Secure Data Sensor Access Using Attribute-Based Encryption With Revocation For Environmental Monitoring

Arpitha P M[1], Janhavi V[2]
Computer science and engineering
VVCE, Mysore.
(arpithamys0@gmail.com, janhavi.v@vvce.ac.in)

Abstract— ***In Internet of Things (IoT) era, everybody can access data anytime and anywhere. Information in a data center can be accessed by users using end-user devices such as a smartphone, and Personal Computer. The data should be secured and cannot be accessed by illegal users from the environment monitoring. To secure and prevent the sensor data from illegal access by the user then it is required a security with a user revocation mechanism. CPABE (Ciphertext-Policy Attribute-Based Encryption) becomes a solution for this issue to protect the sensor data and revoke the user. In this paper, a secure system is proposed using CP-ABE with user revocation. This system does not only perform a sensor data encryption, but also a revocation to the user.***

Keywords— ***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 in a smart city [2] [3]. The environmental monitoring system uses WSN technology to obtain information such as carbon dioxide, carbon monoxide, temperature, humidity 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 sensor data 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.

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.

In this case, this paper will try to perform the data encryption and revocation to the user who conduct illegal access. The problem is how to perform the revocation to the user who has an access right. To revoke a user, we need the user's attributes. CP-ABE is a method that can be used to secure the data and perform a revocation to users with the attributes of the user.

II. LITERATURE SURVEY

R.Roy and M.Chuah [8] Proposed CP_ABE scheme in which encrypted data can only be accessed by authorized nodes. The author mentioned that there are two unique features of the scheme : the incorporation of dynamic attributes where the value of attribute may change over the time and a revocation mechanism.

M.Chuah et. al. [9] described implementation of a late-binding router that supports our security solution. In addition to the incorporation of dynamic attributes and revocation scheme. F.Jing-yi et. al. [11] proposed a new concept, efficient and privacy-preserving attribute-based broadcast encryption (BE) (ABBE) named EP-ABBE. It can reduce the overhead of decryption computation, and protect user privacy by making access policy of cipher text and user's attributes. The author showed that this scheme has three features includes secure, efficient and privacy-preserving.

F.Jing-yi et. al. [11] presented a generic attribute based data sharing system based on hybrid mechanism of CPABE and symmetric encryption scheme. It offered constant computation cost and constant size ciphertext. S.Gupta and C.Kumar et. al. [10] proposed security mechanism, Random Electronic Code Book (RECB) combined with permutation functions. This is used for converting the plaintext into ciphertext.RECB contains 16 bit unique random cipher code for each 16 bit of plaintext information. Codebook generated through simple algorithm.

A.Sudarsono and T.Nakanishi [5] presented a technique by which encrypted data can be kept confidential even if the storage server is untrusted and the methods are secure against collusion attacks.

III. SECURITY REQUIREMENTS

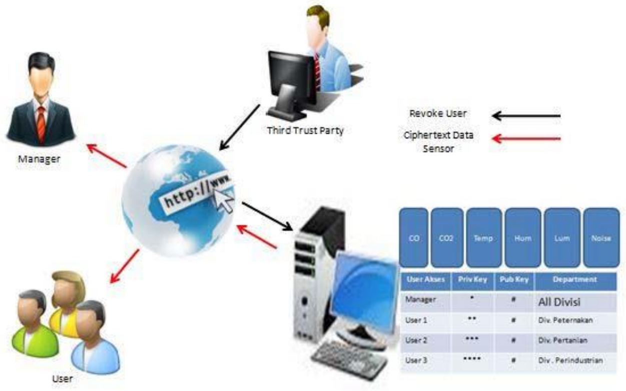
To create a data security, to control the users who access the data, and to secure the illegal access to the data center of the environment monitoring system. We propose The Secure Sensor Data Access using CP-ABE to guarantee the confidentiality of the data, integrity, and user access rights.

We propose a method to secure the sensor data with encryption. The sensor data in the data center will be encrypted, before the user with access right read the data. Only the user with the appropriate attribute in policies can decrypt the data. If the user cannot decrypt the data because their access right does not match with the policies, then the user is labeled as conducting illegal access, and they will directly put into the revocation list.

We adopt a method for securing the data center using Ciphertext Attribute-Based Encryption with Revocation for the user who conduct illegal access. Our security will update the attribute from the user to perform the revocation [10]. The user with attributes that have changed cannot decrypt the sensor data because they attribute does not match with the policies from the data.

IV. SENSOR DATA ACCESS SECURITY PROPOSAL

In this section, we discuss our proposed method for securing sensor data access using CP-ABE with revocation. Figure 1 shows the topology of security and revocation for environmental health monitoring.



User Akses	Priv Key	Pub Key	Department
Manager	*	#	All Divisi
User 1	**	#	Div. Peternakan
User 2	***	#	Div. Pertanian
User 3	****	#	Div . Perindustrian

Figure 1. Proposed system of Sensor Data Access Security

We propose a CP-ABE to encrypt the sensor data 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 and a data center such as Figure1.

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.

Third Trust 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 sensor data, the user, and the 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.

A. The Proposed Architecture

In our proposed system, we design three protocols, those are a registration protocol, a sharing data protocol and a revocation protocol:

1. Registration Protocol

Figure 2 shows the flow of user registration, where the data center is generating private keys and public keys. Manager and user make registration by entering username, password, and attribute. Registration is validated by a third trust party to be stored in the data center. Then, the key is distributed to the manager and users who have already done the registration.

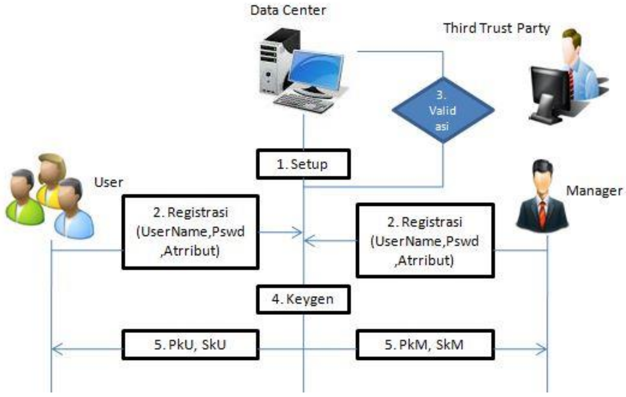


Figure 2. Registration Protocol

2. Data Sharing Protocol

Figure 3 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 have described the mechanism how to get the key. After the manager and users get the key, they can download the decrypted data and read it from that sensor data.

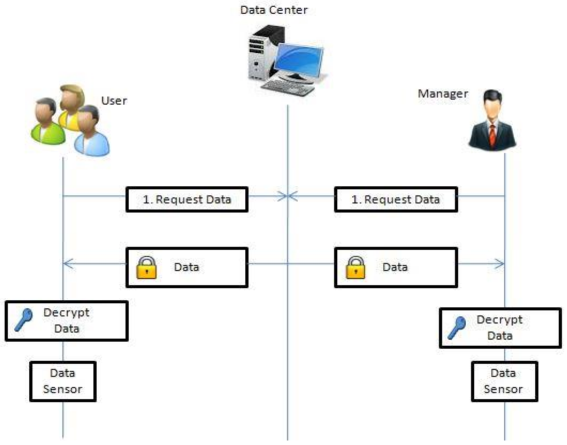


Figure 3. Data Sharing Protocol

3. Revocation Protocol

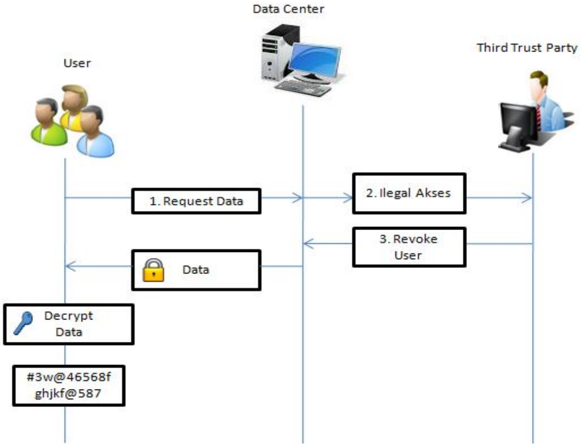


Figure 4. Revocation Protocol

Figure 4 shows the flow of user revocation who conducts 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.

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, where the base of access policy permission is defined as figure 5. 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.

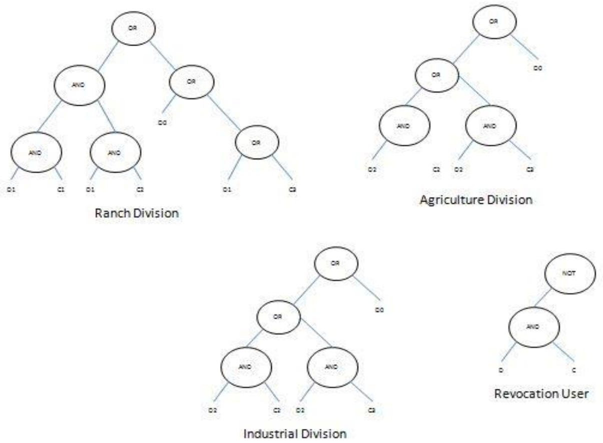


Figure 5. Rule of Access Policy

V. AES RIJNDAEL ALGORITHM

AES Rijndael Encryption Algorithm Steps :

- **Step 1:** KeyExpansion **-** round keys are derived from the cipher key using Rijndael’s key schedule. AES requires a separate 128-bit round key block for each round plus one more.
- **Step 2:** Initial round key addition :

  a. AddRoundKey **-** each byte of the state is combined with a block of the round key using bitwise XOR.
- **Step 3:** 9, 11 or 13 rounds :

  a. SubBytes **-** a non-linear substitution step where each byte is replaced with another according to a lookup table**.**

  b. ShiftRows **-** a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

  c. MixColumns **-** a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.

  d. AddRoundKey
- **Step 4:** Final round (making 10, 12 or 14 rounds in total)

  a. SubBytes

  b. ShiftRows

  c. AddRoundKey

VI. SHAMIR KEY TECHNIQUE

Shamir's Secret Sharing is used to secure a secret in a distributed way, most often to secure other encryption keys. The secret is split into multiple parts, called **shares**. These shares are used to reconstruct the original secret.

To unlock the secret via Shamir's secret sharing, you need a minimum amount of shares. This is called the **threshold**, and is used to denote the minimum amount of shares needed to unlock the secret. Let us walk through an example:

Problem: Company XYZ needs to secure their vault's passcode. They could use something standard, such as AES, but what if the holder of the key passes away? What if the key is compromised via a malicious hacker? Or, what if the holder of the key turns rogue, and uses his power over the vault to his benefit?

This is where SSS comes in. It can be used to encrypt the vault's passcode, and generate a certain amount of shares, where a certain amount of shares can be allocated to each executive within Company XYZ. Now, only if they pool their shares together can they unlock the vault. The threshold can be appropriately set for the number of executives, so the vault is always able to be accessed by the authorized individuals. Should a share or two fall into the wrong hands, they couldn't open the passcode unless they had cooperation from the other executives.

a) Mathematical definition:

The goal is to divide secret ***S*** (for example, the combination to a safe) into ***n*** pieces of data $S_1, \ldots, S_n$ in such a way that :

1. Knowledge of any ***k*** or more S_i pieces makes ***S*** easy to compute. That is, the complete secret ***S*** can be reconstructed from any combination of ***k*** pieces of data.
2. Knowledge of any ***k-1*** or fewer S_i pieces leaves ***S*** completely undetermined, in the sense that the

possible values for ***S*** seem as likely as with knowledge of **0** pieces. Said another way, the secret ***S*** Cannot be reconstructed with fewer than ***k*** pieces.

This scheme is called ***(k, n)*** threshold scheme. If ***k = n*** then every piece of the original secret ***S*** is required to reconstruct the secret.

Shamir's secret sharing scheme:

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a parabola, 4 points to define a cubic, curve and so forth. That is, it takes ***k*** points to define a polynomial of degree ***k-1***.

Suppose we want to use a (***k, n***) threshold scheme to share our secret ***S*** , without loss of generality assumed to be an element in a finite field ***F*** of size ***P*** where **0 < k < = n < P; S < P** and **P** is a prime number.

Choose at random ***k-1*** positive integers $a_1, \ldots, a_{k-1}$ with $a_i < P$, and let $a_0 = S$. Build the polynomial
$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_{k-1}x^{k-1}$.

Let us construct any ***n*** points out of it, for instance set ***i = 1, ... , n*** to retrieve ***(i, f (i)).*** Every participant is given a point (a non-zero integer input to the polynomial, and the corresponding integer output) along with the prime which defines the finite field to use. Given any subset of ***k*** of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

VII. CONCLUSION

So here using CP-ABE technique, with the help of AES algorithm and shamir key technique we can revoke the users who conduct illegal access and protect the security of the system from the user irresponsibility. This revoke additions do not affect the performance of the system from the data center environment health monitoring. The revocation list can only be accessed by the third trust party that is trusted by the manager and the user to perform monitoring and validation. Compared with the user in revocation list with the same encryption time but requires longer time for decrypt the data.

Our future work is adding a signature and digital time stamp to the messages sent by the manager to perform monitoring for the active user and add a validity of the data from the data center and make sure that the system should take the same decryption time as that it takes for encrypting the data. Also we can set department wise data access privileges for user's to make the system even more secure.

REFERENCES

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

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

[3] S.Huda, A.Sudarsono, and T.Harsono. 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.

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

[5] A.Sudarsono and T.Nakanishi. 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.

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

[7] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[8] R. Roy, M. Chuah 2005. "Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs", Journal of Cryptography, 17(4): pp.297-319,2004.

[9] M.Chuah, S.Roy, and I.Stoev, "Secure Descriptive Message Dissemination in DTNs", Proceeding of MobiOpp'10, 2nd International Workshop on Mobile Opportunistic Networking, pp. 79-85, 2010.

[10] S.Gupta and C.Kumar, "Shared Information Based Security Solution for Mobile Ad Hoc Networks", international Journal of wireless &amp; mobile networks(IJWMN), Vol.2, No.1, February 2010, pp.176-187, 2010.

[11] F.Jing-yi, H.Qin-long, M.Zhao-feng, and Y.YI-xian, "Secure personal data sharing in cloud computing using attribute-based broadcast .