International Journal on Advanced Science Engineering Information Technology

Vol.8 (2018) No. 5
ISSN: 2088-5334

Secure Data Exchange Using Authenticated Attribute-Based Encdryption with Revocation for Environmental Monitoring

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

[#] *Politeknik Elektronika Negeri Surabaya PENS), Surabaya, Indonesia*

**Universitas Muhammadiyah Banjarmasin Banjarmasin, Indonesia*
E-mail: munsyi@politala.ac.id, {amang,udinharun}@pens.ac.id

***Abstract*— Internet of things grown very rapidly, one of them is application smartcity for monitoring the environment. The environmental monitoring use the wireless sensor networks (WSN) technology to collect all of the data. All the data collected by the WSN will be sotred in the Data Center, where all of the data in the Data Center can be accessed by the user everytime and everywhere. The data center without security mechanism is very dangerous because all of data can be tracked and even modified by the users. There are need security mechanism for securing the data and monitoring access from each user. Chipertext Policy Attribute Based-Encryption (CP-ABE) with Authentication and Revocation can become a solution for this problem, where all of data in the data center can be protected with encryption and decryption mechanism. Its jut not protect the data, the security will give a guarantee for originality in the data and can give a control access for user who did the illegal access. The user who did the illegal access will be revoked by the system. Our security mechanism using the CP-ABE and timestamp digital signature using Rivest, Shamir Adleman (RSA) 2048 does not affect to performance of the system.**

***Keywords*— environment monitoring; CP-ABE; authentication and revocation; timestamp digital signature RSA 2048.**

I. INTRODUCTION

Internet of things (IoT) grown very rapidly in this era. IoT make everyone can easy to get and collect the data everytime and everywhere. The environmental monitoring system is one of aplication from IoT where WSN technlogy developing rapidly in the current era, there is much research conducted by researchers in monitoring environmental conditions in a particular place by using wireless sensor network (WSN) technology [1][2][3][6]. WSN technology can be used to collect data information from an environmental condition, the data will be sent to the Data Center to be stored and used to determine the environmental conditions of a particular place. All users can access the data using existing devices such as laptops, computers, and smartphones. The previous researchers [1] using WSN technology by applying the real hardware in their research to get the information condition of an environment from a particular place. The data were obtained from WSN will be sent to the Data Center to store and use as information for users to obtain the information on environmental conditions in the area. In this research, the system did not use a security mechanism for all of the data. the users can access and get the data without security on the system.

In internet of things era, recently there are many researchers has been researched about the environmental monitoring system. Fahmi, et al. [5] their research developeda fuzzy logic for environmental health monitoring system through the WSN technology. The researcher using the real hardware with communication between the sensor node and the gateway use ZigBee 802.15.4 standard protocol. The researchers applied real hardware using Microcontroller ATMega 1281 and Sensor Board developed by Waspmote. All of data collected by the WSN will be sent and stored in the Data Center. The user can access the system using web based communication through the HTTP protocol.

An environmental system with the Data Center without security will be dangerous because user can intercept, tracked and even modified the data. The research for securing data andprotecting the original data from illegal access have many methods, for example. Sudarsono, et al. [6] build a security mechanism with the authentication system using pairing-based verifier-local revocation group signature. This scheme to authenticate wireless node of a particular privilege group to the gateway node in transmission data. This research use the real hardware using Raspberry Pi2, PC with Intel Core i7 2.60 GHz and Broadcom BCM43xx 1.0 with 4 GB RAM for the Data Center, 1.80 Ghz with 2 GB RAM and Intel Dual Band Wireless-N 7260 IEEE802.11

a/b/g/n for User, and using TP-Link TL-WN722N 150 Mbps IEEE802.11b/g/nfor the communication.

All of the data in the Data Center must be secured and the original of data have been protecting. The system without any security will be very dangerous because anyone can access, change all of data and send fake the data to other users. a security mechanism will be required to protect the data and ensure the authenticity of data during the sending process to user. In this case, CP-ABE [4] can be implemented to secure all of the data in the Data Center. Before the data will be sent to user, the data will be encrypted with policy rules that have been creating, then the system provides a security in the data. After the data encrypted and then the system will be generated a ciphertext. The ciphertext will be sent directly to the users. Users cannot be able to directly read the contents of the data, the ciphertext must be decrypted to get the original data. The user who want to decrypt the ciphertext use a private key to get the original data, If the attributes of the user is appropriate with rules of policy in the ciphertext then the decryption process will success and the user can read the contents of the received data, but if the attributes of the user does not appropriate with the rules of policy in the ciphertext then the decryption process will fail.

In the previous research [8]. The researcher use the digital signature with RSA to enhance the data security of cloud in Cloud Computing. For providing the security system and to enhance the data security in the Data Center need the encryption process for the data in the system. To avoid for sending data from fake Data Center and replaying data transmission then the system provides warranty that the data was sending is original and can be done a proof.

In our previous work [5][7] we construct the security mechanism system to protect all of data in the Data Center. We use CP-ABE with revocation mechanism to revoked the user who did the illegal access to the system. All of the data was storing in the Data Center will be secured with encryption using CP-ABE where the data requested by the user will be encrypted to become a ciphertext before sent to the user. We create the rules policy in ciphertext to the user in the revocation list. Users in the revocation list cannot accomplish of decryption process because the attributes from users in the revocation list was updating in the system. We make in the system for user with the access right and not include in the revocation list can get the original data. Our previous work, there is still a weakness of the security mechanism that is on the authentication for integrity of the data. For solving this issues we use the timestamp digital signature with RSA 2048 to construct and provide the data integrity has been sent to the users [5]. Our preivious work [11] we developt the security mechanism with validation for the data after process decription success. Using RSA 2048 for signing timestamp in the data from the Data Center to give the guarantee for originality of the data who received by the user. We adopted CP-ABE with revocation and construct a mechanism to validate the authentication of the data. The data received by the user is assured of its authenticity and the data can not be denied by the Data Center. the system with using the timestamp digital signataure feature provides security from replay attack in the Data Center, because the different time for sending a message will result in different validation values.

Structure organization in this paper as follows. In Section 2, we explain our related work from previous researcher in Internet of Things using wireless sensor network and about security mechanism from our previous work. In Section 3 we present the experiment result and measurement. In Section 4 we describe the conclusion from the security mechanism in our systems.

II. Material and Method

In this section we describe our adopted method CP-ABE and our method using Authenticated Ciphertext Policy Attiribute-Based Encryption with RSA 2048. The different process can seen in Fig. 1 and Fig. 2.

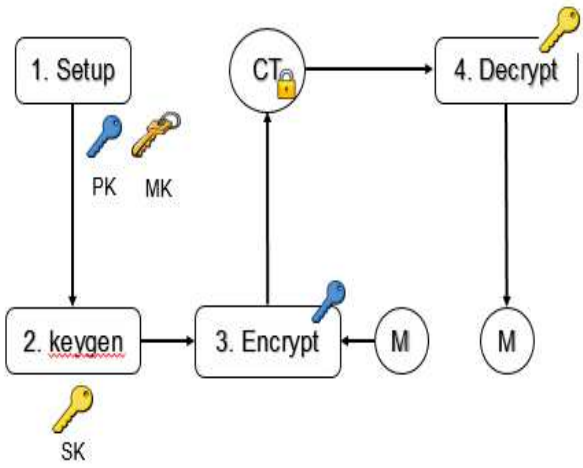

Fig. 1. Security in CP-ABE

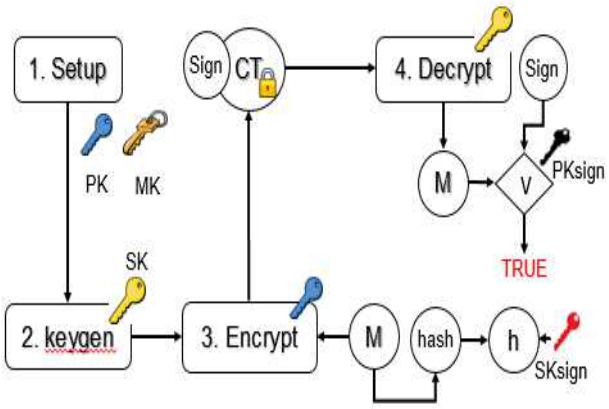

Fig. 2. Security in CP-ABE with Authentication

Our adopted method CP-BE and our proposed have 4 process, there are setup, key generator (keygen), encryption process and decryption process. Our propesed method have a different process from adopted method, the different is in processof encryption and decryption, we enhance encryption and decryption process with signature using RSA 2048. In Fig. 1 and Fig. 2 shows the process of security mechanism where each process are described as follows:

Setup: Setup is the first process in CP-ABE where in this process the system generate the Master Key (MK) and Public Key (PK).

Keygen: keygen is the next process in CP-ABE where in this process are generating the secret key with attributes each user embedded in them.

Encrypt: encrypt is the process to make a ciphertext with access policy attached with the attributes in the ciphertext from the message created by user.

Decrypt: decrypt is the process to recovered the message from ciphertext using the private key each user

Fig. 1 shows in the CP-ABE there is not have an authentication process after decryption process success, but in Fig. 2 shows our propose system have a security mechanism with authentication and revocation.

our propose system have 4 actors such : Data Center, Manager, User and Trust Third Party (TTP). Fig. 3 shows the Proposed our system.

Fig.3. Security System for Data Sensor Access

In the data center stored a lot of existing sensor data such as CO, CO2, Temperature, Humidity, Luminosity and Noise. All of the data can be accessed and requested by the user and manager. All user make a request in the system to get the data sensor, then the user's request will be responded. Before sensor data will send to the user, the data sensor will be encrypted with CP-ABE to generate a ciphertext and a timestamp digital signature to be sent along with the ciphertext. These two data will be sent to user who make a request in the Data Center.

We proposed our system withfour actors such as Figure1. There are Manager, Users, Trust Third Party and Data Center

Manager : An actor with a special access, a Manager can decrypt all sensor data in the data center. The Manager will not be included in the revocation list and the manager is also able to report to Trust Third Party to remove the user on the revocation list.

User : An actor where the access of the user is limited according to attributes from the user. If the user is doing the illegal access then the user will be directly inserted into the revocation list.

Third Trust Party : Someone who has been trusted and agreed between the user and manager for monitoring and supervising the system. TTP is responsible for the confirmation and validation of registration data from users and manager. TTP also acts to revoke the users who did the illegal access ems

Data Center : a storage media for storing all the data such User, Manager and Data Sensor. In the Data Center, all of data will be encrypted before sent to the requesting user. The Data Center also generate the key where the key will be sent to the user whose registration has been validated by TTP.In the data center also stored list of user revoked.

In performing data transactions on our systems, we divide these transactions into three protocols such :

1) RegistrationProtocol

The first step in data transactions is the registration protocol. This is the stages where users and managers who want to access the system and request data to the data center. Users and managers input their personal data and select the attributes that will be used to access the system. After the data is entered then the data will be sent to the Data Center to be validated by TTP. If the data has been validated then the data center will generate the Secret Key and send the Secret Key (SK) to the user and manager who has completed the registration process where the SK will be used to decrypt the ciphertext. Fig. 4 shows the process of registration protocol.

Users with the access rights can request in the system to get the data sensor in the Data Center. The system will respond form user's request and then the system will be sent a ciphertext to the users. To get the data sensor, the user must decrypt the ciphertext whose received before If decryption process performed by the user fails then this process will be stored in the system where the system have been monitored by TTP. The data from user that fails to decrypt the ciphertext will be monitored by TTP.

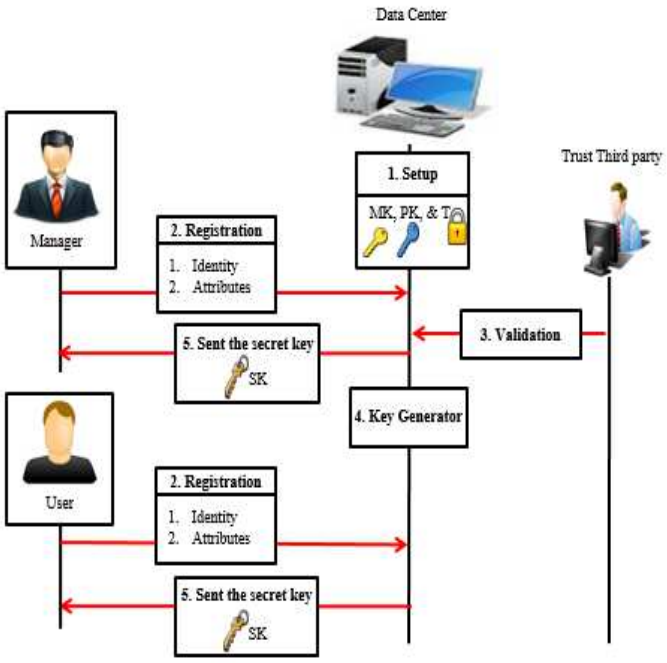

Fig. 4. Registration Protocol for User and Manager

2) Data Sharing Protocol

In Fig. 5 shows the process of data sharing protocol. Users and managers who have done the registration process and have SK can access the system to perform data

transactions. All sensor data that has been stored in Data Center can be downloaded by user and manager with make a request to system. This request will be directly responded by the system where the system will send the data sensor stored in the Data Center to be sent to the user and manager. Before the data sensor have been sent from the Data Center, the data sensor will be encrypted first according to the policy rule that has been made before. After this encryption process completed then the system will generate a ciphertext (CT) Which will be directly sent to users and managers who have requested data on the system. After CT is received by the user and manager, the data in ciphertext will not be readable, it needs to be decrypted to get the original data from the ciphertext. User and Manager perform the decryption process by using each SK that has been received previously in the registration process. If the SK from the user and manager matchs with rules of access policy (T) in the ciphertext then the decryption process will be successful. If the decryption process is successful then the user and manager will get the original data and they can read the content of the data sensor.

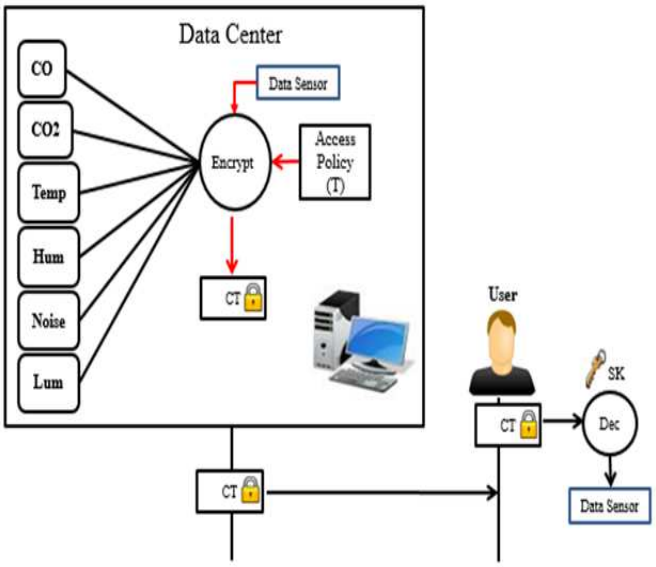

Fig. 5. Data Sharing Protocol for User and Manager

3) Revocation Protocol

Users with the access rights can request in the system to get the data sensor in the Data Center. The system will respond form user's request and then the system will be sent a ciphertext to the users. To get the data sensor, the user must decrypt the ciphertext whose received before. If decryption process performed by the user fails then this process will be stored in the system where the system have been monitored by TTP. The data from user that fails to decrypt the ciphertext will be monitored by TTP where the user who did the illegal access acts outside the access that has been given when the registration process. It is make that user will be included in the revocation list by TTP. Users have been registered in the revocation list will never successfully perform the decryption process even though the user is still able to make a request in the system. Fig. 6 shows how the revocation user process.

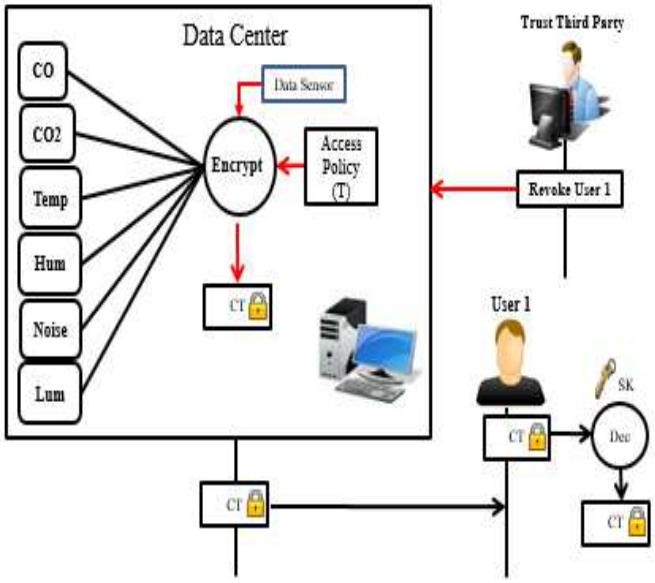

Fig. 6. Revocation Protocol for User did the illegal access

To construct the security mechanism from illegal access to the system of data sensor in the data center such as CO, CO2, Humidity, Luminosity, Noise and Temperature, hence we divide the three grub for policy rules on sensor data stored in the Data Center and also three grub for the division of user and manager. We create for the group on data sensor is C1 for CO and CO2, C2 for Temperature and Humidity, C3 for Luminosity and Noise. As for the group of user and manager, we divide the user based on the division selected user during the registration process where each division has attributes that will be associated with the policy rules on the ciphertext have been sent by the Data Center. The division of the user group is D1 for Manager and User on Ranch Division, D2 for user on Agriculture Division and D3 for User on Industrial Division.

We use each attributes on the user and manager to use as a rule of access policy which will be associated in the ciphertext. We divide three access policy (T) rules on the ciphertext that we will apply to the security system that we build. The rules can be seen in Fig. 7 where we also add rules to revoke the users who did the illegal access.

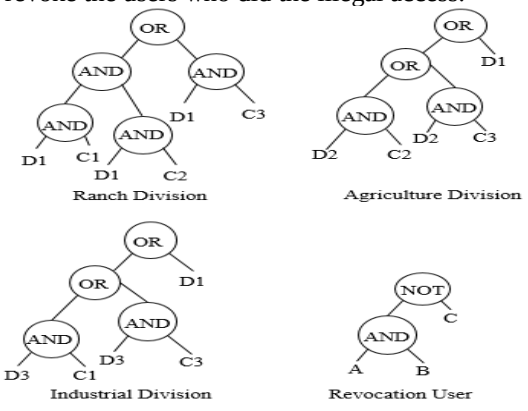

Fig. 7. Rule of Access Policy in Ciphertext

We implement the system we build using real hardware where the communications use wireless local area network with HTTP protocol. The hardware and software specifications that we use as table below :

TABLE I
THE SPECIFICATION OF THE HARDWARE AND THE SOFTWARE

Actor	Details
Data Center	Hardware
	Intel Xeon CPU E3-1225 3.20 GHz, 4GB DDR3, Dell Precision T1650
	Operating System
	Ubuntu Linux 16 kernel 4.4.0-22
	Software
	GMP-6.1.1, pbc-lib-0.5.14, glib-2.34, libbswabe-0.9, openssl-1.0.1e,cpabe-0.11 apache2, Mysql.
	Wireless Communication
	Access Point TP-Link TL-WR740N IEEE 802.11n
Manager, User, and Third Trust Party	Hardware
	Intel core i3-3110M 2.4GHz, 4GB DDR3, Lenovo G400s
	Operating System
	Windows 10 64-bit
	Software
	Mozilla Firefox Browser-52.02
	Wireless Communication
	Qualcomm Atheros AR9485WB-EG

We propose a system where all of data stored in the Data Center can be accessed by the users using web based with http protocol. We use the wireless local area network for the communications. All of access by the users will be supervised by TTP to protect the system from illegal access. In Fig. 8 shows our design system for environmental monitoring.

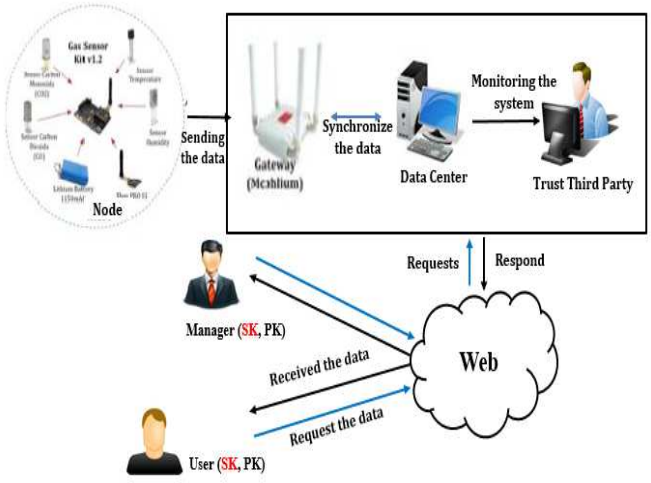

Fig. 8. Design System for Environmental Monitoring

In the system that we build all data in the Data Center will be encrypted using CP-ABE before sent to the User or Manager. To enhance the security mechanism in the system, we provide the feature to authentication of the data integrity using timestamp digital signature RSA 2048. After the decryption process is successful then the user and manager can perform the validation process of the data, if the value from validation process has true then the data obtained is the original from the Data Center, but if the validation process from data received is false then the data have been received not from the data center or the data received is fake. This mechanism enhances the security and give the guarantee of the authenticity of data to each user registered in the system to perform data transaction process. This mechanism also provides protection against the repetition of data transmission, because when the validation process from the first received data and the last received data have the different value. In Fig 9 shows the process for encryption and decryption a ciphertext from the Data Center until received by the user. User with the access right make a request to the system for downloading the data. The request from user will be respond by the Data Center, before the data will be send to the user, all of data will be encrypted using rule of polcy (T) each attributes from user and sign from the Data Center. This mechanism to give the security aspect in the data that only user with access right can get the original data and make a verification in the data, but for user in the revocation list, they cannot get the original data and cannot doing the verification process.

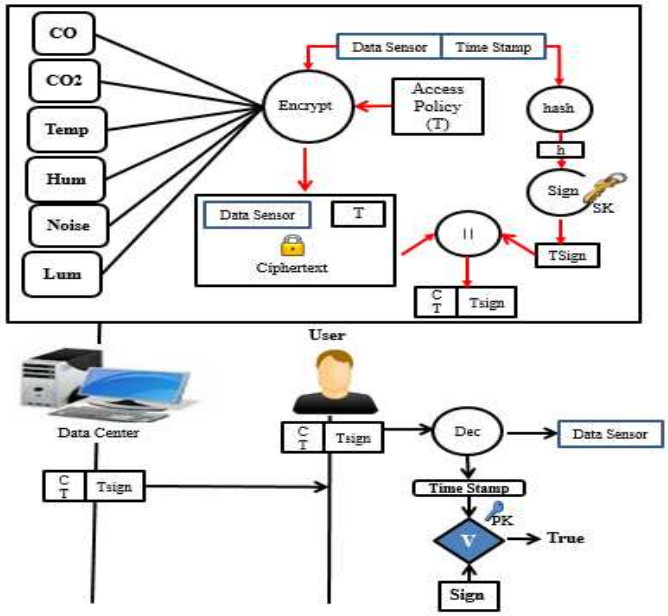

Fig. 9. Encryption process datain the Data Center

III. RESULT AND DISCUSSION

Our system can be accessed by the user with the access right or without the access right but the only user with the access right can download the data sensor in the data center. To download the data sensor the user with the access right must login to the system. After the user with access right login to the system, the user can make a request in the Data

Center to get the data. Fig. 10 shows menu for user in our system when user log in to the system.

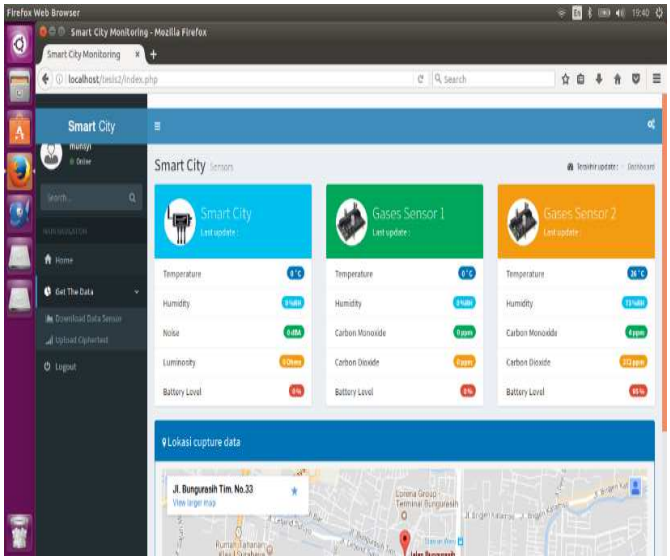

Fig. 10. Front view menu in our system

From Fig. 10, if the user want to get the data, the user can choose a menu in the system. Fig. 11 shows the menu for downloading the sensor data.

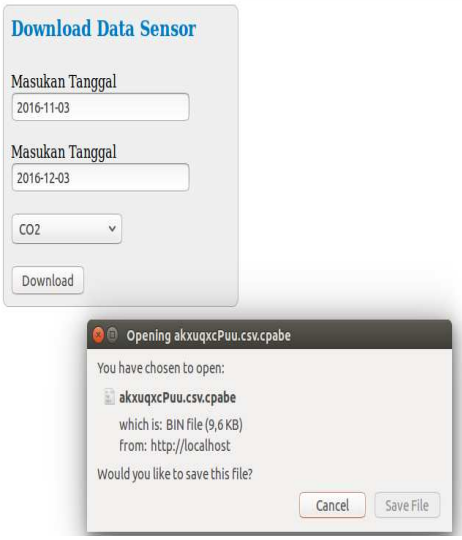

Fig. 11.Menu for downloading data

After the ciphertext received to the user. The user cannot directly read the content of the data, There is need the decryption process of ciphertext to get the original data, the user must decrypt the ciphertext if they want to read the content of the data. To decrypt the ciphertext the user uses the secret key, if the attributes of the user are appropriate with the access policy of ciphertext then the decryption will be a success. To decrypt the ciphertext, the user can choose the decryption menu in our system. The ciphertext must be upload to the system with the secret key of the user. If the attributes of user appropriate with the access policies from the ciphertext, then the process decryption the ciphertext will be a success and the user can download the original data. When the user get the original data then the user can verify the data using the timestamp digital signature. In Fig. 12 shows decryption menu to decrypt ciphertext..

Fig. 12. Decryption menu to decrypt the ciphertext

The user with the access right can success get the original data but not for the user in the revocation list, the user in the revocation list will be failed to get the original data. It is because the attributes of the user in the revocation list was be updated by trust third party then the attributes is not appropriate with access policy in the ciphertext. In Fig. 13 and Fig. 14 shows the recovered process from the user with the access right and the user in the revocation list to decrypt the ciphertext.

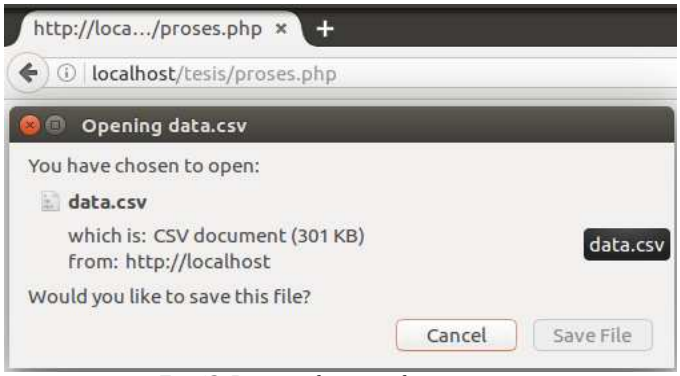

Fig. 13. Recovered process data success

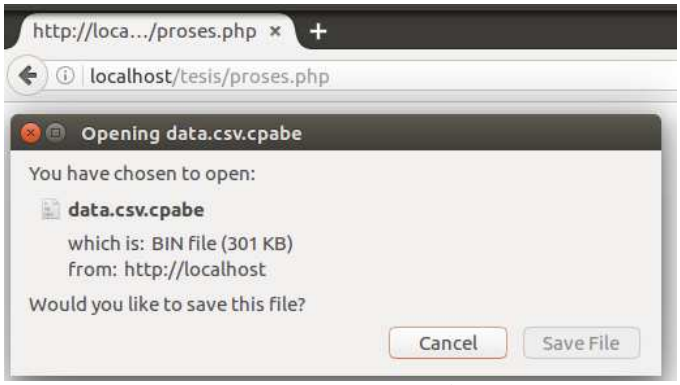

Fig. 14. Recovered process data failed

We analyze the processing time for encryption, decryption, and verification the timestamp digital signature using different access policy (T) with 1000 revoked users. We using the data sensor for one month with each access policy (T) for T1, T2 and T3. In Fig. 15, Fig. 16 and Fig. 17 shows our experimental result. We analyze with each group of the user to view the different processing time for

encryption and decryption process for the data between user with the access right and user in the revocation list.

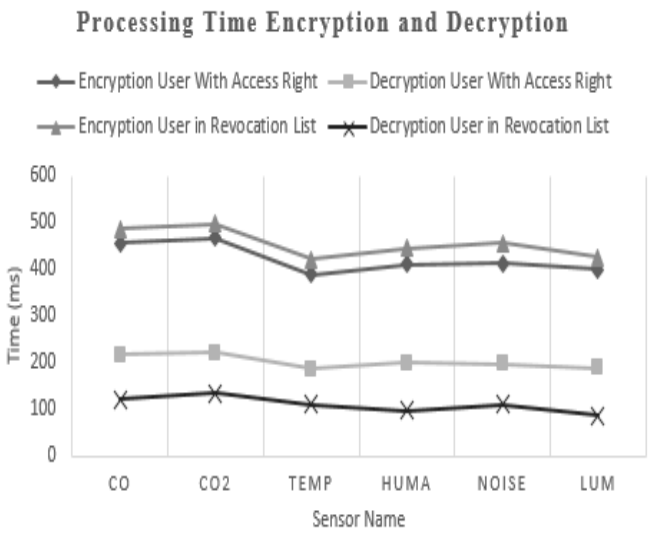

Fig. 15. Processing time for encryption and decryption T1

In Fig. 15 shows the processing time in T1 for encryption process only needs less than 467 ms for user with the access right and only less than 498 ms for user in the revocation list, for decryption process only needs less than 222 ms for user with the access right and only less than 134 ms for user in the revocation list.

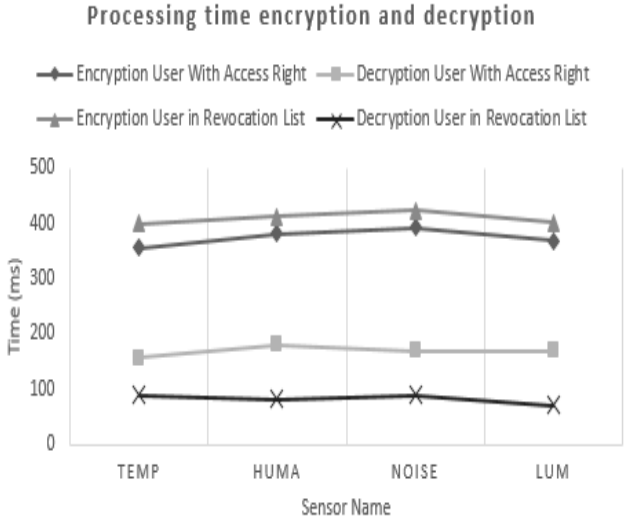

Fig. 16. Processing time for encryption and decryption T2

In Fig. 16 shows the processing time in T2 for encryption process only needs less than 392 ms for user with the access right and only less than 422 ms for user in the revocation list, for decryption process only needs less than 169 ms for user with the access right and only less than 89 ms for user in the revocation list.

In Fig. 17 shows the processing time in T3 for encryption process only needs less than 439 ms for user with the access right and only less than 467 ms for user in the revocation list, for decryption process only needs less than 202 ms for user with the access right and only less than 127 ms for user in the revocation list.

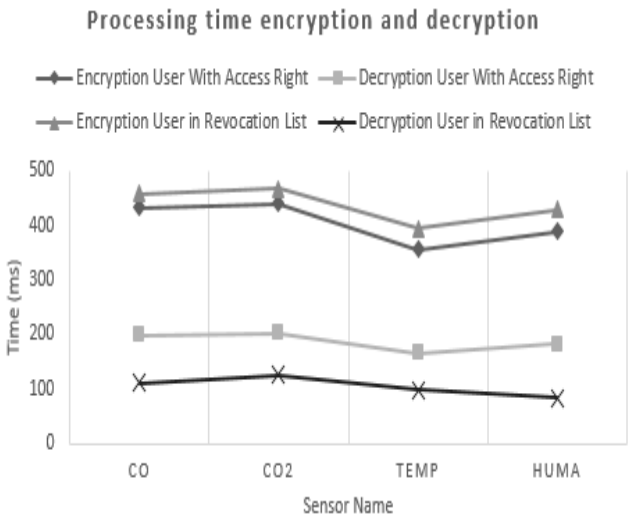

Fig. 17. Processing time for encryption and decryption T3

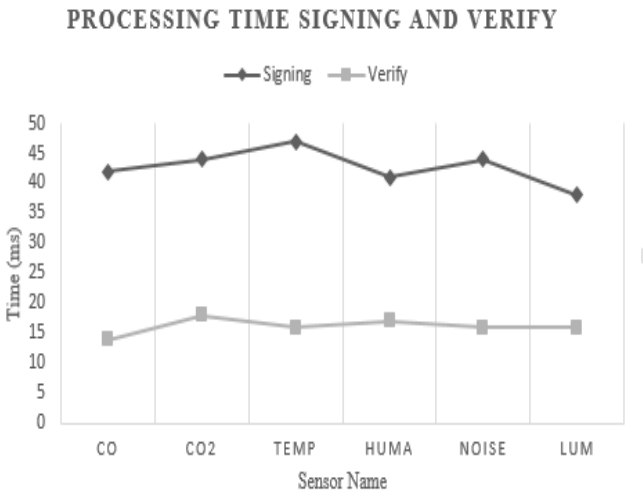

Fig. 18. Processing time for signing and verification

We analize the processing time for signing and verification using timestamp digital signature RSA 2048. In Fig. 18 shows the processing time for signing only needs less than 47 ms and for verification only needs less than 18 ms. We also analize the revocation check time for 10 until 1000 numbered of revoked users. In Fig. 19 show the revocation check time for 1000 numbered of revoked users.

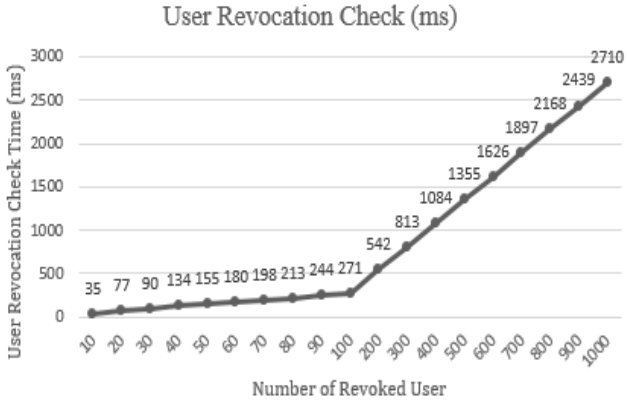

Fig. 19. Numbered of revocation check time

IV. CONCLUSIONS

We implementation CP-ABE with combining a timestamp digital signature using RSA 2048 to sign and verify the data, the timestamp digital signature will provide data integrity and give a guarantee the authenticity of data that has been sent. Our system can secure the data information and give the guarantee to the data information will not change during the process from the data center until the user received the data, we provide the guarantee the user will not receive a fake data. The combination between CP-ABE to secure the data with encryption and decryption process to protect the data sensor, to revoke the user did the illegal access and timestamp digital signature with RSA 2048 in the data is not affecting to performance of the system. Our experimental show the results all of process less than 3 second with 1000 number of revoked users.

REFERENCES

[1] 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.

[2] M. Udin Harun Al Rasyid, Achmad SayfudinAchmad Sayfudin, Arif Basofi, Amang Sudarsono. Development of Semantic Sensor Web for Monitoring Environment Conditions. International Seminar on Intelligent Technology and Its Applications (ISITIA),pp. 607-612, 2016.

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

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

[5] Munsyi, Amang Sudarsono, and M.U.H. Al Rasyid, "Secure Data Sensor In Environmental Monitoring System Using Attribute-Based Encryption With Encryption", International Journal on Advanced Science, Engineering and Information Technology, Vol 7, pp., 2017.

[6] A.Sudarsono, M.Udin Harun 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, 2016.*

[7] Munsyi, Amang Sudarsono, M. Udin Harun Al Rasyid, "Secure Data Sensor Access Using Attribute-Based Encryption With Revocation Environmental Monitoring", Knowledge Creation & Intelligent Computing (KCIC), pp. 73-79, 2016.

[8] K. H. Patel, S.S Patel. 2016, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" International Journal for Scientific Research & Development, vol. 4, pp.543-548, 2016.

[9] 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 2016].

[10] B.Lynn. PBC (Pairing-Based Cryptography) library. [Online]. From: http://crypto.stanford.edu/pbc. [accessed on Oktober 2016].

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.