Jurnal Teknologi

Full Paper

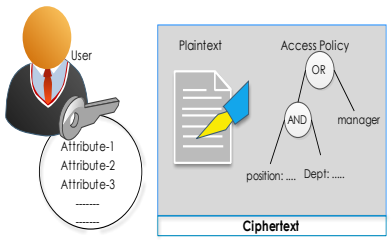
SECURE DATA SENSOR SHARING ON UBIQUITOUS ENVIRONMENTAL HEALTH MONITORING APPLICATION

Samsul Huda*, Nurul Fahmi, Amang Sudarsono, M. Udin Harun Al Rasyid

Graduate School of Informatics & Computer Engineering Politeknik Elektronika Negeri Surabaya, Surabaya, Indonesia

*Corresponding author
samsul@pasca.student.pens.ac.id

Article history
Received
7 June 2015
Received in revised form
8 September 2015
Accepted
9 December 2015



Abstract

In Internet of Things (IoT) era, The limitation storage on Wireless Sensor Network (WSN) can be solved by synchronized data sensors from the gateway node to the data center server. Data in the data center can be remotely accessed by the user at any time and anywhere from end user devices such as PCs, laptop PCs, and smart phones., and data should be accessed securely. The Only legitimated user can access the data sensor from an environmental health data center. CP-ABE (Ciphertext-Policy Attribute-Based Encryption) is becoming a robust cryptographic scheme solution to this issue. To enable a secure data sensor sharing and access on an environmental health data center, we propose a secure system model using CP-ABE which ensures confidentiality, integrity, and user privacy features. Experimental results prove that the implementation of CP-ABE does not overload the system.

Keywords: Secure data sensor; environmental health data center; access policy

1.0 INTRODUCTION

Wireless sensor networks (WSNs) have many applications in critical condition, like in the military, disaster management, homeland security and other critical conditions [1]-[3]. The environmental health monitoring system through WSN which inform environmental health information such as temperature, humidity, luminosity, noise, carbon dioxide (CO) and carbon monoxide (CO2) from sensor nodes transmitted to the gateway and synchronize to the environmental health data center. Hence, data sensor can be accessible at anytime and anywhere by all legitimate users using any type of end user devices, both fixed and mobile devices, i.e., PCs, laptop PCs, and smartphones.

Data sensor is the core data in the data center so that it needed for restrictions on the right of access only to authorized users. Moreover, the distribution of data through internet network. Numerous techniques to exchange data securely in the data center, one of them by applying the encryption algorithm. [10] proposed secure Electronic Medical Record (EMR) system cloud-based using ECC. [11] proposed a secure data access mechanism based on identity-based encryption and biometric authentication for cloud tenants and compared with RSA and ECC algorithm.

However, the existing security system is still based on authentication user personal data, such as username or some other personal data. CP-ABE[4] is one of the techniques that provide features to hide the user personal data by utilizing insensitive user attributes as user identity. In CP-ABE, access policy embedded on the ciphertext. Hence, the manager can control it. CP-ABE is appropriate for most applications, like for data exchange over wireless medium [8], Secure content exchange in Delay Tolerant Networks (DTN)[9] and etc.

To enable secure access and data sharing in an environmental health data center, we propose secure data sensor sharing using CP-ABE by present two protocols, registration and data sharing protocol, and various rules access policy for each sensor groups to ensure confidentiality, integrity, and user privacy aspects. Experimental results prove that the implementation CP-ABE does not overload the system.

2.0 RELATED WORKS

[6]Proposed new architecture for inter-organizational data sharing in multi-clouds and implemented for healthcare data. The proposed system provided a high level of security and privacy for patient data in semi-trusted cloud computing environments. The security features are selective access authorization using attribute-based encryption and cryptographic secret sharing in order to avoid collision data in multiple clouds.

[5]proposed a new mechanism to reduce the decryption computation overhead by partial decryption, and protect user privacy by obfuscating access policy of ciphertext and user's attributes namely efficient and privacy-preserving attribute-based broadcast encryption (BE) (ABBE). The proposed system is implemented in personal data sharing scheme in cloud computing which ensure secure, efficient and privacy-preserving

[7]proposed new security data access control in cloud computing scheme by combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. The proposed scheme satisfy three security properties: user access privilege, confidentiality and user secret key accountability.

3.0 OVERVIEW OF CP-ABE

In this section, we review some basic concepts of CP-ABE scheme [4]. In the CP-ABE scheme, the access policy structure is related with the set of attributes At of user that embed in the secret key SK. The access policy is linked with encrypted data, even if over radio link medium which is not secret, the confidentiality of data cannot be revealed. Only when the set of attributes associated with the decryption key corresponding with the access policy, the user will be able to decrypt the CT and get back the plaintext like shown in Figure 1. The CP-ABE has four phases which include setup, key generation, encryption, and decryption.

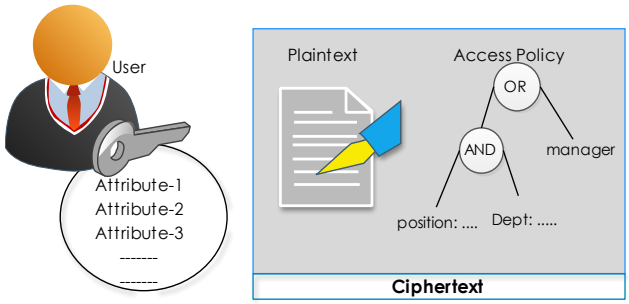


Figure 1 Ciphertext-policy attributed based encryption

a) Setup (PK, MK): On input a security parameter, this algorithm randomly outputs the public parameters PK and a master key MK which is kept private. PK will be used for encryption and decryption mechanisms while MK will be functionalized for generating user's secret keys.
b) KeyGen (PK, MK, At): On input the public key PK, master key MK and attribute list At. The output is a secret key SK for the user. That's associated with attribute At.
c) Encryption (PK, M, τ): This algorithm is run by the manager who will act as an encryptor. On input a message M, an access policy τ, and the public key PK. It outputs a ciphertext CT.
d) Decryption (PK, CT, SK): This algorithm is operated by all participating nodes who will act as a decryptor. On input a ciphertext CT, a secret key SK. If and only if At = τ the message M can be recovered to original message M, and error symbol ⊥ otherwise.

4.0 OUR PROPOSED SCHEME

In this section, we present the system model of secure data sensor sharing on ubiquitous environmental health monitoring application and then describe our design protocols.

4.1 System Model

Figure 2 shows system architecture of environmental health monitoring system. Sensor nodes sensing and collecting some environmental health information such as temperature, humidity, luminosity, noise, carbon dioxide (CO) and carbon monoxide (CO2). The transmitted data sensors are propagated through IEEE802.15.4-based communication toward a gateway which equipped with a small-size storage.

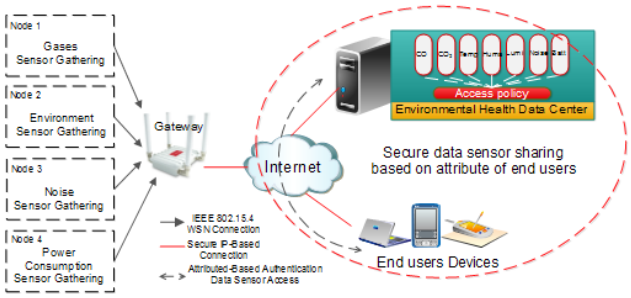


Figure 2 Ubiquitous Environmental Health Monitoring Application

Further, the collected data sensors in the gateway are synchronized to the data center server through TCP/IP connection for permanently storing. Legitimated users are able to access the data sensors. We propose secure data sharing which satisfies security requirements are as follows:

User privacy: It means the user data is unexposed.

Data Sensor Confidentiality: It means the exchange of data sensor between the user and manager is kept undisclosed to others. No one user is able to recover the original data sensor except the right user whose have an attribute satisfied with the access policy.

Data Sensor Integrity: It means the data sensor is guaranteed, safeguarding correctness of information. No one user is able to access or modify, delete, create and reply the data sensor. If data modificated, should be detected.

Our system model involves three parties: Manager, user, and environmental health data center like shown in figure 3. To access data files shared by manager, user download data files of their interest from the data center and then decrypt it.

Manager: A person who stores the data in encrypted form in the data center. Manager defines the access policy for data sensor which determines 'who to access what'.

Environmental health data center: data storage which can be accessed remotely over the internet. The other functions execute setup phase, key generation to generate the public key and the master key. The private key Sk generated are distributed to manager and users that participate.

Users: the entities who accessing the data sensor. Having right to access that data.

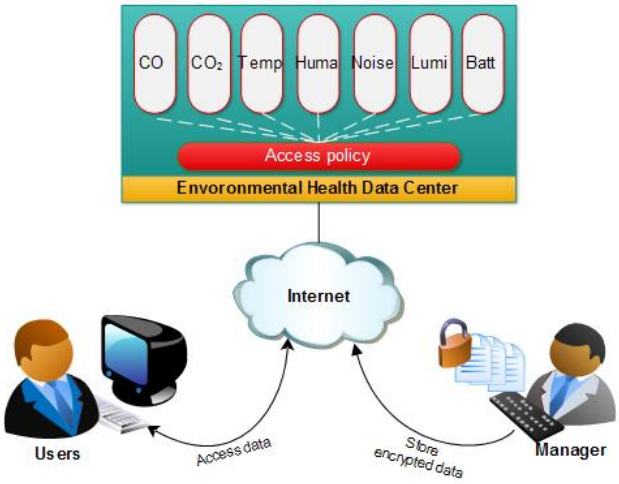


Figure 3 System model of secure data sensor sharing

4.2 Design Of Protocols

We design two protocols in our proposed scheme: Registration and data sharing as follows:

A. Registration

Figure 4 shows the registration protocol. At first, the environmental health data center as a key generation server (KGS) operate setup phase which resulting MK and PK. Then, users who want to participate include manager request their secret key SK by attaching username, password, and a set of user attributes. Based on the user attributes, KGS act KeyGen to generate users secret key SK. User's password will be used as a shared key K for HMAC process. Then, KGS distribute the public key PK and user's secret key SK for data sharing mechanism to all participants through secure channel communication, for example using VPN.

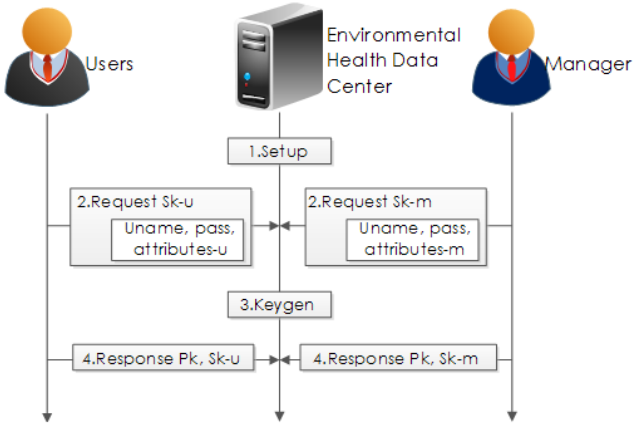


Figure 4 Registration protocol

B. Data sharing

The data sharing protocol mechanism is shown in Figure 5. To enable data confidentiality feature, the

data to be shared is encrypted before uploading into the environmental data center. For more detail, manager as data sensor owner encrypts data sensor using public key PK. Moreover, in our proposed system maintain the data integrity while sharing of sensor data to ensure data unchanged using HMAC process. Then, the encrypted data host to the environmental health data center with hosting format like shown in Figure 6. All users exclude manager request data sensor what they needed to the environmental data center. Based on the request, the environmental health data center give response by send data sensor on encrypted form. Users must decrypt it. A user with right attributes can decrypt data sensor.

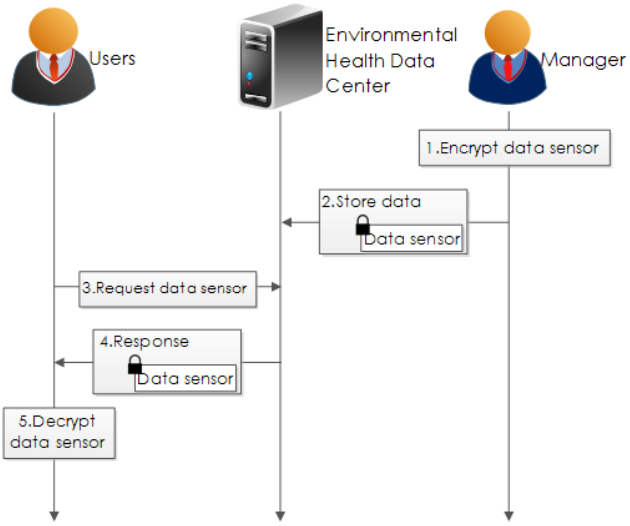


Figure 5 Data sharing protocol

Figure 6 Hosting format data

The environmental health data center have many data sensors include temperature, humidity, luminosity, noise, carbon dioxide (CO) and carbon monoxide (CO2) and battery. We collect all data sensor into four group and define different access policy T for each group. Group 1 gasses condition consists of gas sensor means CO and CO_2. Group 2 environment condition consists of temperature, humidity, and luminosity. Group 3 noise condition consist of noise and the group four power consumption consists of the battery. Data sensor will be used for research from physics and chemistry department. Hence, from Table 1 we describe the inherent of user attributes and possible be registered and enable for construct the access policy.

We choose the occupation, department and position attributes for use. The access rights of the users based on the access policy defined like shown in Figure 7. Group 1 with T1 allowed accessed by a researcher from physics department or a laboratory analyst. Group 2 with T2 allowed accessed by a researcher from chemistry department or a laboratory analyst. Then group 3 and 4 with T3 allowed accessed by researchers from physics or chemistry department or a laboratory analyst.

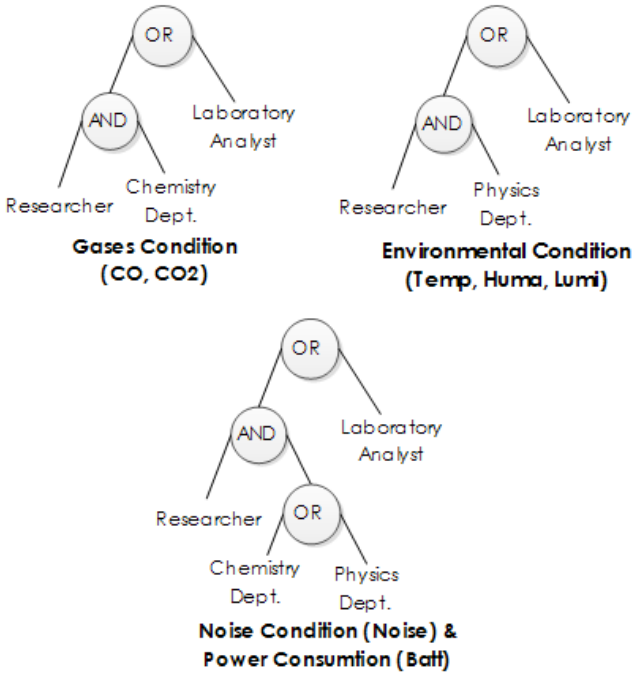


Figure 7 Data sensor access policy T

Table 1 Possible user's attibutes

Attributes	Type	Example values
Name	Sensitive	*****
Birthdate	Sensitive	*****
Salary	Sensitive	*****
Phone number	Sensitive	*****
Gender	InSensitive	Male, Female
Age	Insensitive	23rd, 32nd, ...
Marital Status	Insensitive	Marriade, ...
Occupation	Insensitive	Lecturer, Researcher,..
Position	Insensitive	Chairman, Staff ...
Department	Insensitive	Physics, Chemistry, ...

5.0 IMPLEMENTATION AND EXPERIMENT

The communication between the manager, users, and the environmental health data center is over HTTP connections. Our implementation was built on C language as the middleware. We implemented our system using java through the java server pages (JSP) by porting mechanism to linking communication between C and java platform. The details and specification of the hardware on which the system described in Table 2.

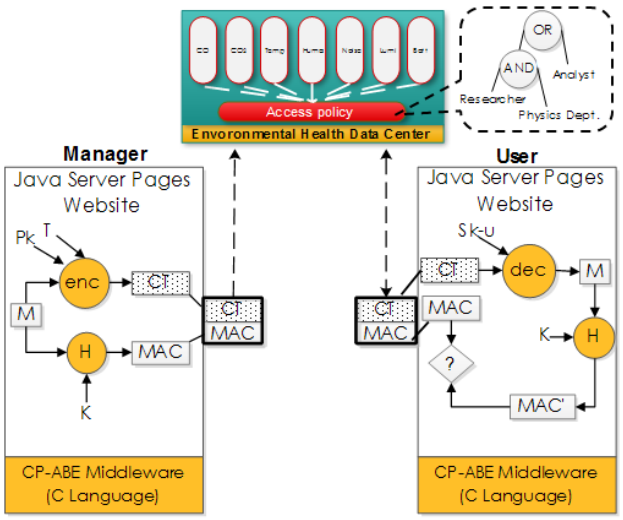


Figure 8 Implementation of secure data sensor sharing system

Table 2 Specification of H/W and S/W Used in experiment

Players	Details
Environmental Health Data Center	OS Debian 7 Linux kernel-3.5.0-17 Hardware Intel core i3 -370M 2.4 GHz, 4GB DDR3, Acer InviLink™ Nplify™ 802.11b/g/n Software 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.
Manager and users	OS Windows 7 64 bit Hardware Intel core i3 -370M 2.4 GHz, 2GB DDR3, Acer InviLink™ Nplify™ 802.11b/g/n Software Mozilla firefox Browser-40.0.3

In our system, the input parameter of encryption algorithm are the data sensor as message M, public key Pk, and access policy T like shown in Figure 7. Then, the output from this step is ciphertext CT. On another hand, the system executes HMAC process using HMAC256 [14] to ensure the data integrity of data sensor with shared key K and resulting message authentication code (MAC). Then, CT concatenates with MAC hosted to the environmental health data center. Users who want to access the data sensor from the environmental health data center download the data sensor in encrypted form concatenates with the MAC. After that, CT and MAC are separated. Then, decrypt the CT. If the user attributes that embedded on the user's private key match with an access policy that has been defined in CT, the user can recover the original message M. After that, execute HMAC and obtain MAC'. Then, MAC' and MAC compared, if true it can be ascertained that data integrity maintained. Otherwise, the message has changed.

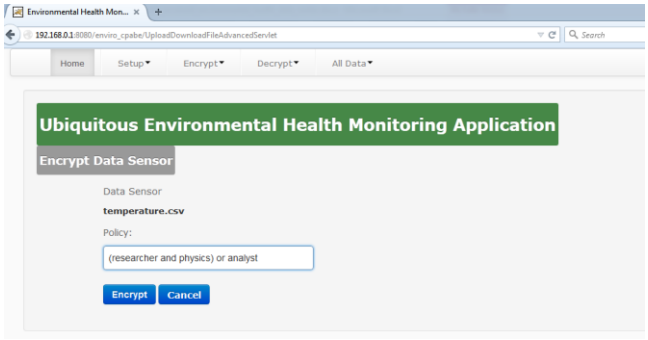


Figure 9 Data sensor encryption

All data sensors on environmental health data center have almost the same size around 7 KB. Data sensor of temperature with size 6837 byte used for the test bed. That data is used for encryption and decryption with a variety of access policy T. Table 2 shows that encryption process takes about 30 ms for T1 and T2 and 50 ms for T3. The ciphertext size increases around 1150 bytes by applying T1 and T2 and by applying T3 the ciphertext size increases around 1436 bytes. For storing data to data center take time about 115 ms. Meanwhile, for the decryption process takes quite stable time about 10 ms. like shown in Table 3. Therefore, total processing time take in sharing data sensor securely taken processing time less than 1 second.

Table 3 Data test bed of execution time

T	Encryption		Transmission Time (ms)	Decryption	
	Time (ms)	Size (byte)		Time (ms)	Size (byte)
T1	30.261	7983	98	10.124	6837
T2	30.295	7985	98	10.098	6837
T3	50.323	8273	113	10.122	6837

Thus, the difference structure of access policy T greatly affects the length of the execution time of encryption and size of ciphertext formed.

6.0 CONCLUSION

We have presented an implementation of ciphertext policy attribute-based encryption for secure data sensor sharing on ubiquitous environmental health monitoring application. In the proposed system, fulfill three security requirements, includes user privacy, data sensor confidentiality, and data sensor integrity. The experimental results prove that the implementation of CP-ABE does not overload the system.

7.0 FUTURE WORKS

Our future works include adding security features like enhance authentication, make so more scalable and also provides user revocation features.

Acknowledgement

This research was made possible through the help and support in part by Ministry of Research, Technology, and Higher Education of Indonesia, Insentif Riset SINAS Scheme, under Grant No.147/M/Kp/IV/2015.

References

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

[2] Liu, J. H., Chen, Y. F., Lin, T. S., Chen, C. P., Chen, P. T., Wen, T. H., Sun, C.H. Juang, J.Y. and iangAN J.A.J. 2012. Air Quality Monitoring System for Urban Areas Based on The Technology of Wireless Sensor Networks. *International Journal on Smart Sensing and Intelligent Systems*. 5(1): 191-214.

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

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

[5] Fu, J Huang, Q., Yang Y. 2014. Secure personal data sharing in cloud computing using attribute-based broadcast encryption. *The Journal of China Universities of Posts and Telecommunications*. 21(6): 45–51.

[6] Fabian, B. Ermakova, T. and Junghanns P. 2015. Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*. 48: 132–150.

[7] Yu, S. Wang, C. Ren, K. and Lou W. 2010. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. *INFOCOM, 2010 Proceedings IEEE*.1-9.

[8] Huda, S. Sudarsono, A. and Harsono T. 2015. Secure Data Exchange using Authenticated Ciphertext-Policy Attributed-Based Encryption. *2015 International Electronics Symposium (IES 2015)*. Surabaya, Indonesia. 29-30 September 2015. 140-145.

[9] Sudarsono A. and Nakanishi. T. 2014. An Implementation of Secure Data Exchange in Wireless Delay Tolerant Network Using Attribute-Based Encryption. *2nd International Symposium on Computing and Networking (CANDAR 2014)*. Shizuoka, Japan. 10-12 December 2014. 536-542.

[10] Tsai, K. Leu, F. Wu, Chiou, T. S. Liu, Y. and Liu H. 2014. A Secure ECC-based Electronic Medical Record System. *Journal of Internet Services and Information Security (JISIS)*. 4(1): 47-57.

[11] Rong, C. and Cheng, H. 2012. A Secure Data Access Mechanism for Cloud Tenants. *Cloud Computing 2012: The Third International Conference on Cloud Computing, GRIDs, and Virtualization*. Nice, France. 22-27 July 2012.113-119.

[12] Benthencourt, J. Sahai, A. and Waters B. 2015 Cpabe Toolkit In Advanced Crypto Software Collection. [Online]. From: http://hms.isi.jhu.edu/acsc/cpabe. [Accessed on Oktober 2015].

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

[14] Topal. M. 2015. Libgcrypt. Standalone HMAC-256 implementation. [Online]. From:http://svn.cubrid.org/cubridengine/trunk/external/libgcrypt-1.5.2/src/hmac256.c. [Accessed on Oktober 2015].