International Journal on Advanced Science Engineering Information Technology

Vol.11 (2021) No. 4
ISSN: 2088-5334

Secure Data Exchange Based on Wireless Sensor Network for Environmental Monitoring Using Dynamical Attributed Based Encryption

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

[a]*Department of Da'wah and Islamic Communication, UIN-Antasari Banjarmasin University, Banjarmasin, Indonesia*
[b]*Department of Information and Computer Engineering, Politeknik Elektronika Negeri Surabaya (PENS), Surabaya, Indonesia*
Corresponding author: [*]munsyi@uin-antasari.ac.id

***Abstract*—The basics Internet of things based on Wireless Sensor Network (WSN) has grown rapidly in Industrial Revolution 4.0. Many researchers use the Wireless Sensor Network technology for obtaining the sensor data and stored in the Data Center. The collected data through WSN from an environment was sent to a Data Center. In the Data Center, all the sensor data can be accessed by everyone using their devices. In this case, the user can get the data with a smartphone, laptop, and personal computer through the HTTP Protocol. Data Center without protection from illegal access is extremely dangerous. All the sensor data stored in the data center can be intercepted, tracked, and even changed by a user without access. There is required a security mechanism for protecting all of the data stored in the Data Center. Ciphertext Policy Attributed-Based Encryption can be deployed as a security mechanism for protecting all the sensor data in the Environmental Monitoring. The security mechanism protected Data Center with encryption, decryption, verification, and revocation access for all the users. The only user with the access right can get the sensor data from environmental monitoring. Our security mechanism offers revocation and verification with a dynamic attribute for each user with a lower computational time. We used the CP-ABE with Dynamical attribute and timestamp digital signature based on Elliptic Curve Digital Signature Algorithm (ECDSA) 384 bits.**

***Keywords*— Internet of Things; wireless sensor networks; CP-ABE; environmental monitoring; elliptic curve cryptography.**

Manuscript received 10 Apr. 2019; revised 7 Aug. 2020; accepted 26 Nov. 2020. Date of publication 31 Aug. 2021.

I. INTRODUCTION

Many researchers have implemented the Wireless Sensor Network (WSN) technology for collecting all the data sensors for environmental monitoring On the internet of things era [1]–[3]. They use WSN technology to collect data sensors such as luminosity, noise, humidity, temperature, carbon monoxide (CO), and carbon dioxide (CO2) to the Data Center in the environmental monitoring system. All data sensors from WSN technology are collected and stored in the Data Center. All data sensors in the Data Center can be accessed by a user with end devices such as a computer, laptop, and smartphone. All of the users can get and read the data sensor in the environmental monitoring system. For accessing the system, all of the users use web-based communication with HTTP protocol for the communication. An environmental monitoring system in Data Centers without security mechanisms will be dangerous because the system can be intercepted, tracked, and even modified by illegal access from users [4]–[6]. The system must be secured from illegal access using a security mechanism with encryption and decryption. All the data sensors must be encrypted before sending the data to the user. There are have security aspects for securing the data sensor in the data center, such as the data that is privacy, confidentiality, and integrity [5]. Prevention for those who are not important to get a piece of information, relating to data given to other parties for certain purposes and only allowed for certain purposes. Integrity is information that may not be changed without the owner of the information. The authenticity of the message can be ascertained that the information sent is not modified by unauthorized people. No one user can access or modify, delete, create and reply to the data sensor. If the data was modified by the other, then it will be detected. To protect the system, it must have all aspects of the network security to give the user that all data is secure and provide data in the Data Center safe from the user without access rights and illegal access by the user.

All the data sensors in the environmental monitoring system must be protected. There are many methods from previous researchers to protect all of the data sensors in environmental monitoring systems. One of the security mechanisms for securing the data sensor is encryption and decryption based on ciphertext policy attributes [1]. The researchers use the security mechanism with the CP-ABE method and validation for data integrity using hash message authentication codes (HMAC) for providing authentication in data communication using a mobile ad-hoc network protocol.

There are problems with data integrity; users cannot have data guaranteed to be genuine. In this study, we enhanced a security system in CP-ABE to protect all data in Data Center to guarantee the user that the data is genuine. Our security mechanism for securing the data and the system can create a revocation mechanism for users. Only registered users can access the environmental monitoring and request the system for requesting data sensors in the Data Center. The user who wants to collect the data sensor in the Data Center must be registered before requesting the environmental monitoring system. Our system uses web-based communication through the HTTP protocol for data sharing in environmental monitoring systems. In this case, we consider developing a web-based to enhance the security system for environmental monitoring systems in our previous work.

A security mechanism was created in the previous research using the Elliptic Curve Digital Signature Algorithm (ECDSA) in smart objects for IoT nodes [7]. Therefore, we applied the same method using the Elliptic Curve Digital Signature Algorithm to adopt Time Stamp Digital Signature in our security mechanism. From our previous work [8], we implemented the CP-ABE with a revocation mechanism to secure data sensors and revoke users who did illegal access to the Data Center. We create a security system and guarantee data integrity to the user who has access rights in the Data Center. We combined and enhanced our system using CP-ABE with ECDSA timestamps. Our security mechanism is not only for securing data, but our security system can also guarantee security requirements such as authenticity, integrity, and non-repudiation for the data sensors.

This paper contributes to the security mechanism for implementing CP-ABE with web-based communication using PHP programs and timestamps using ECDSA and revocation access to the user. Our revocation mechanism is only for revoking users who did illegal access. Our security mechanism will secure all data in the data center with encryption and combining with authentication using ECDSA with a timestamp before sending it to the users. The user can verify all of the data sent from the data center. Users can validate originality in the data sensor. This mechanism guarantees that data does not change during the process from the data center to the user. Our system can be accessed by all of the users anywhere and anytime using their end devices.

The organizational structure in this paper is as follows.

- In Part 2, we explain the CP-ABE adopted with dynamic attributes. Then, our digital signature cryptography mechanism was adopted to make digital timestamp signatures on our system.
- In Part 3, we explain the mechanism exchange of our secure data in environmental monitoring using CP-ABE with time stamp digital signature algorithms schemes by analyzing experimental results and measurements.
- In Section 4, we conclude and discuss security mechanisms in our environmental monitoring system.

II. Materials and Method

We describe the difference between the original CP-ABE and our method using dynamical CP-ABE with authentication and revocation. Our method has a similar process in the CP-ABE algorithm [9], a message (M) encrypted using the public key (PK) with access policy associated with user attributes. The logical attributes from users express the rule of access policy in the ciphertext. The different process in our method from the original CP-ABE is we adopted the ECDSA and revocation for revoked each user.

A. Scheme of CP-ABE

In the CP-ABE algorithm mechanism for securing the data [9], there are have four steps involved in the data security process. The first step is setup, which is the first process in the CP-ABE security mechanism for generating keys; the keys generated by the system are Master Key (MK) and Public Key (PK). The next step is the Key Generator (Keygen), which is the next process for creating a secret key (SK) for each user. The master key and public key are used to generate a Secret Key (SK) where SK was generated by policy rules from input parameters and a set of user attributes. The next step is the encryption process. Encryption is the process of making a plaintext become ciphertext using PK with associations from each user attribute. The last step is the decryption process. Decryption is the process of returning a ciphertext to plaintext. The process of the original CP-ABE can show in Figure 1.

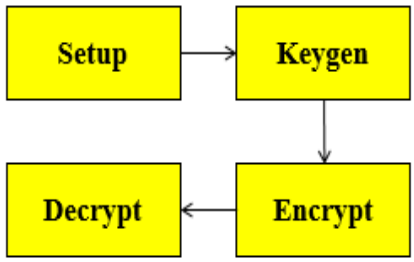

Fig. 1 Four steps for processing CP-ABE

B. Scheme of Dynamical CP-ABE

In our method with the dynamical CP-ABE algorithm have similar to CP-ABE from the original creator. The difference is in the keygen process where our method can update the attributes for each user and doing the revocation process. in our method user can request updating his attributes, for example, if the attributes user is A & B, then for updating the attributes can become A & C. The process steps in our method shows in Figure 2.

Besides the difference in the keygen process, our method has a difference in encryption and decryption process. We create the rule of policy in ciphertext with include the NOT logic for revoking the user and including the time stamp digital signature using ECDSA to guarantee the integrity of the message has not changed during the process.

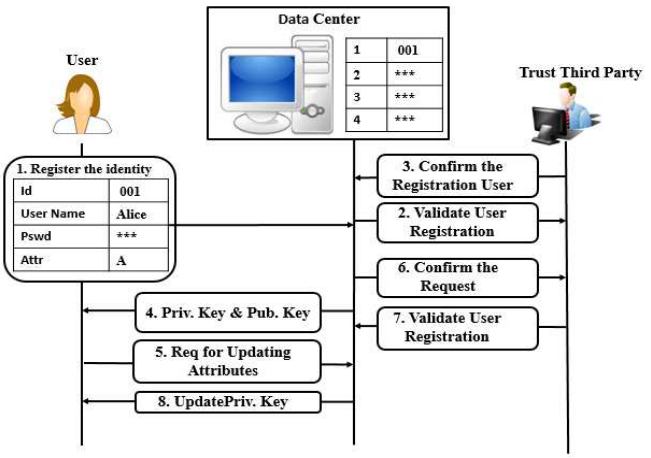

Fig. 2 Updating processing attributes user

In figure 3. we show the example rule access policy in ciphertext with the revoked user.

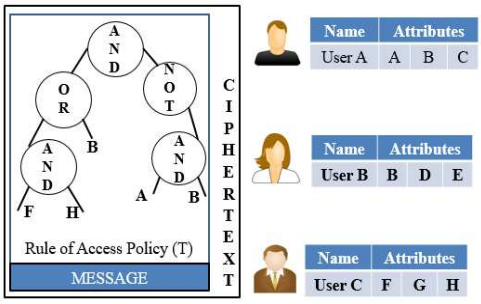

Fig. 3 Rule of policy in ciphertext with revoked user

Figure 3. shows a message that was encrypted with the access policy T = (((F AND H) 0R B) AND (NOT (A AND B)). Hence, User B is effectively revoked from the system. This revocation technique will require each message to be encrypted with a modified access policy T. Users can decrypt and get original messages are Users B and C Users because their attributes follow the ciphertext access policy. This is different from user A. It cannot decrypt ciphertext because its attributes are revoked in the access policy of ciphertext In Figure 4. shows User A, User B, and User C trying to decrypt the ciphertext. The user can successfully decrypt and get the message is User B and User C because the access policy in the ciphertext does not revoke the attribute.

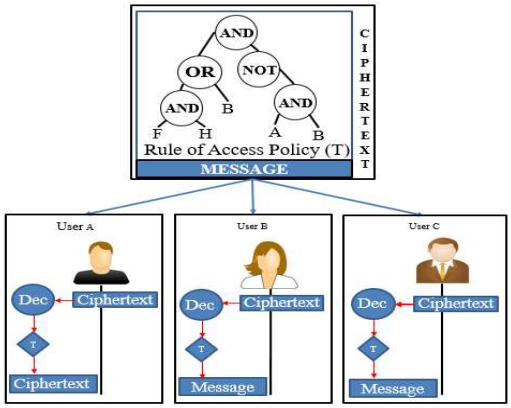

Fig. 4 Scheme in CP-ABE method with revoked user for Encryption and Decryption

C. Scheme of Dynamical CP-ABE

The idea of digital signatures first appeared in Diffie and Hellman [10], [11]. They proposed that each user publish a public key to validate the signature while keeping the secret key used to produce the signature. In their scheme, for example, user A, the user's signature for the message (M) is a value that depends on M and the user's secret key A. Hence, anyone can verify the validity of user A's signature using public key A. However, knowing public key A is enough to allow one to validate A's signature, it does not allow one to easily falsify signature from user A.

A digital signature is an asymmetric cryptography that provides a layer of validation and security for messages sent via unsafe communication. After the correction is applied, the digital signature gives the recipient reason to believe that the claimed sender sent the message. Digital signatures are equivalent to traditional handwritten signatures in many things, but digital signatures that are implemented correctly are more difficult to falsify than types of handwriting. In a sense, digital signature schemes are cryptographic-based and must be applied correctly to be effective. Digital signatures can also provide non-repudiation, which means signatories cannot claim that they did not sign the message while also claiming their private key remains confidential. Digital signatures can also provide non-repudiation, which means that signatories cannot claim that they did not sign the message while also claiming their private key remains confidential. Furthermore, some non-repudiation schemes offer a timestamp for digital signatures. Thus, even if the private key is opened, the signature is valid. There are several common reasons for applying digital signatures in communication and securing data such as authentication, integrity, and rejection.

Security parameter (K), chosen by the user when he creates a public and secret key. The parameter k determines the number of quantities of the signature length. Message (M), which is a set of messages that a signature algorithm can apply. Verification algorithm (V) for verifying true or false signatures. Figure 5. shows a digital signature scheme.

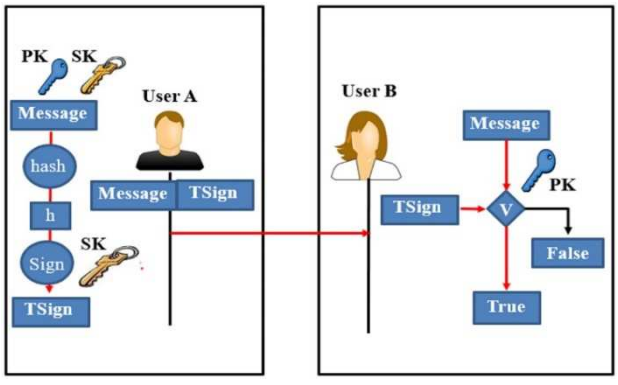

Fig. 5 Scheme in digital signature cryptography

In Figure 5, user A and user B make communication where user B knows the public key of user A. User A creates a message (timestamp) to make a signature. The message is processed using a hash function to generate a hash value (h). The hash value will be entered into the Signature Algorithm to create a timestamp digital signature (TSign) using the secret key (SK) of user A. The message and signature are sent

to user B. After user B receives a message from user B, the message and TSign will be verified using user A's public key (PK). If the value of the message is proper with TSign, hence the message received is valid.

In the scheme that we propose, we combine digital timestamp signatures using ECDSA and CP-ABE, where the process for our ciphertext encryption includes a timestamp for providing data integrity services.

III. Result and Discussion

Our previous work made a scheme [8] for securing the data; we used the CP-ABE method with static attributes and revocation users. We improve our system with dynamic attributes, adopt digital signatures to build the authentication features, and download data integrity. To ensure data does not change during the process downloaded by users, we include digital timestamp signatures using elliptic curve cryptography. Elliptic curve cryptography is a public key cryptographic approach based on elliptic curve algebraic structures over a finite plane. ECC requires smaller keys than non-ECC cryptography to provide equal security [12]. Figure 6 shows our research scheme by including a digital time stamp. We add digital timestamps in the scheme to guarantee users of data integrity. Data will not change during collecting data from the Data Center until the user receives the data. The difference between our methods from the previous work is that the user can update the attribute with a new rule. For example, if the user from the agricultural division wants to migrate to the farm division, then he can change the attribute with confirmation from TTP to change his new attribute.

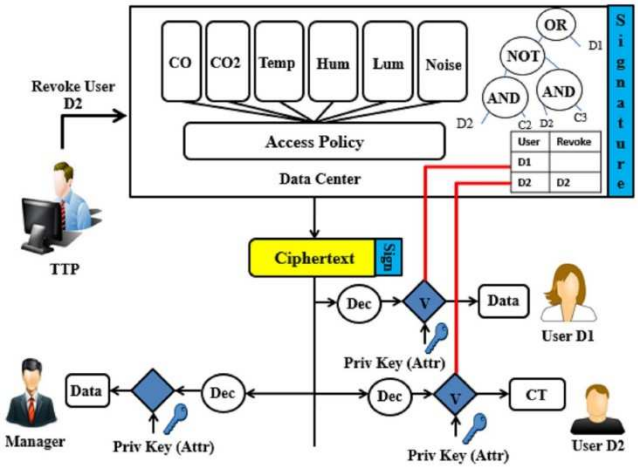

Fig. 6 Scheme design system in our previous research

In Figure 7 We include a timestamp digital signature in ciphertext to authenticate and provide guarantees of data that has not changed during the request process by the user. The user makes requests data to the system and the system responds to the user's request and sends data, before the data is received to the user, it will be encrypted using the CP-ABE method and time stamp, when the user makes a request then the time of requesting from the user's will be entered in the hash value to create a digital timestamp using the Elliptic Curve method Cryptography. When digital signature encryption and timestamps are complete, digital signatures and digital ciphertexts are sent directly to the user. Users who receive ciphertext and digital timestamps from the system cannot directly read the data. Users who want to get the original data must be encrypting the ciphertext. If the user is not in the revoked user, then the user can complete the decryption and get the original data. The original data is then taken by the timestamp to be checked into the verification algorithm for the comparison value with the time stamp digital signature that has been downloaded, if the value in the verification algorithm is the same, then the data has does not change during the process and authenticity, and data integrity is guaranteed.

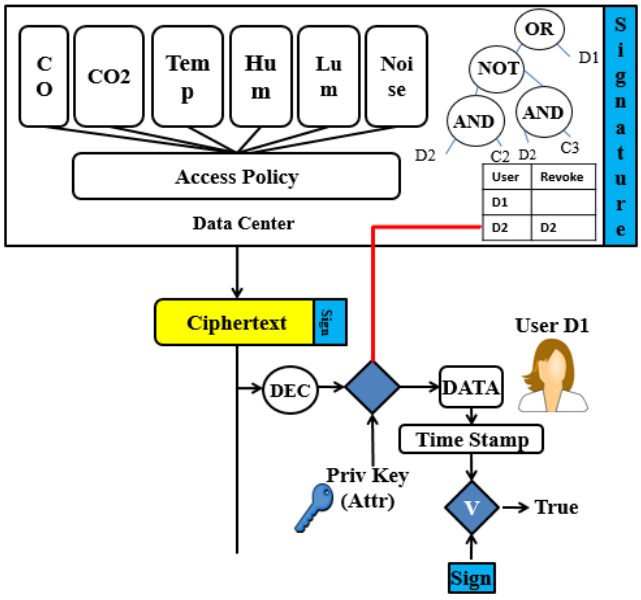

Fig. 7 Scheme design system in our proposed system using ECDSA

We develop our system to collect all data in an environmental monitoring system using wireless sensor technology. We use WSN devices with six sensors, including carbon monoxide, carbon dioxide, humidity, noise, temperature, and luminosity. We use the meshlium devices to store all sensor data sent by each node. To send data sensors from nodes to our meshlium devices using Zigbee, the data center will be synchronized with meshlium devices to obtain data sensors. All data in the data center is secured using the CP-ABE method. Only registered users and users with access rights can access the system and obtain original data. Our system not only secures data centers using encryption and decryption but guarantees integrity in data and can also be revoked for users. We apply encryption based on ciphertext attributes with digital time extraction and signature with elliptic curve cryptography using PHP programs with web-based communication systems for all protocols. All users can access the data center with web-based communication using a computer, laptop, or smartphone. Users in the revocation list cannot read and obtain original data from the Data Center in our system. Figure 8. shows the sensors of our system's data security scheme in environmental monitoring.

In Figure 8, we show our secure system scheme for environmental monitoring systems. User 1 and User 3 register their identity to the system. A third-party trust will confirm user identity to store in the data center. When data from user 1 and user 3 is stored in the data center, the system immediately sends a private key to user 1 and user 3 to be

used for decrypting the ciphertext to get the original data when the user makes access to the system. in our system, we make 4 (four) protocols for communication. There are registration protocols, data sharing protocols, protocol update attributes, and revocation protocols.

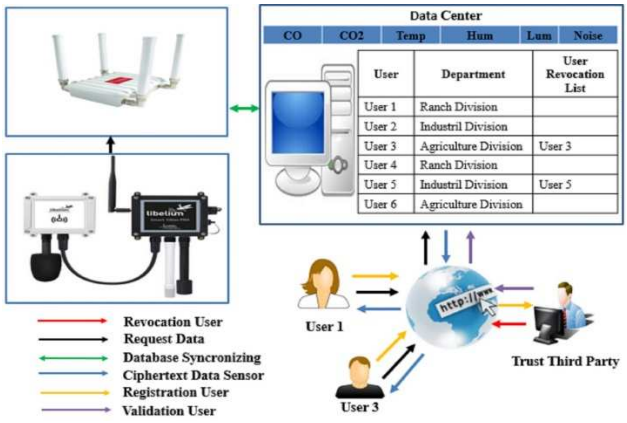

Fig. 8 Scheme design system secure data exchange in environmental monitoring

A. Registration Protocol

The registration protocol is the first process in the system for users to access the system. The user must complete registration to the system. Users send their identities (including user attributes) to the system. Data sent from users will be confirmed by third-party trust trustees to be stored in the data center when data from users is stored in the data center. The system will be sent to the user's private key and public key. The private key will be used to decrypt the ciphertext when the user gets the ciphertext from the data center, in Figure 9 we show the registration protocol.

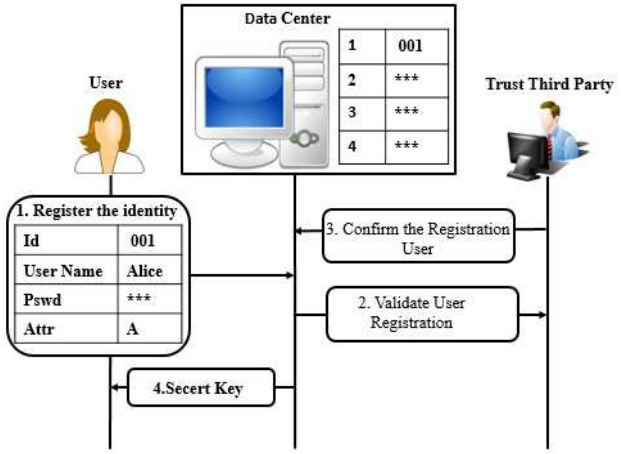

Fig. 9 Scheme for registration protocol user

B. Data Sharing Protocol

Users who have registered with access rights can obtain data in the system. Users must log in using their username and password to get data sensors. Users who want to get data must include the date and type of sensor data. When the user enters the date and type of sensor data they want to download, the system will send digital time signatures and data in the form of ciphertext. Ciphertext cannot be read by the user. To read the contents of the data, the user must do the decryption process in the ciphertext to get the original data. Users use a private key to decrypt ciphertext if the user attribute is following the ciphertext access policy, users can obtain original data. They can also try to verify the original or fake data using a verification algorithm in the system to compare the timestamp when the user downloads the data with the time stamp digital signatures, but if the user attribute is not following the access policy rules in the ciphertext, the decryption process will fail, Figure 10 shows the data sharing protocol.

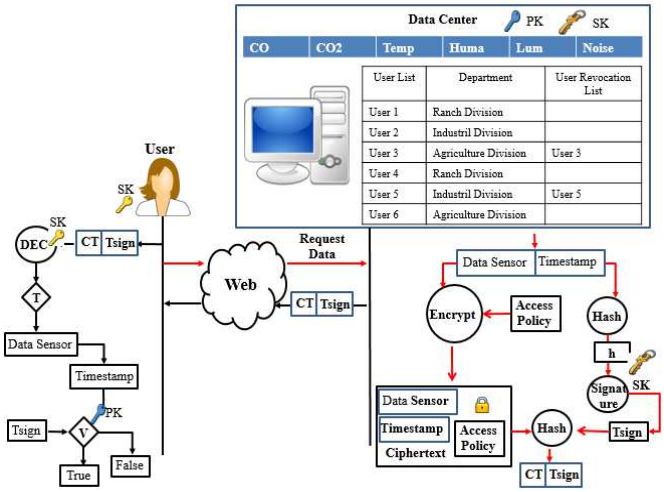

Fig. 10 Scheme for registration protocol user

C. Updating Attributes Protocol

The original CP-ABE [9] and our previous method [8] have a static attribute. When the keygen generates an SK related to the user's attributes, the attribute cannot be changed. SK can only generate a key is once for each request with the attributes of each user. Attributes from the user that have been generated by keygen cannot be updated. We improve our system in CP-ABE for updating attributes in this key that have been generated by keygen. Users can make requests on the system to update their attributes in the keys that they had. The process for updating attributes user shows in Figure 11.

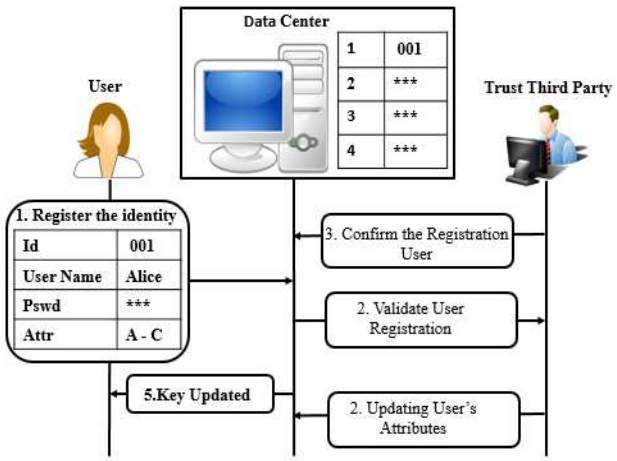

Fig. 11 Process updating attributes from the user

In figure 11, we show the process for updating attributes of a user's key. The user requests into the system to update its attributes. For example, the user has to attribute A, and then the user wants to change the attribute to B. User request will be validated by the Trust Third Party for making a

confirmation to the Data Center. When the confirmation process is done, the system will update the attributes from the user's key. Hence attributes from the user's key will be changed.

D. Revocation Protocol

Registered users with access rights can access the system to get data from the data center, but the system will monitor their access. If the user makes illegal access, the user will immediately be included in the revocation list. Revoked users can access the data center, but they cannot do the decryption process to get the original data because their attributes are updated on our system how users enter in the category of illegal access. The user makes illegal access when he tries to decrypt the sensor data without their own rules and access rights when the user registers. The user has not met the rules in the ciphertext that decrypted; it will fail. This activity will be recorded in the system. TTP will be monitored by users who make illegal access. If the user makes illegal access, then the TTP will save the user in the revocation list. Users in the revocation list can access our system and make requests to update it associated with the system. Even though user attributes can be updated, users in the revocation list cannot do the decryption process. Process for revoking user shows in Figure 12.

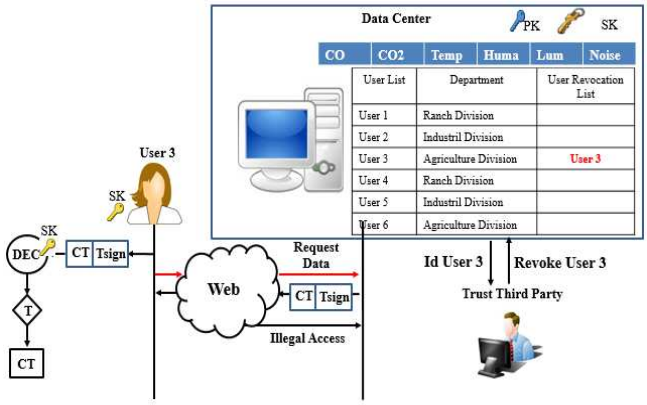

Fig. 12 Rule of policy each (T) group in the ciphertext.

Each user attribute is related to data sensors for each rule in the access policy in this system. We create and divide users into 3 (three) groups and data sensors with 3 (three) rules for access policy. Each group's rule will be used to encrypt and decrypt the data sensor for getting the plaintext in the Data Center. The group for users is D1 is the ranch division, D2 is the agriculture division, and D3 is the industrial division. We divide into three groups to make access rules. These groups will be used to monitor users for illegal access where groups such as C1 are data sensors for CO and CO2, C2 for humidity and temperature, and C3 for luminosity and noise. We select the attributes of each group from the user division to encrypted and then for decrypting data in the data center. We create a policy rule (T) with each group for data sensor encryption and decryption. Group 1 with the policy rule (T1) to decrypt all data sensors in the system. Group 2, where the policy rule (T2) only decrypts C2 and C3 groups in the data center. Group 3 where the policy rule (T3) can only decrypt C1 and C2 data in the data center. Users who make illegal access where they did a decryption process without their own rules will be included in the third-party trust revocation list, where their attributes will be updated using the "NOT" logic in the policy rules. The rule of policy permission shows in figure 13.

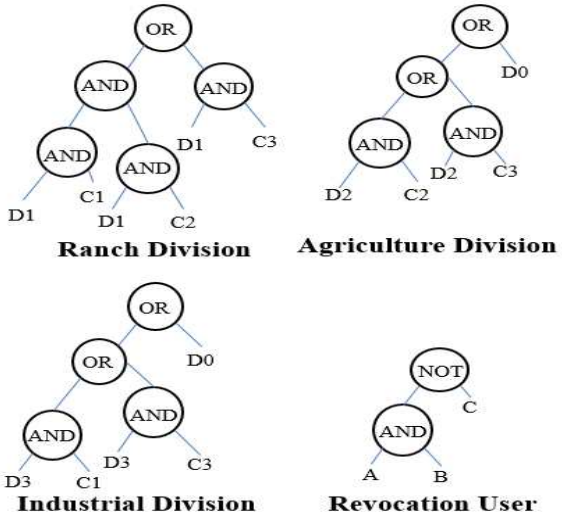

Fig. 13 Rule of policy each (T) group in the ciphertext.

We develop our system using PHP programs with HTTP protocol for communication between the data center, trusted third party, and all the users through local area networks using wireless communication. In this research for the specification of device, hardware, and software in Table I below:

TABLE I
SPECIFICATION OF HARDWARE AND SOFTWARE

Specifications	Actor	
	Data Center	All Actor
Hardware	Intel Xeon CPU E3-1225 3.20 GHz, 4GB DDR3, Dell Precision T1650	Intel core i3-3110M 2.4GHz, 4GB DDR3, Lenovo G400s
Operating System	Ubuntu Linux 16 kernel 4.4.0-22	Windows 10 64-bit
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.	Mozilla Firefox Browser-60.0.2
Wireless Communication	Access Point TP-LINK TL-WA901ND IEEE 802.11n, IEEE 802.11g, IEEE 802.11b	Qualcomm Atheros AR9485WB-EG

Our system only sends data to users who registered earlier. Registered users can update their attributes on the SK by requesting the system. Users without access rights can only see the current conditions from the last data sensor. If the user wants to get information from our system, the user must be registered and make a registration to the system. User identity who makes registering data will be validated by a trust third party stored in the data center. When user registration is complete, the private key will be sent to the user. Figure 14 shows the current condition of the environmental monitoring system when the user logs in to the system.

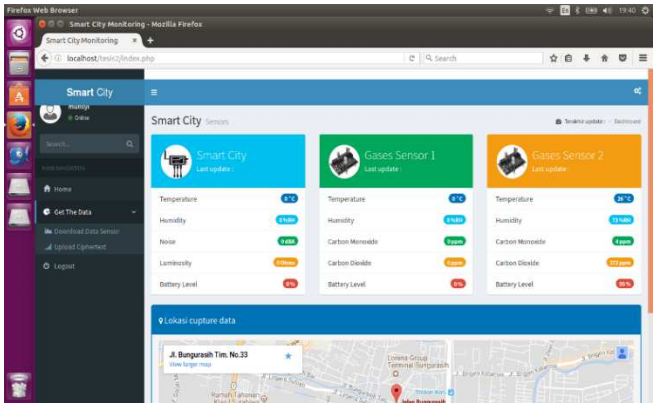

Fig. 14 Current conditions the data sensor in the system

When a user is entering the system, the user can get the data sensor to request the system and update the attribute. In the system for getting the data sensor, the user requests into the system to get the data, and the system responds from the user's request and then sends the ciphertext to the user. Users cannot read the contents of data directly because the data is still ciphertext. If the user wants to get the content and read the original data in the ciphertext, the user must do the decryption process in the system using their private key. In figure 15 shows the form for the user to download the data.

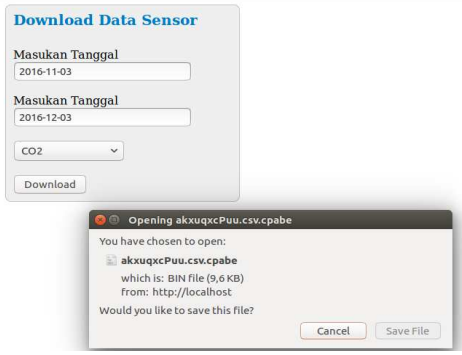

Fig. 15 Form to download the data sensor for the user

After the user gets the ciphertext from the Data Center in our system, the user can choose the decryption menu in the system. All users can upload ciphertexts and private keys to the system to obtain original data. If the user's private key is appropriate with the policy rules in the ciphertext, the ciphertext will be decrypted into the plaintext for getting the original data. When the decryption process is successful, the contents of the sensor data can be seen and read by the user. In figure 16. we show the process of decrypting the successful ciphertext.

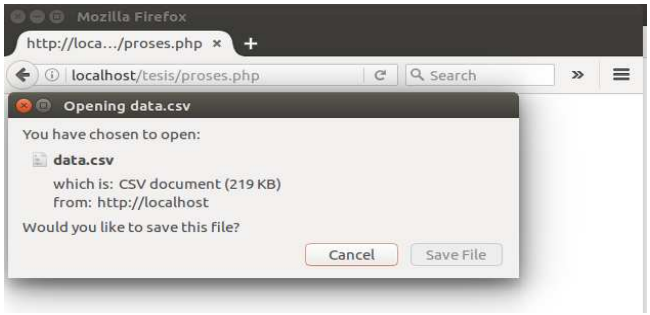

Fig. 16 The original data after decryption was a success

Figure 17 shows users who want to make a decryption process the ciphertext in the system. Users in the revocation list can access the system and get data in the data center. All data downloaded by users in the revocation list is still in the form of ciphertext. There needs to be a ciphertext decryption process to obtain original data and view content in the data sensor. All revoked users cannot successfully decrypt the ciphertext. Hence user attributes are updated by a trusted third party.

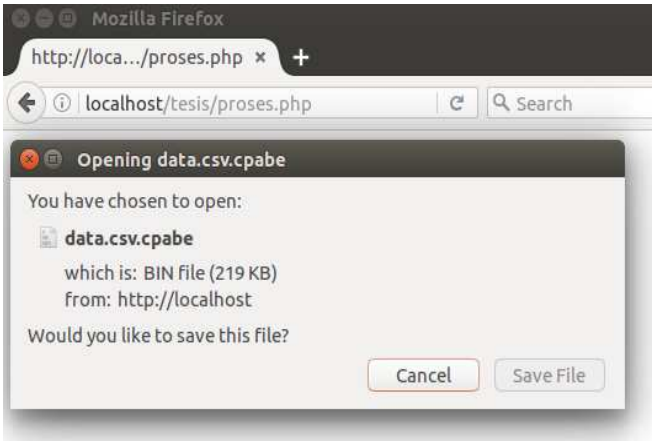

Fig. 17 The decryption ciphertext failed by the revoked user

We analyzed computation from our previous work using static CP-ABE attributes with dynamic CP-ABE such as time for encryption, decryption, verification processes with timestamps, and revocation checks using data sensors for one month with different variation rules policies to each division. We compare different processing times for users in revocation lists and users with access rights. We compare the processing of time for encryption and decryption and signing and verifying digital timestamps with all access policy rules for all data in the ciphertext between users with access rights and users in the revocation list. We analyze the time processing with one-month data for each rule of policy (T) and 1000 users in the revocation list, and also, we analyze the increased data sensor to the ciphertext. The list of different size ciphertext between the user with access right and user in revocation list shows in Figures 18, 19, and 20.

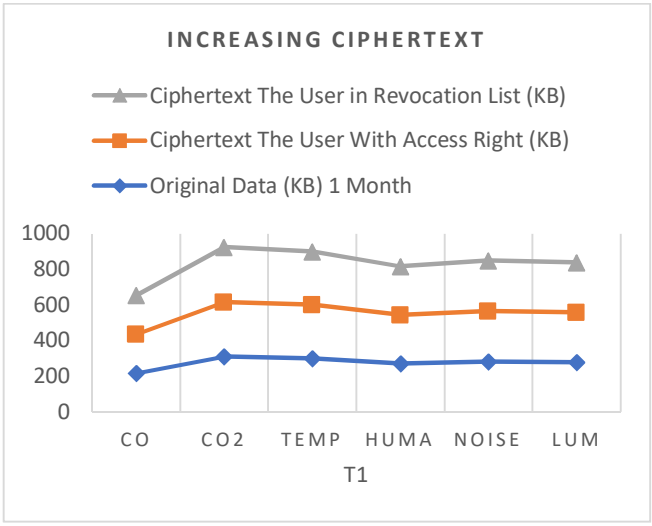

Fig. 18 Increasing size of ciphertext between user with access right and user in revocation list for T1

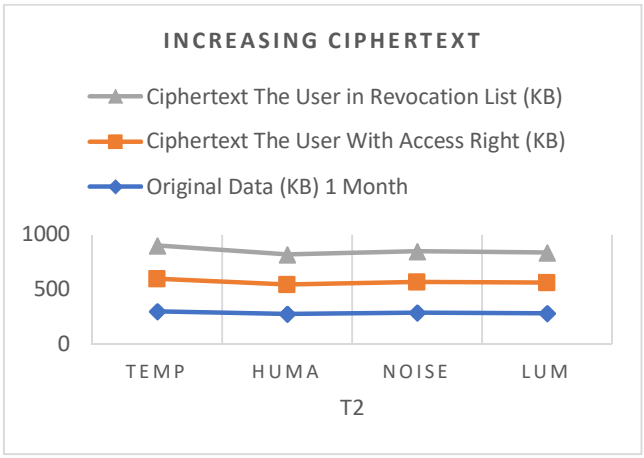

Fig. 19 Increasing size of ciphertext between user with access right and user in revocation list for T2

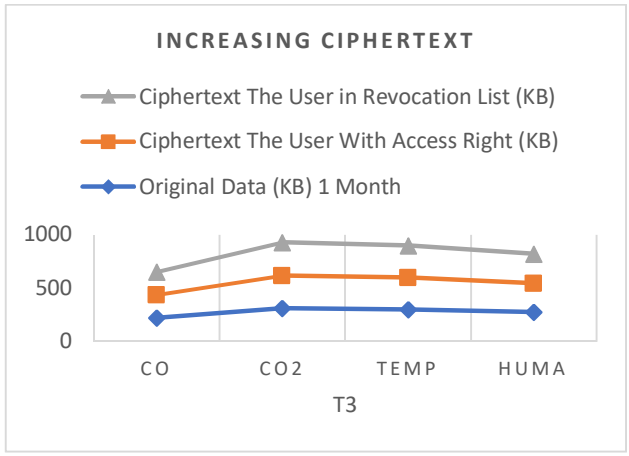

Fig. 20 Increasing size of ciphertext between user with access right and user in revocation list for T3

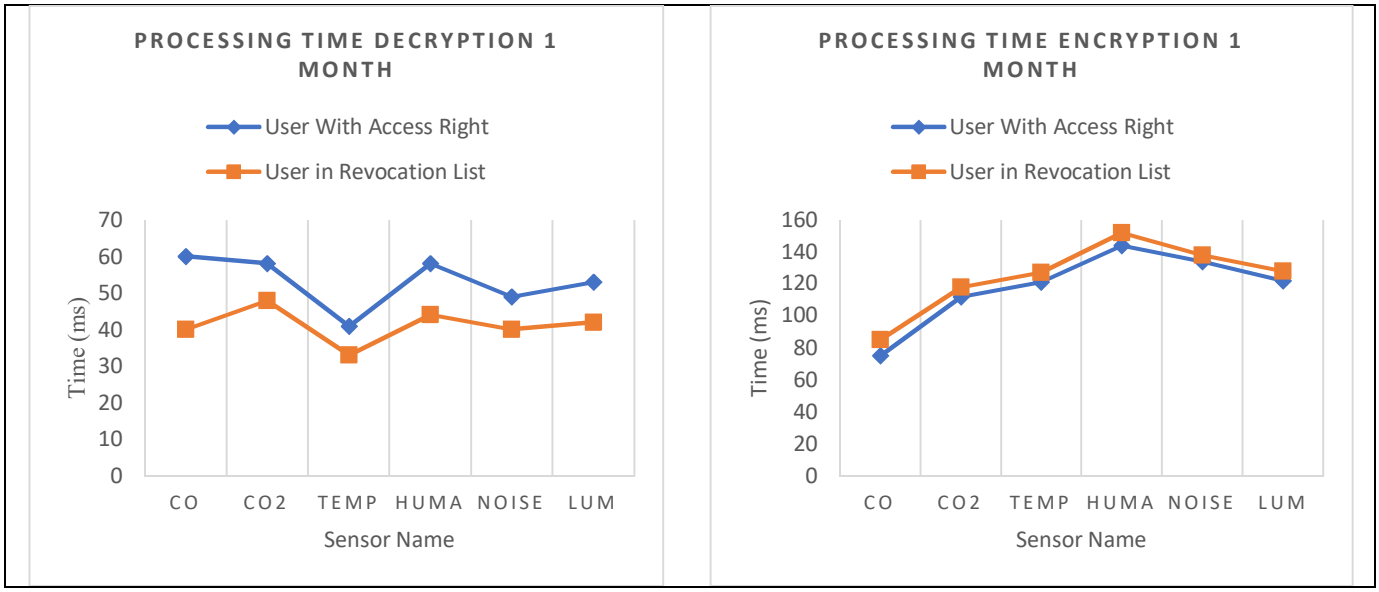

Fig. 21 Processing Time for the rule of acces (T1)

In figure 21, there is only less than 160 ms to encrypt 1 month from data sensors and less than 60 ms to decrypt ciphertext for users with access rights and 17 ms to sign, and 20 ms to verify digital time stamp signatures. For users in the revocation list requires less than 165 ms for encrypting 1-month data sensor and less than 50 ms for decrypting the ciphertext. Revoked users cannot verify digital timestamp signatures.

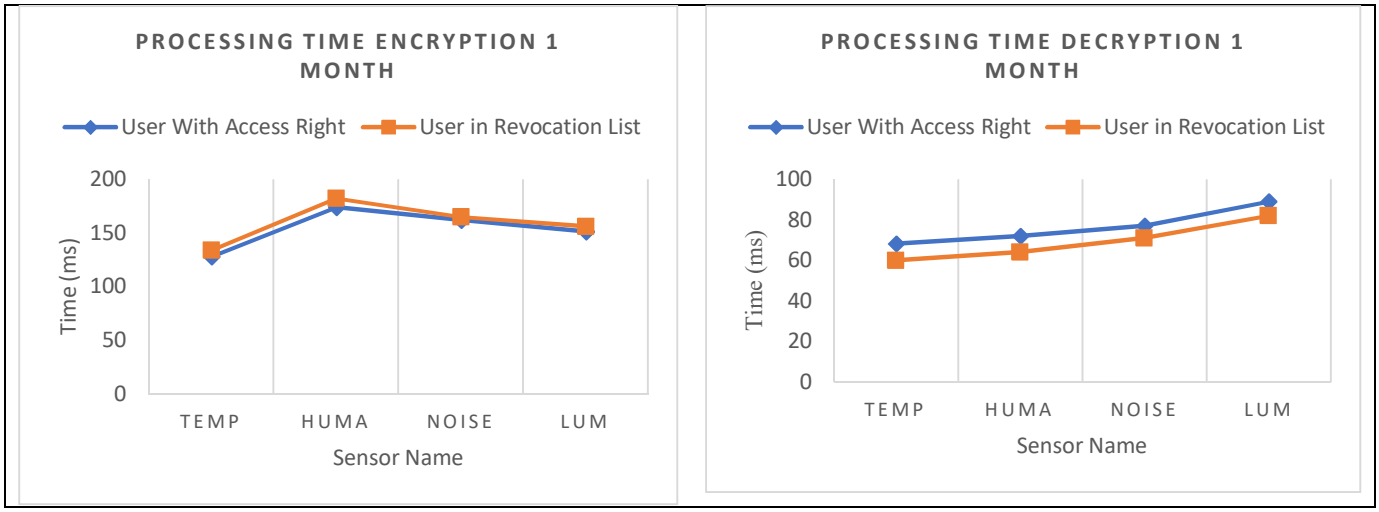

Fig. 22 Processing Time for the rule of access (T2)

In Figure 22, there is only less than 177 ms to encrypt 1-month sensor data and less than 75 ms to decrypt ciphertext for users with access rights and 17 ms to sign, and 20 ms to verify digital time stamp signatures. For users in the revocation list, it takes less than 183 ms to encrypt 1 month of data sensors and less than 83 ms to decrypt the ciphertext.

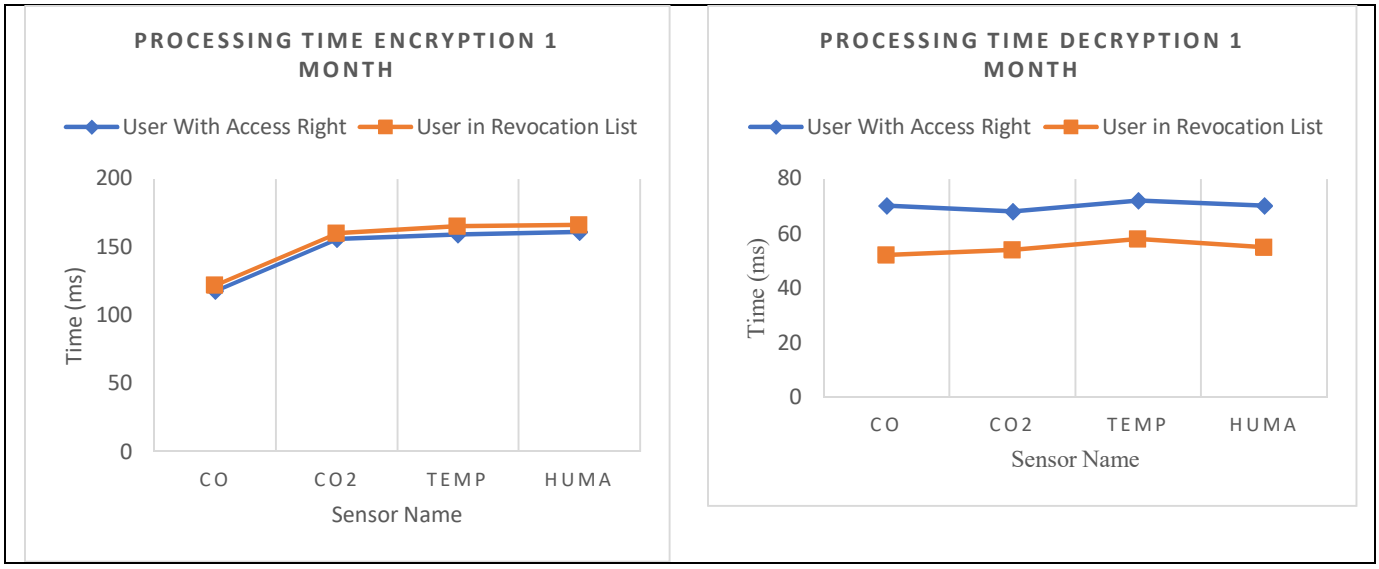

Fig. 23 Processing Time for the rule of acces (T3

In figure 23 there are only less than 170 ms to encrypt 1 month sensor data and less than 74 ms to decrypt ciphertext for users with access rights and 17 ms to sign and 20 ms to verify digital time stamp signatures. For users in the revocation list, it takes less than 180 ms to encrypt 1 month of data sensors and less than 67 ms to decrypt ciphertext. We also analyzed the revocation checks time for the number of revoked users, in figure 24. shows the revocation check with the number of revoked users from 10 users until 100 users. In the system only needs less than 2 Second for checking 1000 revoked users.

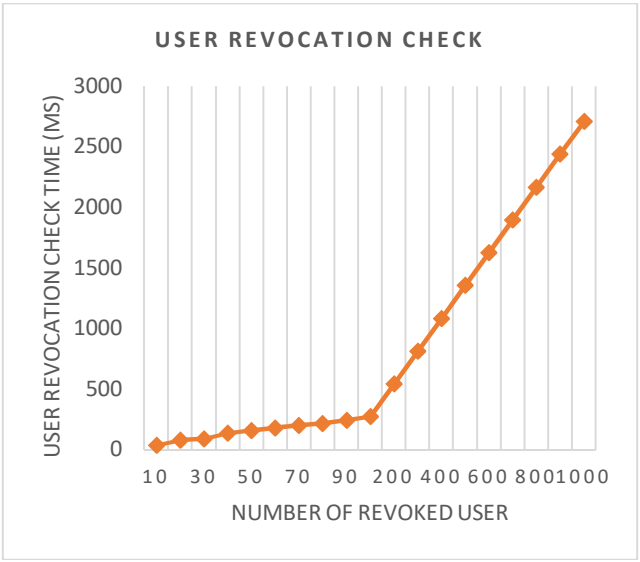

Fig. 24 Revocation check for number of revoked users

IV. Conclusion

We enhanced our system with dynamic attributes from our previous work. This research found that the system does not affect the computation time such as encrypting, decrypting, and verifying process. Also, the digital timestamp signature in the system supported the data integrity and non-repudiation service in the security system from our previous research [8]. The system offered guarantee for the originally of the data since the process from the data center to the user Using CP-ABE with ECDSA does not affect performance in the system. There is only less than 30 ms required for signing and verifying. We compared our previous work using CP-ABE without authenticated with the proposed scheme using ECDSA for security mechanism. Our system with adopted ECDSA gives the additional security aspect in the data sensor such as the data is genuine from the Data Center. The Data Center cannot reject the data received by users, and it is provided in the Data Center for users that the data has been received is genuine and provides the security aspect for users from replay attacks. The system's performance can be implied to the environmental monitoring system in IoT with revocation check for the number of revoked 100 users only needs less than 300 ms. The system will be secure, and all the data sensors in the data center will be safe. The revocation mechanism to revoke the users are similar to our previous work, only the trust third party can do the validation and confirmation the data from the users to the system to be stored in the data center, and only the trust third party can do the revocation to the user if the user who did illegal access to the system.

References

[1] N. Fahmi, S. Huda, A. Sudarsono, and M. U. H. Al Rasyid, "Fuzzy logic for an implementation environment health monitoring system based on wireless sensor network," *J. Telecommun. Electron. Comput. Eng.*, vol. 9, no. 2–4, pp. 119–122, 2017.

[2] A. Lanzolla and M. Spadavecchia, "Wireless sensor networks for environmental monitoring," *Sensors (Switzerland)*, vol. 21, no. 4, pp. 1–3, 2021, doi: 10.3390/s21041172.

[3] N. Fahmi, M. U. H. Al Rasyid, and A. Sudarsono, "Adaptive Sleep Scheduling for Health Monitoring System Based on the IEEE 802.15.4 Standard," *Emit. Int. J. Eng. Technol.*, vol. 4, no. 1, pp. 91–114, 2016, doi: 10.24003/emitter.v4i1.115.

[4] M. F. A. Muhammad Rashidi Wahab, “Jurnal Teknologi,” *J. Teknol.*, vol. 3, pp. 31–39, 2013.

[5] A. Sudarsono and T. Nakanishi, “An implementation of secure data exchange in wireless delay tolerant network using attribute-based encryption,” *Proc. - 2014 2nd Int. Symp. Comput. Networking, CANDAR 2014*, pp. 536–542, 2014, doi: 10.1109/CANDAR.2014.34.

[6] L. Touati, Y. Challal, and A. Bouabdallah, “C-CP-ABE: Cooperative ciphertext policy attribute-based encryption for the internet of things,” *Proc. - 2014 Int. Conf. Adv. Netw. Distrib. Syst. Appl. INDS 2014*, pp. 64–69, 2014, doi: 10.1109/INDS.2014.19.

[7] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, “A decentralized approach for security and privacy challenges in the Internet of Things,” *2014 IEEE World Forum Internet Things, WF-IoT 2014*, pp. 67–72, 2014, doi: 10.1109/WF-IoT.2014.6803122.

[8] Munsyi, A. Sudarsono, and M. U. H. Al Rasyid, “Secure data sensor in environmental monitoring system using attribute-based encryption with revocation,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 7, no. 2, pp. 609–624, 2017, doi: 10.18517/ijaseit.7.2.2175.

[9] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” *Proc. - IEEE Symp. Secur. Priv.*, pp. 321–334, 2007, doi: 10.1109/SP.2007.11.

[10] A. Sudarsono, T. Nakanishi, Y. Nogami, and N. Funabiki, “Anonymous IEEE802.1X authentication system using group signatures,” *J. Inf. Process.*, vol. 18, pp. 63–76, 2010, doi: 10.2197/ipsjjip.18.63.

[11] A. Sudarsono, P. Kristalina, M. U. H. Al Rasyid, and R. Hermawan, “An implementation of secure data sensor transmission in Wireless Sensor Network for monitoring environmental health,” *Proceeding - 2015 Int. Conf. Comput. Control. Informatics Its Appl. Emerg. Trends Era Internet Things, IC3INA 2015*, pp. 93–98, 2016, doi: 10.1109/IC3INA.2015.7377753.

[12] A. H. Koblitz, N. Koblitz, and A. Menezes, “Elliptic curve cryptography: The serpentine course of a paradigm shift,” *J. Number Theory*, vol. 131, no. 5, pp. 781–814, 2011, doi: 10.1016/j.jnt.2009.01.006.