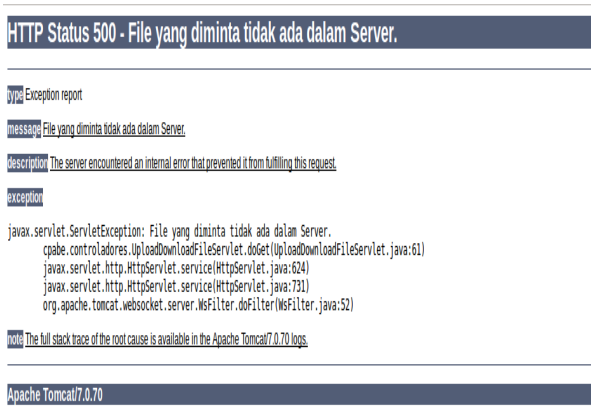


Fig. 16. Recovered data sensor failure

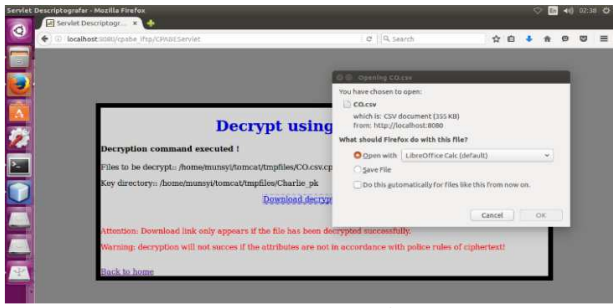


Fig. 17. Recovered data sensor after decryption

All of the sensor data in our project are different for every division (T1, T2, and T3), the original data in the data center has almost the different size. In this section we use the wireless sensor network with communication using zigbee to send the sensor data to meshlium. We synchronize database meshlium to the database in data center. We analyze the processing time for encrypt, decrypt and revocation check using different size of sensor data. we entered date from sensor data with different day such one day, one week and one month. User make a request to the data center with entering date from data sensor and choose the type of data sensor. The original data was encrypted by the data center before user download the data. The ciphertext with a variety of access policy for every division is different for T1, T2, and T3. We analyze the increase data from original data to ciphertext, between user with access right and user in revocation list , the different size of ciphertext data sensor between user and user in revocation can be seen in Table II and Table III.

TABLE II
SIZE OF DATA SENSOR AFTER ENCRYPTED FROM ORIGINAL DATA TO CIPHERTEXT USER WITH ACCESS RIGHT

T	Sensor	Original Data (KB)			Ciphertext User with Access Right (KB)		
		1 Day	1 Week	1 Month	1 Day	1 Week	1 Month
T1	CO	22	112,6	363,8	22,6	113,2	364,4
	CO2	27,1	138,6	447,8	27,7	139,1	448,3
	TEMP	25,4	129,9	419,8	26	130,5	420,4
	HUM	27,1	138,6	447,8	27,7	139,1	448,3
	LUM	20,3	103,9	335,8	20,9	104,5	336,4
	NOISE	21,3	104,9	337,8	21,9	105,5	338,5
T2	TEMP	25,4	129,9	419,8	25,6	130,2	420,1
	HUM	27,1	138,6	447,8	27,7	139,1	448,3
	LUM	20,3	103,9	335,8	20,7	104,4	336,2
	NOISE	21,3	104,9	337,8	21,7	105,2	338,3
T3	CO	22	112,6	363,8	22,6	113,2	364,4
	CO2	27,1	138,6	447,8	27,7	139,1	448,3
	TEMP	25,4	129,9	419,8	26	130,5	420,4
	HUM	27,1	138,6	447,8	27,7	139,1	448,3

TABLE III
SIZE OF DATA SENSOR AFTER ENCRYPTED FROM ORIGINAL DATA TO CIPHERTEXT USER IN REVOCATION LIST

T	Sensor	Original Data (KB)			Ciphertext User in Revocation List (KB)		
		1 Day	1 Week	1 Month	1 Day	1 Week	1 Month
T1	CO	22	112,6	363,8	23	113,4	368,4
	CO2	27,1	138,6	447,8	28,2	139,6	448,8
	TEMP	25,4	129,9	419,8	26,2	130,8	421,2
	HUM	27,1	138,6	447,8	28,1	139,4	448,8
	LUM	20,3	103,9	335,8	21,2	104,8	336,7
	NOISE	21,3	104,9	337,8	22	105,8	338,9
T2	TEMP	25,4	129,9	419,8	25,9	130,7	420,8
	HUM	27,1	138,6	447,8	27,9	139,5	448,8
	LUM	20,3	103,9	335,8	20,9	104,8	336,9
	NOISE	21,3	104,9	337,8	21,8	105,4	338,7
T3	CO	22	112,6	363,8	22,9	113,8	364,6
	CO2	27,1	138,6	447,8	27,9	139,5	448,5
	TEMP	25,4	129,9	419,8	26,2	130,8	420,7
	HUM	27,1	138,6	447,8	27,9	139,3	448,6

We analyze time processing from user with the access right and user in the revocation list such time processing for encrypt, decrypt and transmission time. We tried with each group of the user and all of sensor with the different days such 1 day, 1 week, and 1 month with different rule of policy (T).

In Fig. 18 shows the processing time for encrypt the original data to ciphertext with different grub policy and all of data sensor for 1 day between user in revocation list and user with access right. For T1 to encrypt the data sensor the system requires less than 160 ms for user in revocation list and less than 155 ms for user with access right, for T2 the system requires less than 152 ms for user in revocation list and less than 148 ms for user with access right and for T3 less than 149 ms for user in revocation list and less than 146 ms for user with access right.

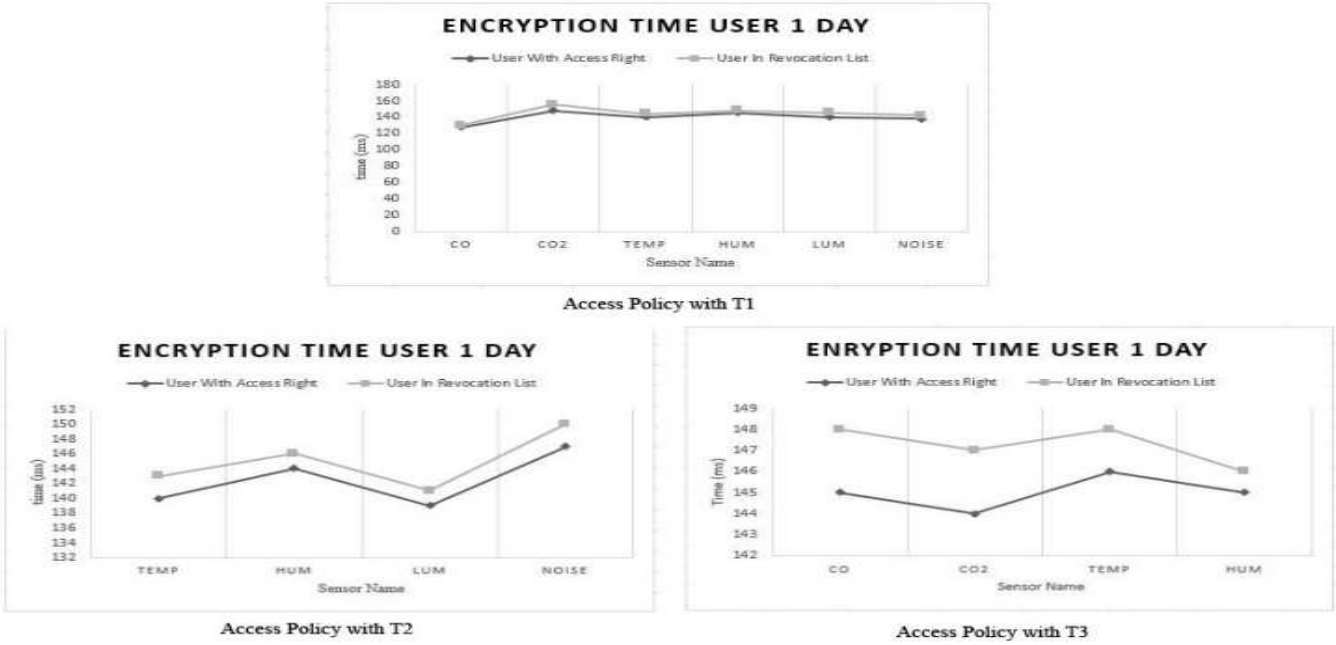
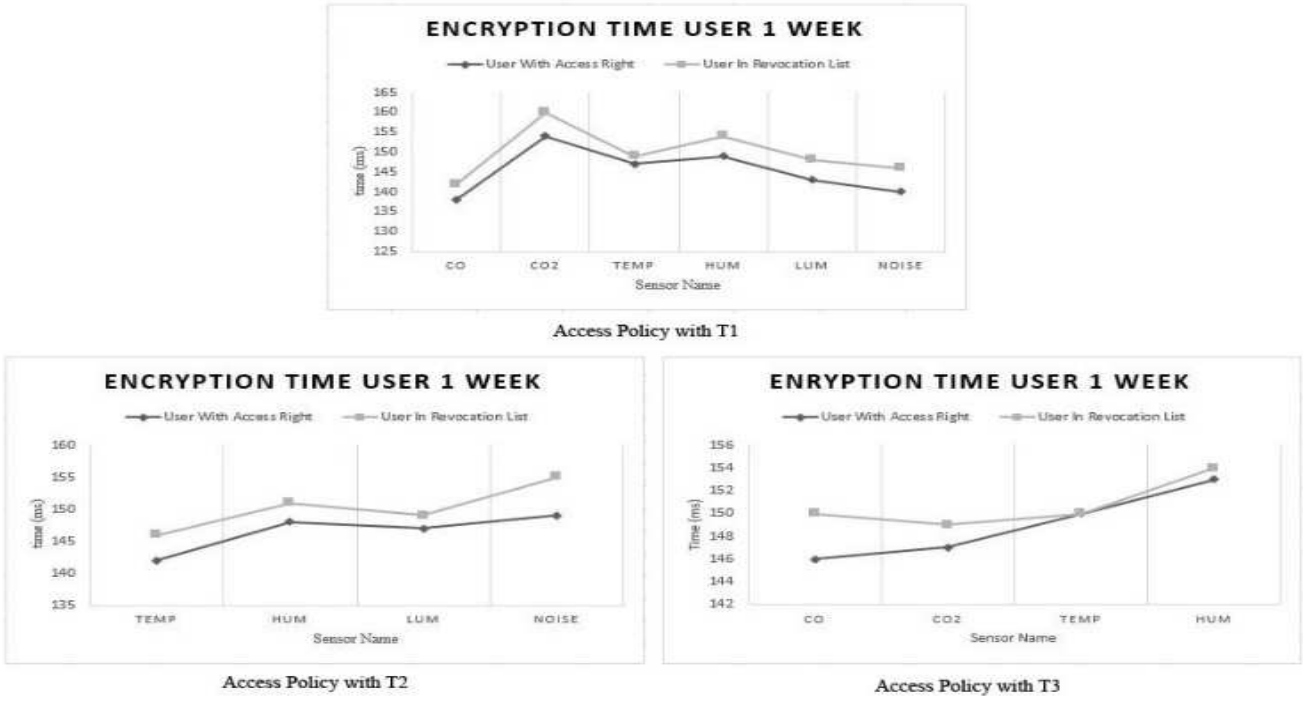


Fig. 18. Processing time encryption data sensor for 1 day

In Fig. 19 shows the processing time for encrypt the original data sensor to ciphertext with different grub policy and all of data sensor for 1 week between user in revocation list and user with access right. For T1 to encrypt the data sensor the system requires less than 165 ms for user in revocation list and less than 155 ms for user with access right, for T2 the system requires less than 160 ms for user in revocation list and less than 148 ms for user with access right and for T3 less than 156 ms for user in revocation list and less than 154 ms for user with access right.



.

Fig. 19. Processing time encryption data sensor for 1 week

In Fig. 20 shows the processing time for encrypt the original data sensor to ciphertext with different grub policy and all of data sensor for 1 month. For T1 to encrypt the data sensor the system requires less than 165 ms for user in revocation list and less than 155 ms for user with access right, for T2 the system requires less than 160 ms for user in revocation list and less than 148 ms for user with access right and for T3 less than 156 ms for user in revocation list and less than 154 ms for user with access right.

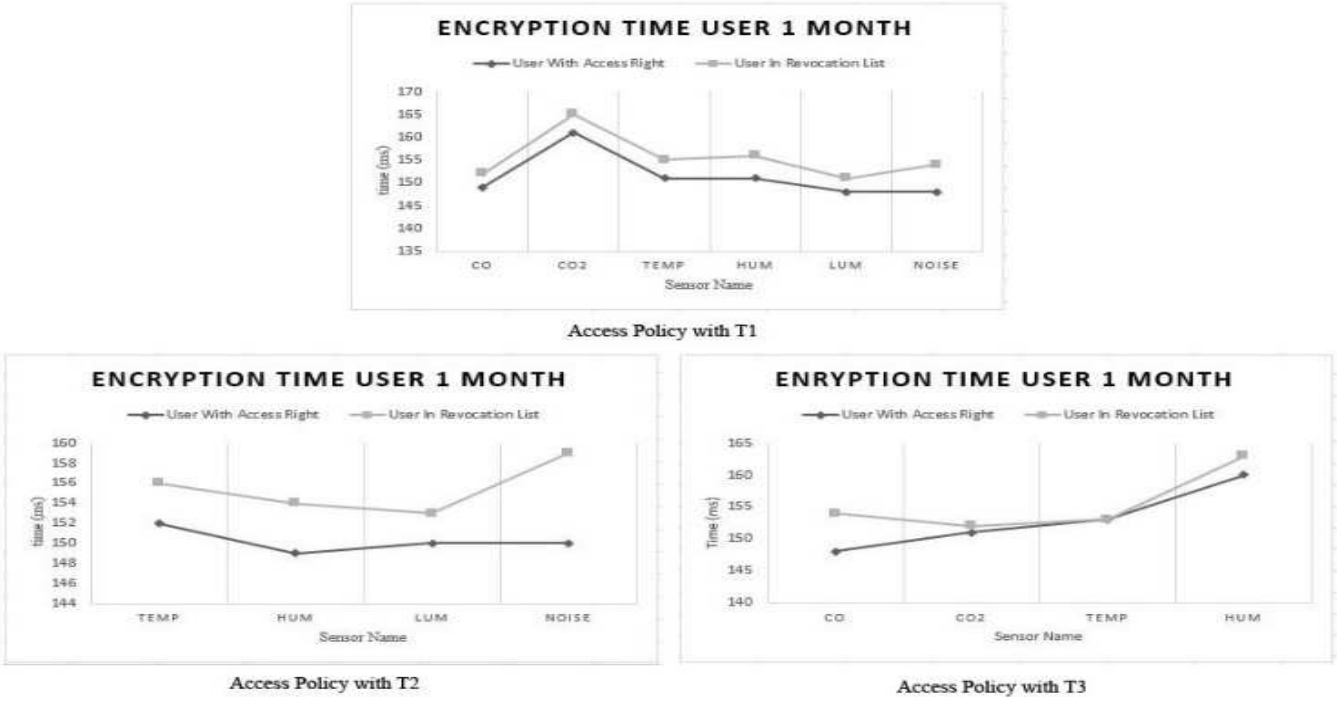


Fig. 20. Processing time encryption data sensor for 1 month

In Fig. 21 shows the processing time for decrypt the ciphertext to original data sensor with different grub policy and all of data sensor for 1 day. For T1 to decrypt the data sensor the system requires less than 130 ms for user in revocation list and less than 150 ms for user with access right, for T2 the system requires less than 135 ms for user in revocation list and less than 145 ms for user with access right and T3 less than 132 ms for user in revocation list and less than 140 ms for user with access right.

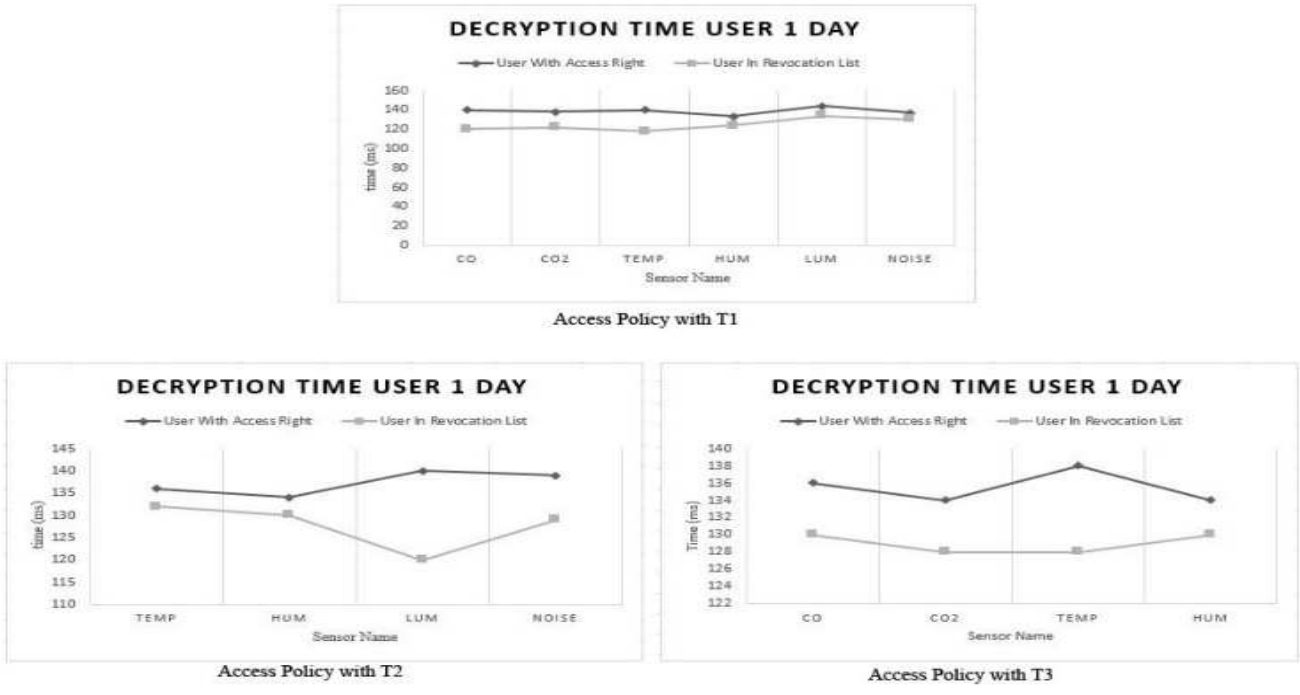
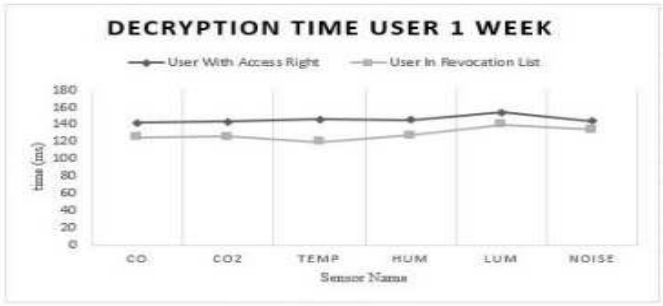


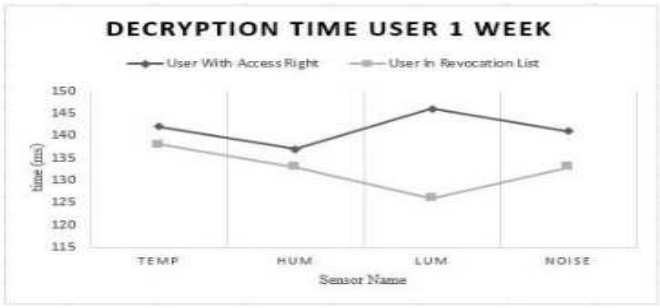
Fig. 21. Processing time decryption data sensor for 1 day

In Fig. 22 shows the processing time for decrypt the ciphertext to original data sensor with different grub policy and all of data sensor for 1 week. For T1 to decrypt the data sensor the system requires less than 140 ms for user in revocation list and less than 160 ms for user with access right, for T2 the system requires less than 140 ms for user in revocation list and less than 150 ms for user with access right and T3 less than 136 ms for user in revocation list and less than 142 ms for user with access right

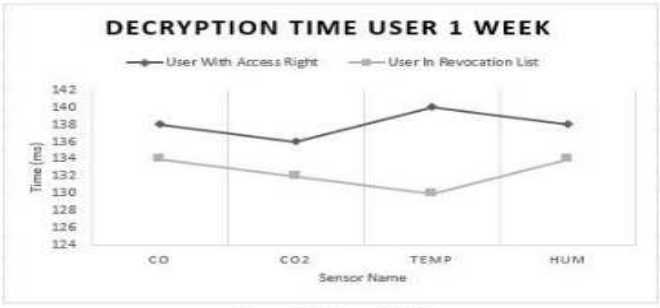
.



Access Policy with T1



Access Policy with T2

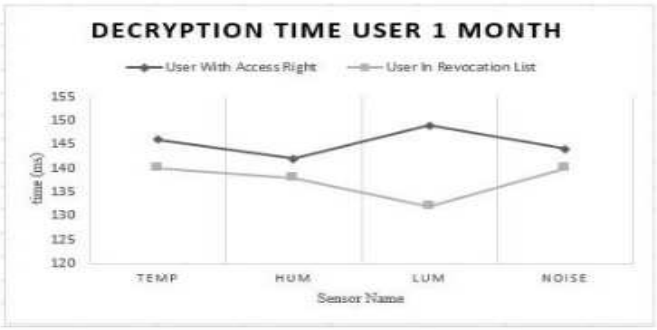


Access Policy with T3

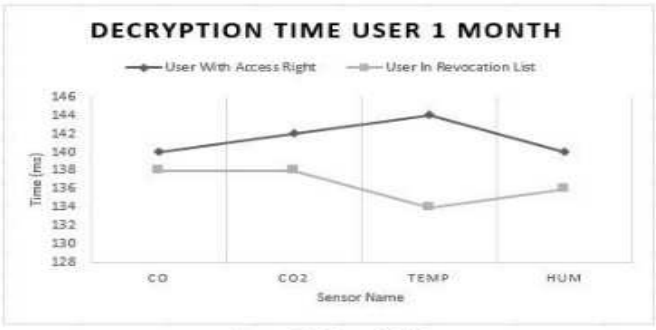
Fig. 22. Processing time decryption data sensor for 1 week

In Fig. 23 shows the processing time for decrypt the ciphertext to original data sensor with different grub policy and all of data sensor for 1 month. For T1 to decrypt the data sensor the system requires less than 145 ms for user in revocation list and less than 160 ms for user with access right, for T2 the system requires less than 145 ms for user in revocation list and less than 150 ms for user with access right and T3 less than 140 ms for user in revocation list and less than 146 ms for user with access right.

Access Policy with T1



Access Policy with T2



Access Policy with T3

Fig. 23. Processing time decryption data sensor for 1 month

in this section we analyze time processing for transmission data with the diffent grub policy and all of data sensor for 1 day, 1 week and 1 month between user with access right and user in revocation list. Fig. 24, Fig 25 and Fig. 26 shows the transmission data.

In Fig. 24 shows the transmission time for transmission data with different grub policy and all of data sensor for 1 day. For T1 the transmission time requires less than 160 ms for user in revocation list and less than 170 ms for user with access right, for T2 the system requires less than 165 ms for user in revocation list and less than 170 ms for user with access right and T3 less than 160 ms for user in revocation list and less than 170 ms for user with access right.

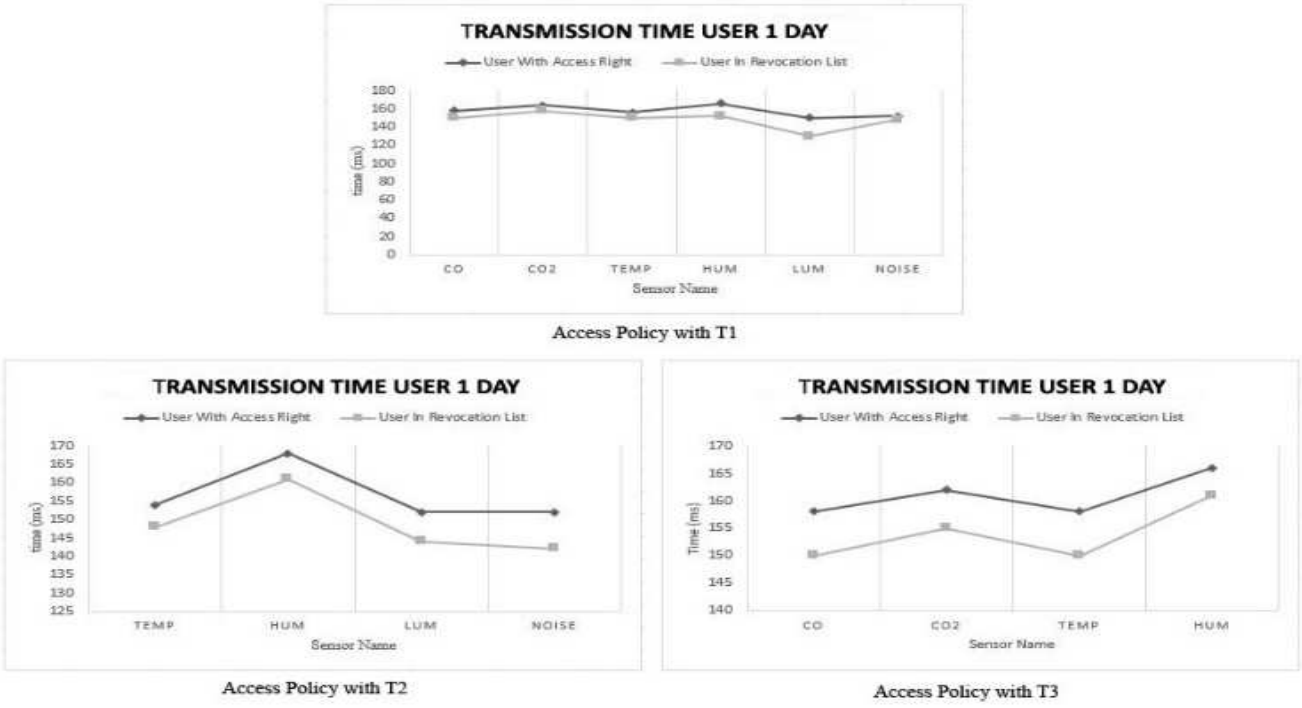


Fig. 24. Processing time transmission data sensor for 1 day

In Fig. 25 shows the transmission time for transmission data with different grub policy and all of data sensor for 1 week. For T1 the transmission time requires less than 160 ms for user in revocation list and less than 180 ms for user with access right, for T2 the system requires less than 165 ms for user in revocation list and less than 175 ms for user with access right and T3 less than 170 ms for user in revocation list and less than 175 ms for user with access right.

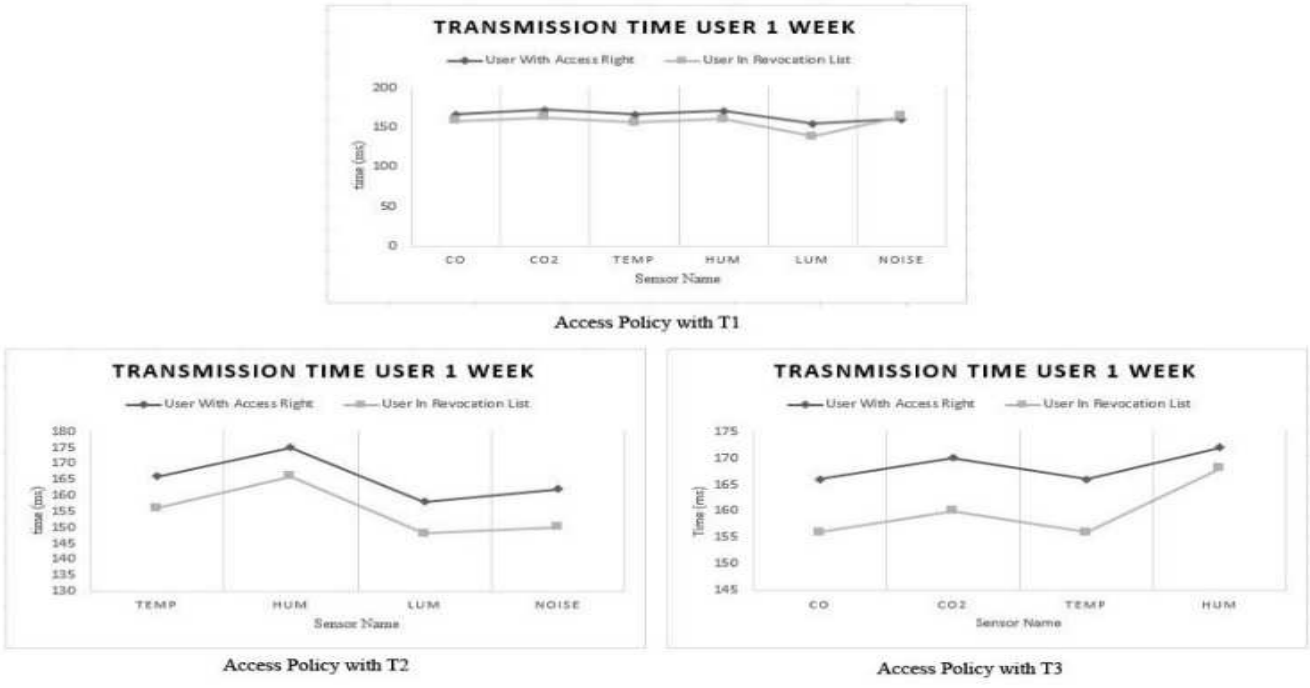


Fig. 25. Processing time transmission data sensor for 1 week

In Fig. 26 shows the transmission time for transmission data with different grub policy and all of data sensor for 1 month. For T1 the transmission time requires less than 160 ms for user in revocation list and less than 180 ms for user with access right, for T2 the system requires less than 170 ms for user in revocation list and less than 185 ms for user with access right and T3 less than 180 ms for user in revocation list and less than 190 ms for user with access right.

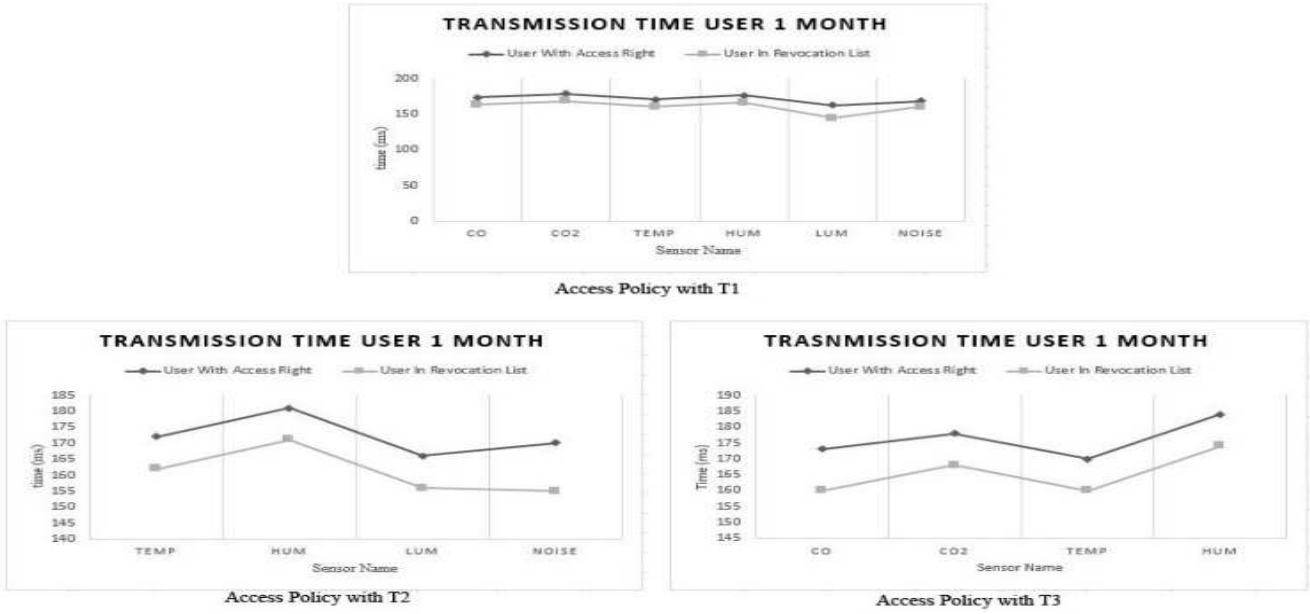


Fig. 26. Processing time transmission data sensor for 1 month

We also analyze the transmission time for our system if the user using Raspberry, in our research we are using Raspberry Pi3 model B with 1.2 GHz 64-bit quad-core ARMv8 and 1 GB RAM with 802.11n wireless for showing our system can be used in embedded system. In Fig. 27 shows the transmission time for transmission data with different grub policy and all of data sensor for 1 day. For T1 the transmission time requires less than 160 ms for user in revocation list and less than 270 ms for user with access right, for T2 the system requires less than 165 ms for user in revocation list and less than 250 ms for user with access right and T3 less than 170 ms for user in revocation list and less than 280 ms for user with access right.

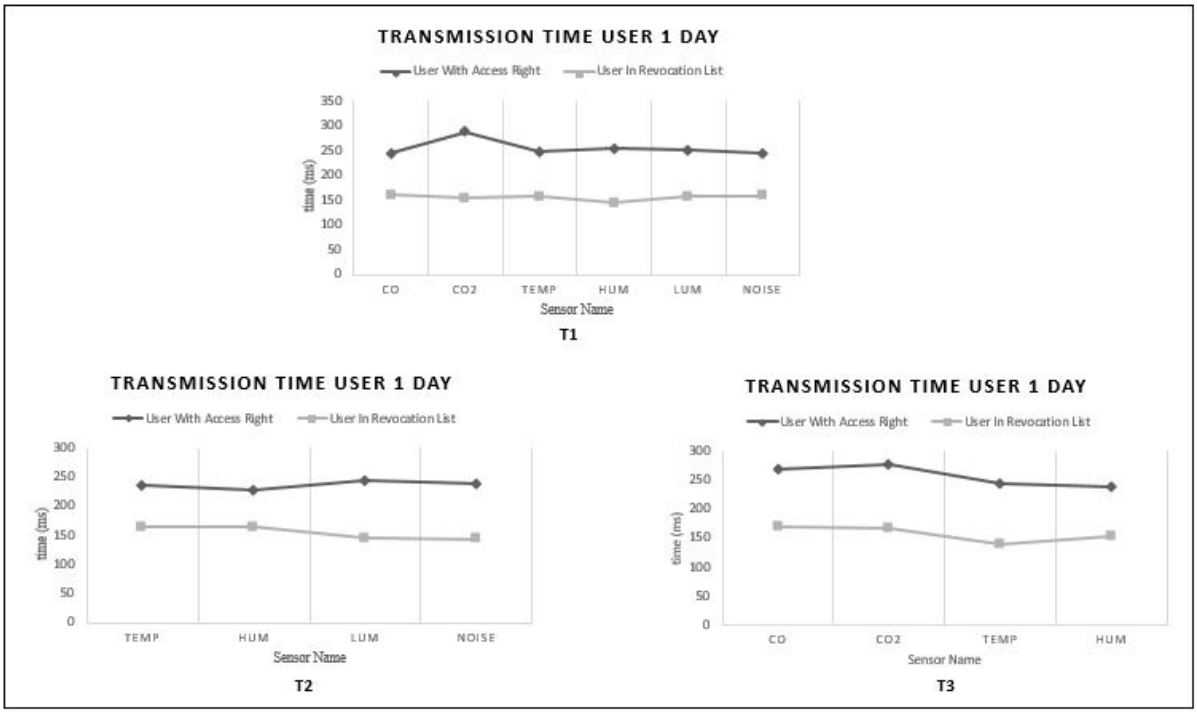


Fig. 27. Processing time transmission data sensor for 1 day

In Fig. 28 shows the transmission time for transmission data with different grub policy and all of data sensor for 1 week. For T1 the transmission time requires less than 165 ms for user in revocation list and less than 285 ms for user with access right, for T2 the system requires less than 160 ms for user in revocation list and less than 280 ms for user with access right and T3 less than 165 ms for user in revocation list and less than 270 ms for user with access right.

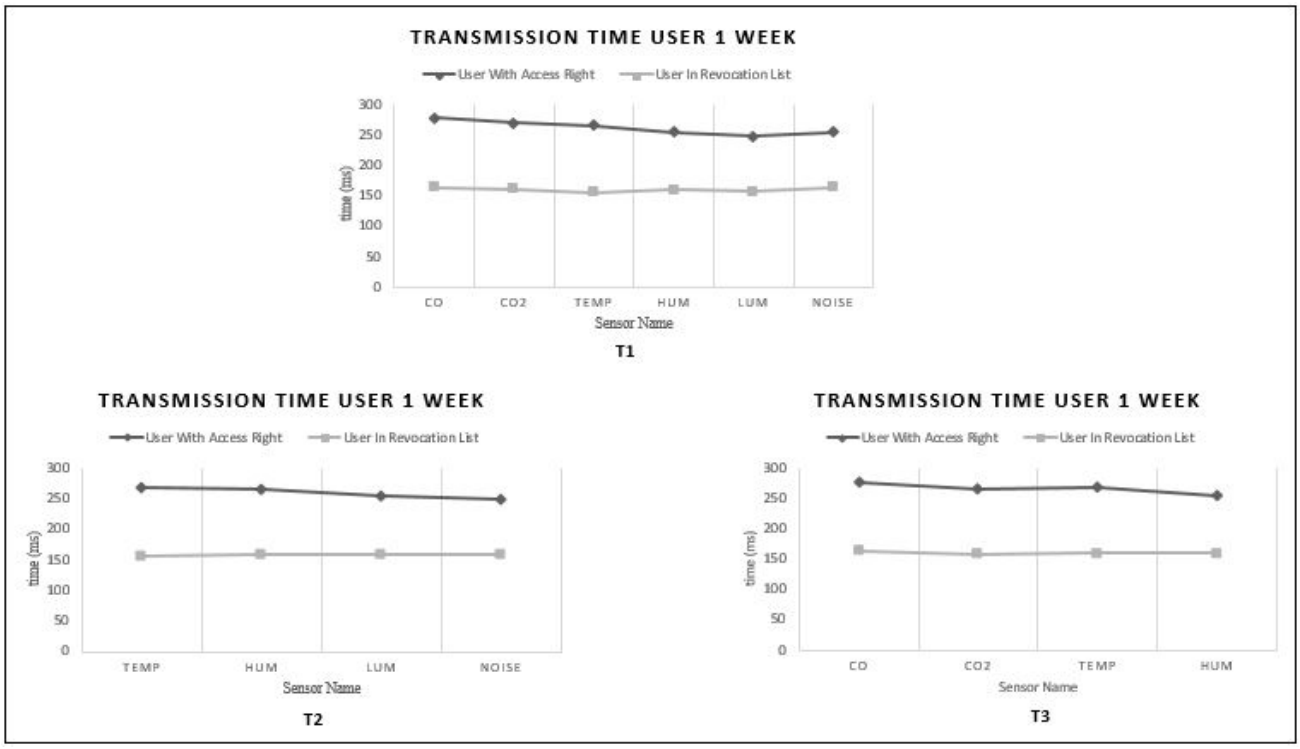


Fig. 28. Processing time transmission data sensor for 1 week

In Fig. 29 shows the transmission time for transmission data with different grub policy and all of data sensor for 1 month. For T1 the transmission time requires less than 170 ms for user in revocation list and less than 320 ms for user with access right, for T2 the system requires less than 160 ms for user in revocation list and less than 300 ms for user with access right and T3 less than 160 ms for user in revocation list and less than 340 ms for user with access right.

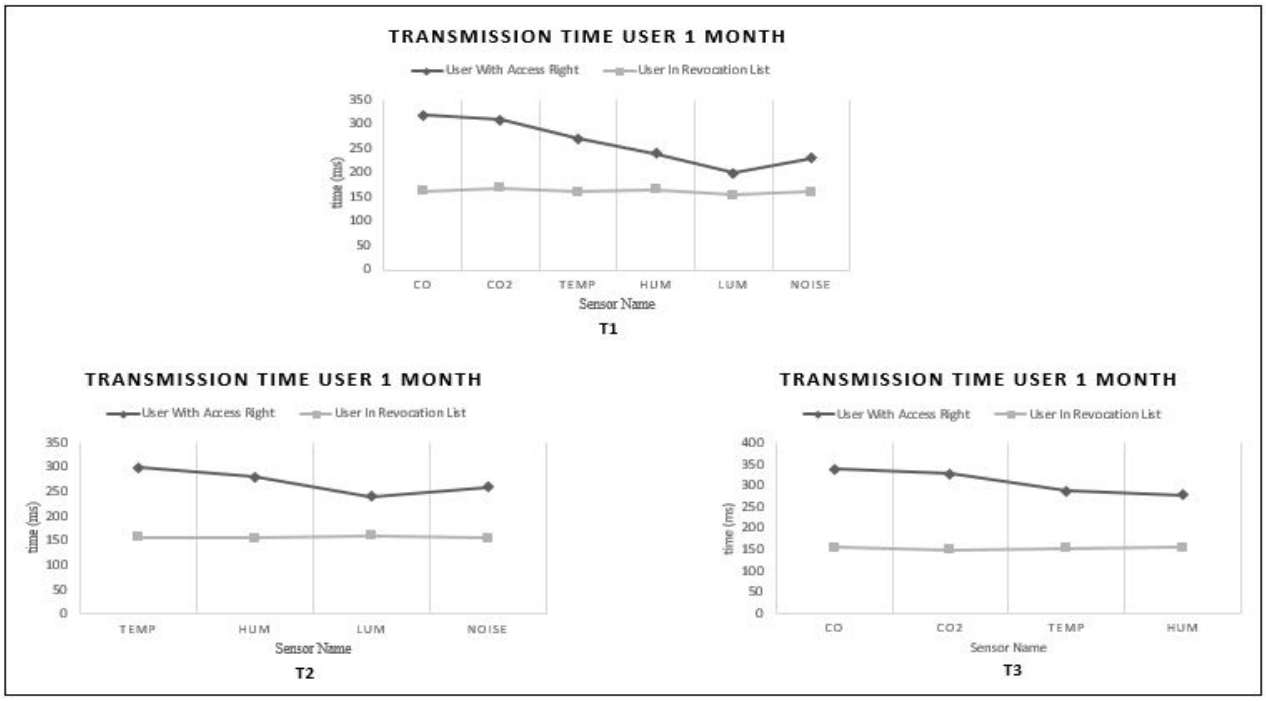


Fig. 29. Processing time transmission data sensor for 1 month

Fig. 30 shows the processing time for the revocation check with the number of users around 10 up to 1000 users. We analyze for 1000 revoked users there are only 2 second processing time for revocation check.

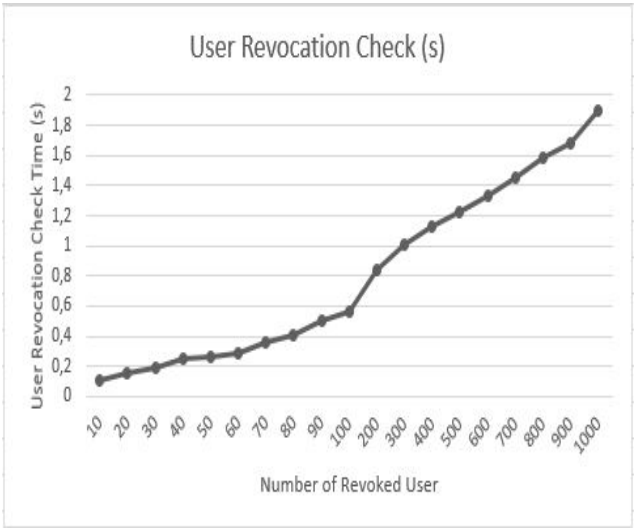


Fig. 30. Processing time for revocation check with 1000 user revoked

IV. CONCLUSIONS

We added a retraction on the method of CP-ABE to strengthen security for users who perform illegal access and protect the security of the system from the user is not responsible. Our revoke scheme do not affect the performance of the system from the data center environment health monitoring. The revocation list can only be accessed by the trust third party that is trusted by the manager and the user to perform monitoring and validation. Our experimental results showed the system requires less than 170 ms for the user with access right to encrypt the data for one month and requires less than160 ms to decrypt the data with 190 ms for transmission time. Compared with the user in revocation list with the same encryption time but requires the longer time for decrypt the data. to encrypt the data for one month user in revocation list requires less than 180 ms, for decrypt the data, user in revocation list requires less than 150 ms with 170 ms for transmission time. In embedded system our performance system only need less than 280 ms for transmission time for 1 Day, 285 ms for 1 week and also less than 290 ms for 1 month. Our experimental also showed time for the revocation check with amount 1000 users. The system requires less than 2 s for checking 1000 users. Our system with trust third party can control all of user in the data center from the illegal access, only third trust party can include the user to the revocation list and remove the user in the revocation list.

Our future work is including the digital time stamp signature to the messages sent by the manager to perform monitoring for the active user and add validity of the data from the data center and ensure there are no changes during the process of transmission data.

REFERENCES

[1] A.Sudarsono, M.U.H. Al Rasyid, An Anonymous Authentication System in Wireless Networks Using Verifier-Local Revocation Group Signature Scheme. International Seminar on Intelligent Technology and Its Application Technology, pp. 49-54, 2016.

[2] M.U.H. Al Rasyid, Bih-Hwang Lee, A.Sudarsono, and Taufiqurrahman, Implementation of Body Temperature and Pulseoximeter Sensors for Wireless Body Area Network. Sensors and Materials, International Journal on Sensor Technology. 27(8), pp. 727-732, 2015.

[3] S.Huda, A.Sudarsono, and T.Harsono, Secure Communication and Information Exchange using Authenticated Ciphertext Policy Attribute-Based Encryption in Mobile Ad-hoc Network. EMITTER International Journal of Engineering Technology, Vol. 4, No.1 , pp. 115-140, 2016.

[4] M.F.Othmana, K.Shazali, Wireless Sensor Network Applications: A Study in Environment Monitoring System. International Symposium on Robotics and Intelligent Sensors 2012 (IR IS 2012), pp. 1204 – 1210, 2012.

[5] Nurul Fahmi, M. Udin Harun Al Rasyid, Amang Sudarsono. Adaptive Schedulling for Health Monitoring System Based on the IEEE 802.15.4 Sleep Standart. EMITTER International Journal of Engineering Technology, Vol. 4, No.1 , pp. 91-114, 2016.

[6] J.Bethencourt, A.Sahai, and B.Waters, Ciphertext-policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy. pp. 321-334, 2007.

[7] J.Benthencourt, A.Sahai, and B.Waters. cpabe toolkit in advanced Crypto Software Collection.[Online].From:http://hms.isi.jhu.edu/acsc/cpabe. [accessed on Oktober 2015].

[8] B.Lynn. PBC (Pairing-Based Cryptography) library. [Online]. From: http://crypto.stanford.edu/pbc. [accessed on Oktober 2015].

[9] S. Roy, M. Chuah. Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs. Journal of Cryptology, vol. 17, No.4, pp.297-319,2004.

[10] Samsul Huda, Nurul Fahmi, Amang Sudarsono, and M. Udin Harun Al Rasyid, "Secure Data Sensor Sharing on Ubiquitous Environmental Health Monitoring Application", Jurnal Teknologi (Sciences & Engineering) 78:6-3 (2016), pp. 53-58, 2016.

[11] J.H. Chen, Y.T.Wang, and K. Chen, Attribute-Based Key-Insulated Encryption, Journal of Information Science and Engineering, Vol.27, pp. 437–449, 2011.

[12] W. Stalling, Network Security Essentials: Applications and Standards, Prentice Hall Press, 4th edition, ISBN-13: 978-0136108054, 2010.

[13] J.H. Chen, Y.T.Wang, and K. Chen, Attribute-Based Key-Insulated Encryption,Journal of Information Science and Engineering, Vol.27, pp.437-449, 2011.

[14] H. Kwon, D. Kim, C. Hahn, and J. Hur, Secure Authentication using Ciphertext Policy Attribute-Based Encryption in Mobile Multi-hop Networks,Multimedia Tools and Applications, pp.1-15, 2016.

[15] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,"Mediated Ciphertext-Policy Attribute-Based Encryption and ItsApplication," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.

[16] Koo, D., Hur, J., and Yoon, H. "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage.", Computers & Electrical Engineering, vol 39, no1, pp 34-46, 2013.

[17] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,"Proc. ACM Conf.Computer and Comm. Security, pp. 121-130, 2009.

[18] A. Lewko, A Sahai and B Waters, "Revocation Systems with Very Small Private Keys". IEEE Symposium on Security and Privacy 2010, pp. 273-285, 2010.

[19] L. Touati, Y. Challal and A. Bouabdallah, "Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things", Internationan Conference on Advanced Networking, Distributed System and Aplications. pp.64-69, 2014.