Vol. 1, No. 1, 2023
ISSN: 2987-3932
https://pubs.ast-ptm.or.id/index.php/eat

Secure Data Sensor Access for Environmental Health Monitoring in the Pandemic Covid-19 Era with Ubiquitos Computing using Attribute Based Encryption

Windarsyah [a,1,*], Ichwan Setiawan [b,2], Munsyi [c,3], Rudy Ansari [d,4], Mukhaimy Gazali [d,5]

[a] Informatics Universitas Muhammadiyah, Jalan S. Parman, Banjarmasin, Indonesia
[b] Civil Engineering Universitas Muhammadiyah, Jalan S. Parman, Banjarmasin, Indonesia
[c] Communication and Islamic Broadcasting Universitas Islam Negeri Antasari, Jalan A.Yani Km 4,5, Banjarmasin, Indonesia
[d] Informatics Universitas Muhammadiyah, Jalan S. Parman, Banjarmasin, Indonesia
[1] windarsyah@umbjm.ac.id*; [2] ichwan@umbjm.ac.id; [3] munsyi@uin-antasari.ac.id; [4] rudy@umbjm.ac.id; [5] mukhaimy.gazali@umbjm.ac.id
* Corresponding Author

ABSTRACT

In the pandemic covid-19 era, health environment become the most important issue for reducing the increase in cases that occur. On the internet of things era, many researchers are using Ubiquitos Computing with integrating Wireless Sensor Network (WSN) technology to obtain the data for Environmental Health health monitoring system. All of collected data from WSN will be sent and stored in the Data Center, where all of the data can be accesed by users using their end devices such personal computer, laptop and smart phone. The Data Center without security mechanism system it would be very dangerous, because anytime and anywhere every single user can make an intercept, track and even modified of the data. The system need a security mechanism to ensure the confidentiality all of data in the data center with the authenticity in the data will not be changed during the collection process. Ciphertext Policy Attribute-Based Encryption (CP-ABE) is the one of solutions for securing the security, confidentiality, and authenticity of the data with encrypting process where only users with appropriate rule of policy can make a process for decrypting to get the original data. The system with CP-ABE security mechanism is not only securing the data but also providing the guarantee in the data that is no changes during the collection prosess of the data from the Data Center on the ubiquitos computing. the process for encrypting and decrypting the data using CP-ABE only need 160 ms on the process encryption and 60 ms on the process decryption.

KEYWORDS
Internet of Things
Ubiquitos Computing
Wireless Sensor Networks
Security Mechanism
CP-ABE

1. Introduction

Every single country in the world currently facing a fairly deadly outbreak, namely is the corona virus or known as the covid 19 virus. The spread of this virus is so very fast and easy to infect the someone in with someone infected this virus. To suppress the spread of this virus, it takes a strong immune system and a healthy environment. In the Revolution Industry 4.0, recently many researchers using Wireless Sensor Networks (WSNs) technology to implementation in many applications with integrated on Ubiquitos Computing. One of them is an application for environment monitoring system [1][2][3][4]. The Environmental Health monitoring system using WSN technology and ubiquitos computing for collecting the data such as carbon monoxide (CO), carbon dioxide (CO2), humidity, luminosity, noise, and temperature. Every sensing data was collected by WSN will be send to the ubiquitos computer and then to saved in the Data Center. The data was collected by ubiquitos computer from WSN will be synchronized and saved in the Data Center. All of the the Data in the Data Center is easily read by all of every single users [5]. The user can access the system through HTTP protocol with web based communication. The Environmental Health health monitoring system can be accessed using end devices such personal computer, laptop, and smartphone. The Data Center without security mechanism access can be intercepted, tracked and even modified by the user [6].

The system requires a security mechanism for securing the data sensor in the Data Center. Before the data will be sent to the user, All of the data in the Data Center must be secured with encryption process. Only user with the permit access can get the original data from the Data Center using decryption process.

To provide security mechanism in the data, there is must be able an security aspect twhre is the system give the secure the data. There is privacy, confidentiality, and integrity [6]. Privacy is mean the data is unexposed. Confidentiality is mean during the process of exchange in data is kept undisclosed to others[7][8]. Integrity is mean the data guaranteed, safeguarding correctness of information. No one user is able to access or modify, delete, create and reply the data sensor[9]. To give the system for protecting the access in the data center then all of the data sensors in the Environmental Health monitoring system there are have many methods from the researchers. One of them is ciphertext policy attribute- based encryption. The researchers using the CP-ABE method with combining hash message authentication code to give the authentication in the data sensor. The researcher using CP-ABE in DTN for mobile network communication [4][10]. In this paper, we propose a security mechanishm for protecting the Environmental Health monitoring system to protect all of the data in the Data Center and give the user the guarantee that the data are genuine.

The contribution of this research is we implementation of CP-ABE through the HTTP protocol for communication using PHP programs in embedded system for ubiquitos computer using raspbery pi3 for node in the system before the data sensor will be send to the data center. This security mechanism will protect all of the data in the data center with encrypted process in the data to become ciphertext before sending to the user and decryption process for getting the original of the data. The system can be accessed by the user at wherever and whenever using their end devices such a laptop, personal computer, and smartphone.

Structure organization of this paper as follows. In Section 2, we describe about our adopted method CP-ABE, In Section 3, we explain our proposed secure data exchange in Environmental Health monitoring using CP-ABE and we present the implementation of our system in the proposed scheme with analyze the experiment result and measurement. In Section 4 we explain the conclusion and discuss the security mechanism in our systems.

2. Method

We adopted and we describe the CP-ABE [11] and implementation it for our research, a message (M) ecrypted using the public key (PK) with access policy that associated with user attributes [12]. The rule of access policy in ciphertext is expressed by the logical on attributes from users. Each user has a set of attributes to expressed information.

2.1 Scheme of CP-ABE

In the CP-ABE security mechanism there are have four steps involved in the process for securing the data [11]. The first step is setup, Setup is the first process in CP-ABE for generating the keys, The systems generated two keys, there are Master Key (MK) and Public Key (PK). Public and Master key will be used to generate the new key for each the user, there is Secret Key (SK). The second step is Key Generator (Keygen). Keygen is the mechanism in the processof CP-ABE to make a new key that is a secret key for the users. In Fig. 1 we describe the process scheme mechanism for all steps process in CP-ABE.

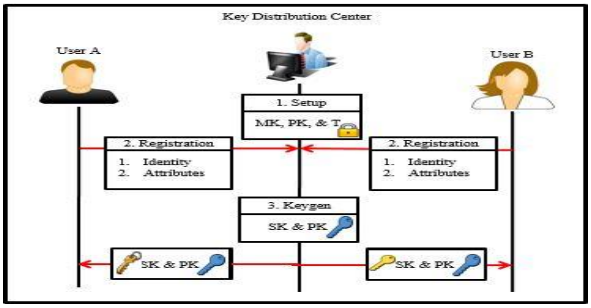

Fig. 1. Scheme Mechanism in Process CP-ABE

2.2 Secure Data Sensor Scheme in Environmental Health Monitoring

In this work we make a scheme in our research to secure the data using the CP-ABE for giving the guarantee in the data will not change during process downloaded by the users. Fig. 2 shown the scheme from our research. The data will not be changed during the process of collecting data from the Data

Vol. 1, No. 1, 2023
ISSN: 2987-3932
https://pubs.ast-ptm.or.id/index.php/eat

Center until received to the user. only user can make a decryption process to the encrypted data from the data center.

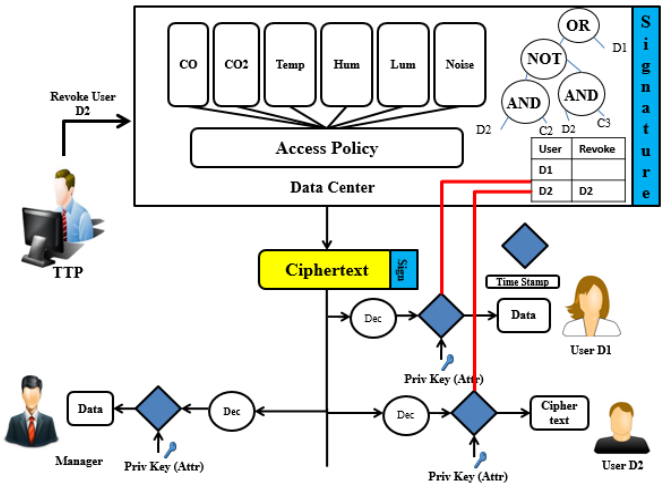

Fig. 2. Scheme design System in the Data Center for Distributing the Access

In this work we make a scheme in our research to secure the data using the CP-ABE for giving the guarantee in the data will not change during process downloaded by the users. Fig. 2 shown the scheme from our research. The data will not be changed during the process of collecting data from the Data Center until received to the user. only user can make a decryption process to the encrypted data from the data center

We proposed our system in the Environmental Health monitoring system with node using raspbery pi 3 including six sensors there are carbon monoxide, carbon dioxide, humidity, noise, temperature and luminosity. We using the microcontroller like the arduino to sensing and send all of data sensor to the node. All of the data in the raspberry pi3 will be synchronized to the data center. All of the data in the data center will be secured using the CP-ABE method, only user's with access right and the user who was finish the registration can access the system and get the original data. Our system not only secures the data center using encryption and decryption but can do the revocation for the user who did the illegal access and give the guarantee of the integrity of the data for the users. We implementation ciphertext attribute-based encryption with revocation using PHP program with HTTP protocol for all communication. The user can access the data center through web based using user's end device such computer, laptop or smart phone. The users without the access right and users in the revocation list cannot read and get the original data from the data center. Fig. 3 shows our scheme system secure data sensor in environmental health monitoring.

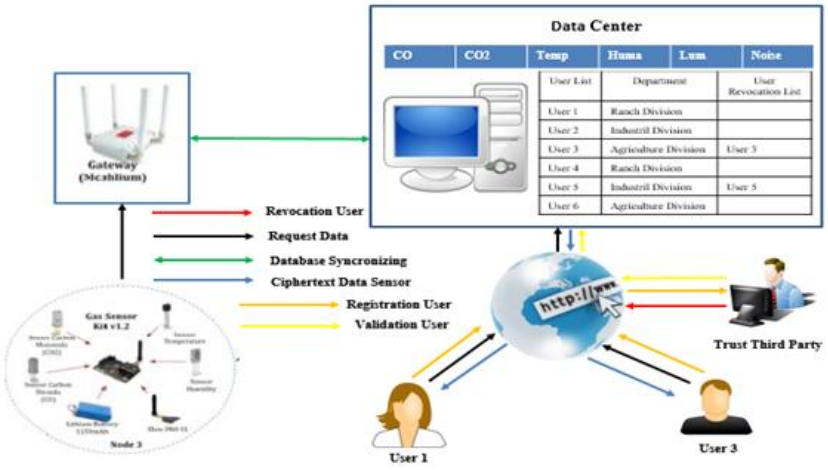

Fig. 3. Proposed scheme design system secure data exchange in Environmental Health monitoring

In Fig. 3 shows the mechanism in our secure system for the Environmental Health monitoring system. User 1 and User 3 make a register with send their identity to the system. The user's identity will be validated by the trust third party to save and stored in the data center. When the data from user 1 and user 3 succes to stored in the data center then the system will send the private key. in our system we create 3 (three) protocol for the communication. There are registration protocol, data sharing protocol, and revocation protocol.

2.2.1 Registration Protocol

The registration protocol is the initial process in the system security mechanism for users to access the system. The user must complete the registration step on the Environmental Health monitoring system. The user fills in and sends his identity (including user attributes) into the system. Data that has been inputted by the user and sent from the user will be validated by a trusted third party to be stored in the data center. When the data from the user is successfully stored in the data center. The data center directly sends the private key and public key to the user. The private key will be used to decrypt the data when the user downloads the data from the data center, in Fig. 4 the built system shows the registration protocol.

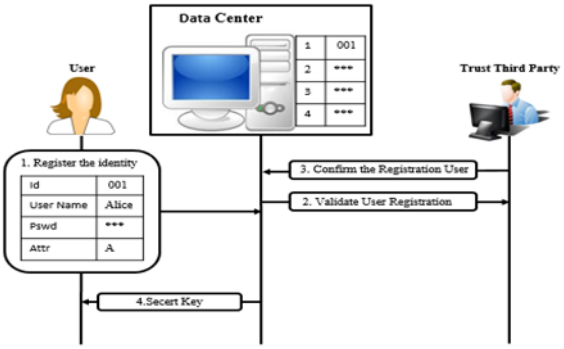

Fig. 4. Mechanism process in the registration protocol

2.2.2 Data Sharing Protocol

Users who are registered and have access rights can make requests to the Environmental Health monitoring system and get data from the data center. Users must first login using a username and password to get sensor data. Users wishing to get data must include the date and type of sensor data. that you want to download when the user enters the date and type of sensor data you want to download, the system will send a digital signature and timestamp data in the form of ciphertext. Ciphertext can not be directly read by users who just got the data, to read the contents of the data, the user must decrypt the ciphertext to get the original data. The user uses the private key to decrypt the ciphertext if the attributes of the user comply with the access policy rules in the ciphertext then the user can get the original data but if the attributes of the user do not comply with the access policy rules in the ciphertext then the ciphertext decryption process will fail, Fig. 5 shows the data sharing protocol.

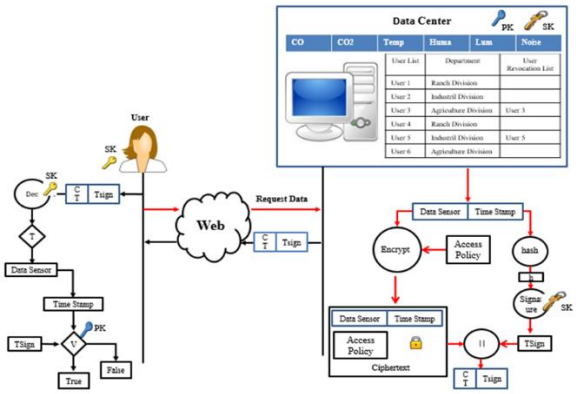

Fig. 5. Mechanism process in the data sharing protocol

Vol. 1, No. 1, 2023
ISSN: 2987-3932
https://pubs.ast-ptm.or.id/index.php/eat

2.2.3 Revocation Protocol

Users with access rights can log in to the system and get data from the data center, but their access will be monitored by the system. If users perform illegal access, they will be put on the revocation list. Users on the revocation list can access the data center but they cannot perform the decryption process to get the original data because their attributes are updated by a trusted third party. How users are categorized in the illegal access category. Users perform illegal access when trying to decrypt sensor data without their own rules and access rights when the user registers. User attributes are related to sensor data. we create and divide users into 3 (three) groups and sensor data with 3 (three) rules for access policies. The user groups are D1 for Animal Husbandry, D2 for Agriculture and D3 for Industry. We divided into three groups to create access rules. The group will be used to monitor illegal access users where C1 is sensor data 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 encrypt and decrypt the data. We create a policy rule (T) with each group for encryption and decryption of sensor data. Group 1 with a policy rule (T1) can decrypt all sensor data in the data center. Group 2 with policy rule (T2) only decrypts C2 and C3 in the data center. Group 3 with policy rules (T3) can only decrypt C1 and C2 data in the data center. Users performing illegal access where they are trying to decrypt from their own rules will be put in a revocation list where their attributes will be updated using a logic "NO" in the policy rule. The policy permission rules are shown in the Fig. 6 and the user performs the illegal access shown in the Fig. 7.

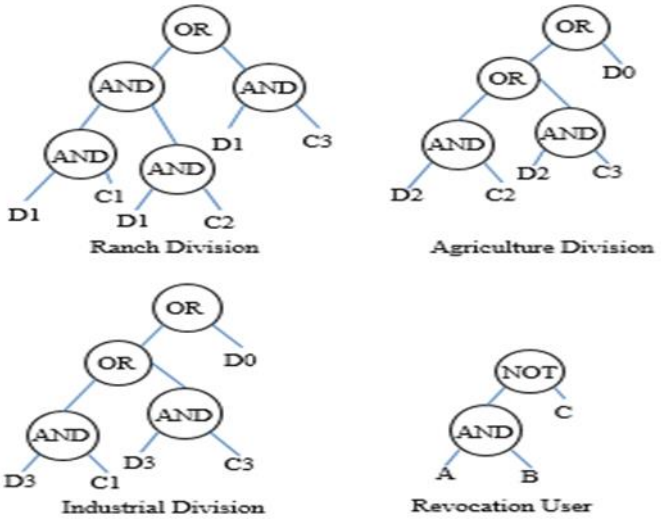

Fig. 6. Rule in the access policy for each group in the secure mechanism CP-ABE

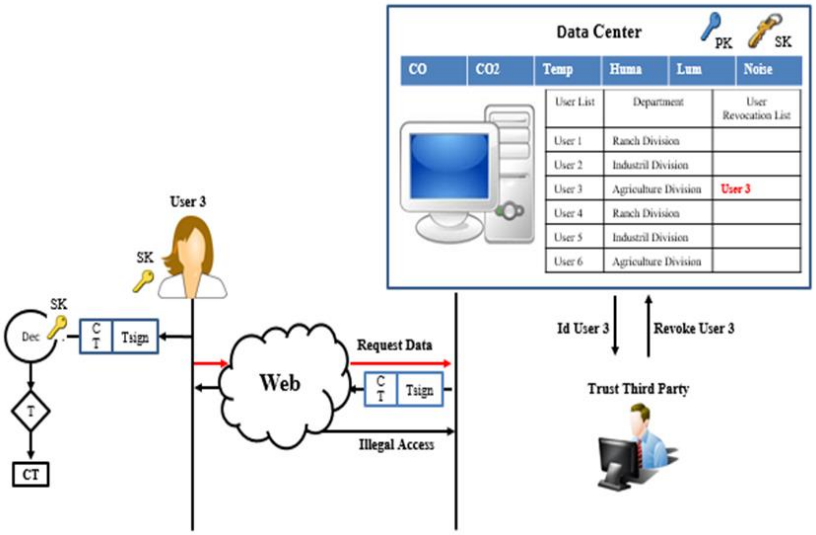

Fig. 7. Mechanism process in the revocation protocol

3. Results and Discussion

We develop our system using PHP programs, where the communication between users,trust third party and the data center uses HTTP protocol with local area network using wireless communication and for each node using raspberry pi 3 and for sensing the data using arduino uno . The specification of hardware and software that we use in this research as seen in Table 1.

Table 1. Specification of hardware and software projects

Actor	Details Hardware	Operating System	Software	Wireless Communication
Data Center	Intel Xeon CPU E3-1225 3.20 GHz, 4GB DDR3, Dell Precision T1650	Ubuntu Linux 16 kernel 4.4.0-22	GMP-6.1.1, pbc-lib-0.5.14, glib-2.34, libbswabe-0.9, openssl-1.0.1e,cpabe-0.11 apache2, Mysql.	Access Point TP-Link TL-WR740N IEEE 802.11n
Trusted Third Party and User	Intel Core i3-3110M 2.4 Ghz, 4GB DDR3, Lenovo G400s	Windows 10 64-bit	Mozilla Firefox Browser-52.0.2	Qualcomm Atheros AR9485WB-EG
Node	Raspberry pi 3 model B	Ubuntu Mate	Python 3	Tp-link TL-WN722N
Microcontroller	Arduino Uno	-	C Programs	Wifi Esp 8266

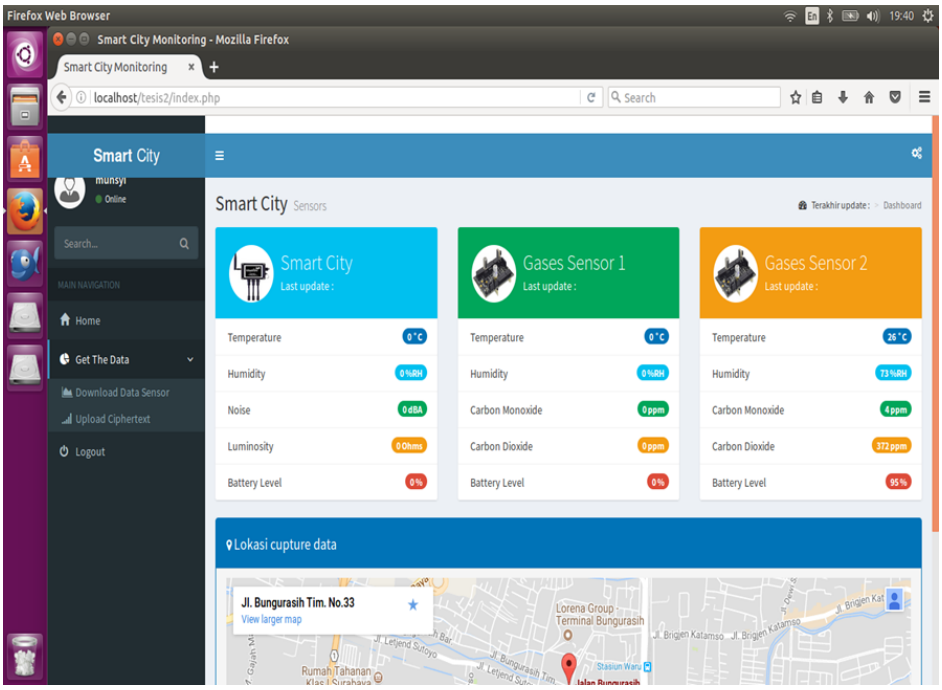

Fig. 8. Dashboard Environmental Health Monitoring System

We analyze the processing time for encryption, decryption, verification and revocation check using the data sensor in one month with the different variety rule of policy for every division for comparing. We compare the different processing time for the user with the access right and the user in the revocation list and also analyze the increase data sensor to the ciphertext. the list of different size ciphertext and the size of timestamp digital signature can be seen in the Table 2. In Table 2 we shows and describe the increase of the ciphertext with each rule policy (T) between the user with the access right and the user in revocation list and also size, If the users in the revocation list are increasing then the size of ciphertext will be increased too, this is because the amount of user to revoked in the rule of policy will be increased. We also analyze the revocation check for numbering of revoked users, in Fig. 9 shows the revocation check with the number of revoked user from 10 users until 100 users. In the system only needs less than 550 ms for checking 100 revoked users.

Table 2. Increase size the ciphertext between the user with access right and the user in revocation list

T	Sensor	Original Data (KB) 1 Month	Ciphertext The User With Access Right (KB)	Ciphertext The User in Revocation List (KB)
T1	CO	217,3	217,9	218,1
	CO2	307,8	308,7	308,9
	TEMP	298,8	300	300,2
	HUMA	271,7	272,6	272,8
	NOISE	282,4	283	283,2
	LUM	278,6	279,3	279,5
T2	TEMP	298,8	298,9	300
	HUMA	271,7	271,9	272
	NOISE	282,4	282,7	282,8
	LUM	278,6	278,8	279
T3	CO	217,3	217,5	217,7
	CO2	307,8	308	308,1
	TEMP	298,8	298,9	300
	HUMA	271,7	271,9	272,1

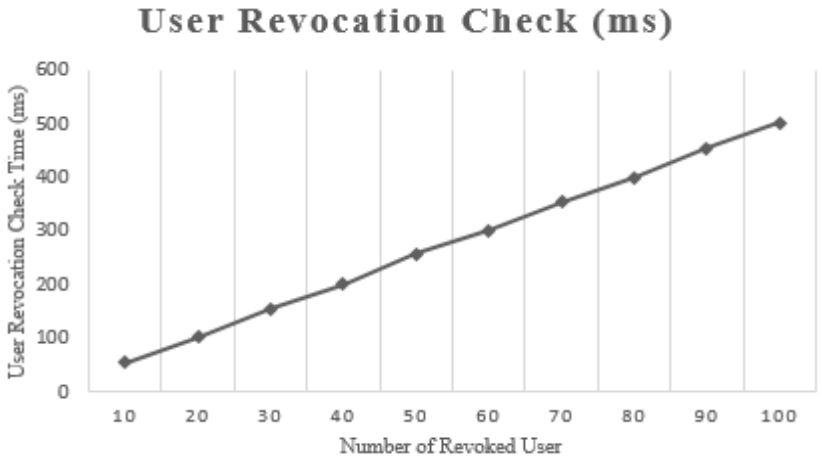

Fig. 9. Revocation Check Time for number revoked users.

4. Conclusion

We use CP-ABE in the Environmental Health monitoring system and provide security mechanisms and guarantee data authenticity and non-repudiation during the process from the data center to the user. The use of CP-ABE does not affect system performance. System performance can be implemented on Environmental Health monitoring systems in Internet of Things Technology with revocation checks for a total of 100 revoked users taking less than 300 ms. The system provides security guarantees and all sensor data in the data center will be safe. Revocation mechanism to revoke users, only trusted third parties can validate and confirm data from users to the system to be stored in the data center and only trusted third parties can revoke users if users have illegal access to the system.

References

[1] 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.

[2] 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.

[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] A. Khalique, K. Singh, and S. Sood, "Implementation of Elliptic Curve Digital Signature Algorithm," *Int. J. Comput. Appl.*, vol. 2, no. 2, pp. 21–27, 2010, doi: 10.5120/631-876.
[9] M. F. A. Muhammad Rashidi Wahab, "Jurnal Teknologi," *J. Teknol.*, vol. 3, pp. 31–39, 2013.
[10] 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.
[11] 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.
[12] K. Saritha, "Block Chain Authentication Using Elliptic Curve Digital Signature Algorithm," vol. 3, no. 2, pp. 71–75, 2020.