Ciphertext-Police Attribute Based Encryption Performance on Notebook Device

[1]I Gede Totok Suryawan
Informatic Engineering
STMIK STIKOM Indonesia
Bali, Indonesia
totok.suryawan@stiki-indonesia.ac.id

[2]Linawati
Electrical Engineering Departement
Udayana University
Bali, Indonesia
linawati@unud.ac.id

[3]Susila Andika
Informatic Engineering
STMIK STIKOM Indonesia
Bali, Indonesia
susilaandika@gmail.com

Abstract— Cryptography is a technique to secure communication or exchange messages between one user with another user, by encrypting the message to be sent guaranteed to be safe from eavesdroppers because the message is equipped with a key that is not possessed by the eavesdropper. One encryption method that can guarantee the security of communication is Ciphertext-Police Attribute Based Encryption (CP-ABE). CP-ABE belongs to the type of public key encryption where the secret key of the user and the ciphertext depends on the user's attributes such as place of birth, position in the organization and other attributes. Ciphertext can only be described if the set of user key attributes matches the ciphertext attribute. This paper discusses CP-ABE performance on notebook devices. Evaluation is carried out on two notebook devices namely MacBook Air (Intel Core i5 1.8Ghz, 8GB RAM) with the MacOS Sierra operating system version 10.12.6. and MacBook Air (Intel Core i5 1.4Ghz, 4GB RAM) with the MacOS Mojave operating system version 10.14.6. Evaluation is carried out on the encryption process and description with the number of attributes from 1 to 30 attributes, with the calculation of the average number of executions, memory and notebook device power. The evaluation results show that the more antributes used as a data access policy, the longer the encryption and description execution time needed, and the more memory and power used. Effect of the largest number of attributes on the average execution time, and power consumption of notebook devices, but not significant on memory usage. Nevertheless CP-ABE is suitable for use in notebook devices.

Keywords— *Cryptography, Encryption, Ciphertext-Police Attribute Based Encryption (CP-ABE)*

I. Introduction

Cryptography is a technique to secure communication or exchange messages between one user with another user, by encrypting the message to be sent guaranteed to be safe from eavesdroppers because the message is equipped with a key that is not possessed by the eavesdropper. Encryption is a process of making messages that can be read (plaintext) into random messages that cannot be read (ciphertext). Generally there are two types of encryption, namely symmetric encryption where the description key is the same as the encryption key, and asymmetric encryption where the description key is not the same as the encryption key.

Attribute Based Encryption (ABE) belongs to the type of asymmetrical encryption. This method was introduced by Sahai and Waters [1] in 2005. ABE is included in the type of public key encryption where the secret key of the user and the ciphertext depends on user attributes such as place of birth, position in the organization and other attributes. Ciphertext can only be described if the set of user key attributes matches the ciphertext attribute. Seen from the ABE access policy it is classified into two schemes [2] namely Key-Police Attribute Based Encryption (KP-ABE) and Ciphertext-Police Attribute Based Encryption (CP-ABE). In the KP-ABE scheme the access policy is placed on the user's private key, and a set of descriptive attributes are in the encrypted data. If a set of attributes meets the access policy, the user can describe the message. Otherwise, the user cannot decrypt the message. Whereas in the CP-ABE access policy is placed on ciphertext, and a set of descriptive attributes resides in the user's private key. If the specified attribute meets the access policy, users can describe user data. This paper will discuss CP-ABE performance in encrypting and describing messages based on the average execution time, memory, and notebook device power.

II. Related Work

The literature survey was conducted on the application of the Attribute Based Encryption (ABE) method [3]. specifically Key-Police Attribute Based Encryption (KP-ABE) and Chipertext-Police Attribute Based Encryption (CP-ABE). In research conducted by [4], in his research implementing ABE in cloud applications with Secure Hash Algorithm (SHA) for authentication, Blowfish Algorithm for encrypting data in the cloud, and Palier Algorithm to create access policies, access files, and file storage processes. The results showed that the algorithm can provide a high level of security to files stored in cloud applications.

Some research on CP-ABE was carried out by [5] in his research proposing ABE with hash functions, digital signatures, and asymmetric encryption methods. An efficient revocation method on CP-ABE for storing data in the cloud by reducing the DO workload proposed by [6], the evaluation results show that the proposed revocation scheme is proven to be computationally safe efficiently, and the revocation performance is better than the complete revocation scheme if the revocation often occur. The measured performance shows that DO will benefit from an efficient revocation scheme if the average number of revocation is greater than 0.462. Review of the implementation of CP-ABE for cloud computing is carried

978-1-7281-2156-7 / 19 / $ 31.00 © 2019 IEEE

out by [7], [8], [9], [10], [11], [12], CP-ABE for mobile devices is carried out by [13], and a review of linear operations KP-ABE is carried out by [14], [15].

Research that discusses KP-ABE was conducted by [16], [17] who conducted a review and analysis of the application of KP-ABE in cloud storage. While [18] used the Multiple Authority ABE (ME-ABE) and KP-ABE for key management and scalability, as well as the Advanced Encryption Standard (AES) for encryption methods for sharing personal health records in the cloud, and [19] proposed KP-ABE for general circuit of bilinear maps. A scheme to avoid user collusion in KP-ABE was proposed by [20], an exclusive KP-ABE with a ciphertext size which was consecutively proposed by [21], [22]. Other developments of CP-ABE and KP-ABE such as multi-level policy control access, ABE multi-authority are carried out by [23], [24].

III. Proposed Work

In the CP-ABE scheme there is the role of authority to produce a public key that can be used by the sender and receiver to encrypt and describe the message. Public key generated by the authority based on the attributes of the user. In this scheme the sender of the message encrypts the message that is to be sent using a public key and a set of descriptive attributes. The role of the recipient of the message is to encrypt the encrypted message with his personal key sent from the authority, so he can read the message received.

To describe the recipient attribute message on the private key will be checked by matching the attribute in the encrypted message. If the match number is at least a threshold value d, the recipient's private key will be allowed to describe the encrypted message. In this section, we will explain how the architecture of the data owner encrypts and sends the ciphertext to another user, and how the recipient of the data can describe the received ciphertext as shown in Figure 1 below.

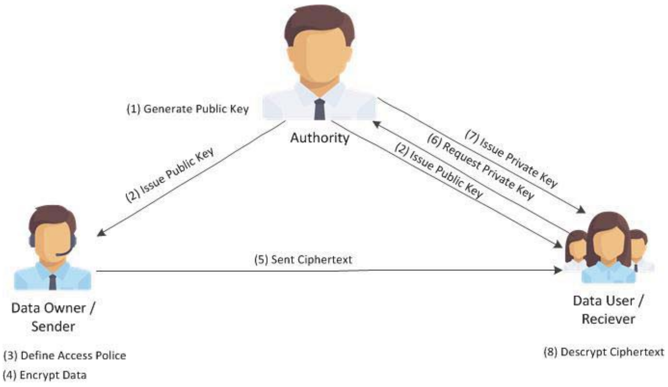

Figure 1. CP-ABE Architecture

As seen in Figure 1 there are eight processes that are carried out in sending data using the CP-ABE model:

A. Generate Public Key

The process of making a public key is carried out by the authority based on the attributes of the user. For example suppose a set of descriptive attributes {WNI, Lecturer, DPS}. This public key can be used by data owners and recipients of data to encrypt and describe data.

B. Public Key Issue

This stage is a public key notification to the data owner and data recipient. The sending process is carried out by the authority to the data owner and recipient of the data.

C. Define Access Police

At this stage the data owner will define access policies for the data he has. The data owner will define a set of descriptive attributes and threshold values for each data held.

D. Encrypt Data

The encryption process is carried out by the data owner after defining the access policy, and all access policies will be attached to the encrypted data. Suppose the data owner makes an access policy in the form of a set of descriptive attributes {WNI, Lecturer, DPS} with a threshold value of {2}. If the recipient of the message wants to detect an encrypted message, the recipient's private key number needs two or more attributes in the encrypted message, so the recipient must have the {Lecturer, DPS} attribute to detect and read the message.

E. Sent Ciphertext

Data that was previously in the form of plaintext after being encrypted by the owner of the data will turn into ciphertext. Data in the form of ciphertext is sent to other users who meet the access policy that has been set as the recipient of the data.

F. Request Private Key

The data recipient will make a request for the private key to the authority, then the authority will match the recipient's attributes with the access policy specified by the data owner. In the previous example it is mentioned that the recipient must have at least the {Lecturer, DPS} attribute.

G. Issue Private Key

Public key notification is carried out by the authority, where the private key will be notified if the user has an attribute match with the access policy specified by the data owner.

H. Decrypt Data

If the private key has been received by the data receiver, the data receiver can describe the ciphertext as a plaintext.

IV. Performance Evaluation

In this section an evaluation is carried out for the encryption process and data description with the number of attributes 1 to 30 attributes, which are measured based on the average execution time, memory usage, and notebook device power usage. The evaluation was carried out on two notebook devices namely MacBook Air (Intel Core i5 1.8Ghz, 8GB RAM) with the MacOS Sierra operating system version

10.12.6. and MacBook Air (Intel Core i5 1.4Ghz, 4GB RAM) with the MacOS Mojave operating system version 10.14.6.

A. *Execution Time*

Based on the following evaluation results Figure 2 shows the average time of encryption and description of data based on the number of attributes used. With a number of attributes from 1 to 30, which for evaluation on the MacBook Air (Intel Core i5 1.8GHz, 8GB RAM) and on the MacBook Air (Intel Core i5 1.4GHz, 4GB RAM) requires the same time, from 0.1 Ms to 0,6 Ms.

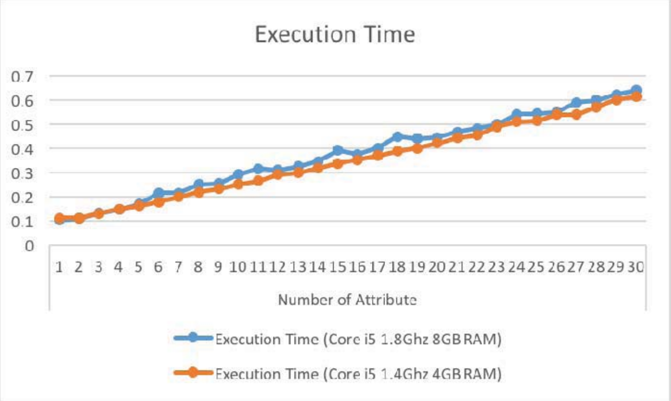

Figure 2. Execution Time

B. *Memory Used*

Evaluation results about the average memory usage are shown in Figure 3, where the number of attributes used is 1 to 30 attributes, and evaluation results show that in one encryption process requires an average memory of 25 MB to 33.8 MB for evaluation on the MacBook Air (Intel Core i5 1.8Ghz, 8GB RAM) and 26MB up to 27.7MB for evaluation on MacBook Air (Intel Core i5 1.4Ghz, 4GB RAM).

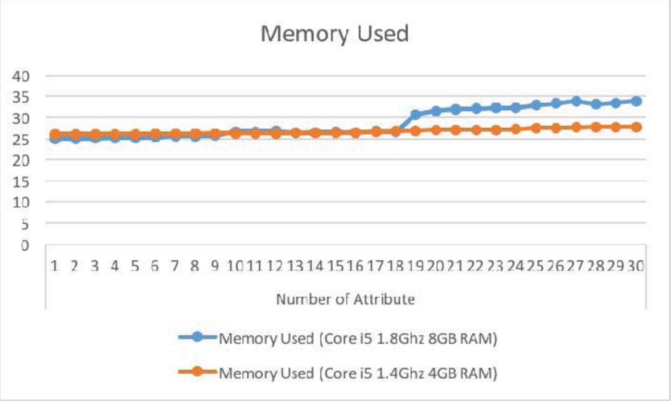

Figure 3. Memory Used

C. *Energy Impact*

Similar to the evaluation of execution time and memory usage, an evaluation for power usage is also carried out on 1 to 30 attributes. The amount of power used to encrypt data on MacBook Air notebooks (Intel Core i5 1.8Ghz, 8GB RAM) is 0.15 mWh to 0.45 mWh while on MacBook Air notebooks (Intel Core i5 1.4Ghz, 4GB RAM) is 0, 07 mWh up to 0.2 mWh. The results of evaluating power usage can be seen in Figure 4.

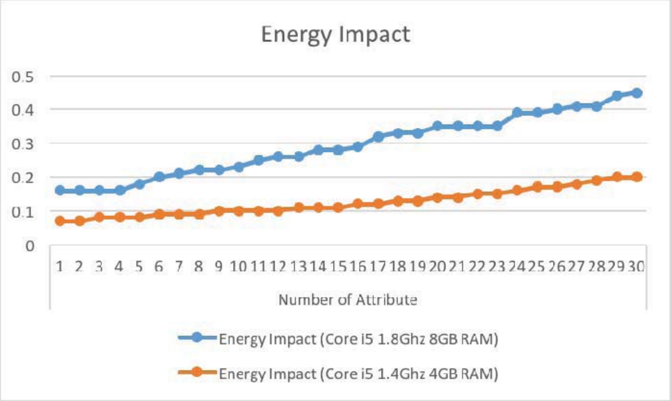

Figure 4. Energy Impact

As shown in Figure 4 Evaluations for power usage are also carried out on 1 to 30 attributes. The results of evaluating the use of power can be seen in Figure 4. The amount of power used to encrypt data with 1 to 30 attributes is 0.15mWh to 0.45mWh

V. Conclution

This paper has presented the Ciphertext Police Attribute Based Encryption (CP-ABE) architecture, the encryption process, data sharing, data description and key sharing to users. An evaluation has been carried out on two notebook devices namely MacBook Air (Intel Core i5 1.8Ghz, 8GB RAM) with the MacOS Sierra operating system version 10.12.6. and MacBook Air (Intel Core i5 1.4Ghz, 4GB RAM) with the MacOS Mojave operating system version 10.14.6. With a number of attributes ranging from 1 to 30 attributes, which are measured based on the average execution time, memory usage, and notebook device power usage. The evaluation results show that the more antributes used as a data access policy, the longer the encryption and description execution time needed, and the more memory and power used. The difference in notebook specifications is most influential on the notebook's power usage but is not significant at execution time and memory usage. Nevertheless CP-ABE is suitable for use in notebook devices.

VI. Acknowledgment

This work was sponsored by the Indonesian Ministry of Technology and Higher Education Research in the Beginner Lecturer Research Grant Scheme. Based on Decree Number 0895 / L8 / LKM / 2019 and Agreement / Contract Number 11/04 / LPPM / P.E / IV / 2019.

References

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” *Lect. Notes Comput. Sci.*, vol. 3494, pp. 457–473, 2005.

[2] C. Lee, P. Chung, and M. Hwang, “A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments,” vol. 15, no. 4, pp. 231–240, 2013.

[3] Rn. Lakshmi and D. Gana Dhas, “Analysis of Attribute Based

Encryption Schemes," *Int. J. Comput. Sci. Eng. Commun.*, vol. 3, no. 3, pp. 1076–1081, 2015.

[4] A. Krishnamurthy, "Implementation of Attribute Based Encryption With Privacy Preserving," no. November, 2017.

[5] N. Saravana Kumar, G. V. Rajya Lakshmi, and B. Balamurugan, "Enhanced attribute based encryption for cloud computing," *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 689–696, 2015.

[6] Y. Cheng, Z. Y. Wang, J. Ma, J. J. Wu, S. Z. Mei, and J. C. Ren, "Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage," *J. Zhejiang Univ. Sci. C*, vol. 14, no. 2, pp. 85–97, 2013.

[7] S. Atram and N. R. Borkar, "A Review Paper on Attribute-Based Encryption Scheme in Cloud Computing," vol. 6, no. 5, pp. 260–266, 2017.

[8] S. C. Parit and R. Rachh, "Ciphertext Policy Attribute Based Encryption," pp. 932–936, 2017.

[9] E. Mathur and M. Sharma, "A Review of Attribute based Encryption Technique for Security in Cloud Computing," *Int. J. Comput. Appl.*, vol. 159, no. 3, pp. 43–45, 2017.

[10] G. Yu, Y. Wang, Z. Cao, J. Lin, and X. Wang, "Traceable and undeniable ciphertext-policy attribute-based encryption for cloud storage service," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 4, 2019.

[11] H. Ba, H. Zhou, S. Mei, H. Qiao, T. Hong, Z. Wang, and J. Ren, "Astrape: An efficient concurrent cloud attestation with ciphertext-policy attribute-based encryption," *Symmetry (Basel).*, vol. 10, no. 10, pp. 1–25, 2018.

[12] S. Maharajanavar, "Anonymous Authentication of Decentralized Access Control of Data Stored in Cloud," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 3, no. 4, pp. 2194–2197, 2015.

[13] S. Moffat, M. Hammoudeh, and R. Hegarty, "A survey on ciphertext-policy attribute-based encryption (CP-ABE) approaches to data security on mobile devices and its application to IoT," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1305, no. Mcc, 2017.

[14] J. Lai, R. H. Deng, Y. Yang, and J. Weng, "Pairing-Based Cryptography – Pairing 2013," vol. 8365, no. September, 2014.

[15] H. Rahmani, N. Sahli, and F. Kamoun, "Distributed denial-of-service attack detection," no. November 2013, pp. 1988–2002, 2011.

[16] P. V. Kumar and J. A. R. Aluvalu, "International Journal of Innovative and Emerging Research in Engineering Key Policy Attribute Based Encryption (KP-ABE): A Review," *Int. J. Innov. Emerg. Res. Eng.*, vol. 2, no. 2, pp. 49–52, 2015.

[17] P. D. Dharmadhikari and S. Deshpande, "Key Policy Attribute Based Encryption in Cloud Storage," *IOSR J. Comput. Eng.*, vol. 18, no. 05, pp. 64–71, 2016.

[18] B. S. Varsha and P. S. Suryateja, "Using Attribute-Based Encryption with Advanced Encryption Standard for Secure and Scalable Sharing of Personal Health Records in Cloud," vol. 5, no. 5, pp. 6395–6399, 2014.

[19] P. Hu and H. Gao, "A Key-Policy Attribute-based Encryption Scheme for General Circuit from Bilinear Maps," vol. 19, no. 5, pp. 704–710, 2017.

[20] Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan, and R. Lu, "User Collusion Avoidance Scheme for Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," *IEEE Trans. Comput.*, vol. 65, no. 9, pp. 2939–2946, 2016.

[21] B. Waters, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, "Public Key Cryptography – PKC 2011," vol. 6571, no. March 2011, pp. 53–70, 2011.

[22] S. Belguith, N. Kaaniche, and G. Russello, "PU-ABE: Lightweight Attribute-Based Encryption Supporting Access Policy Update for Cloud Assisted IoT," *IEEE Int. Conf. Cloud Comput. CLOUD*, vol. 2018–July, pp. 924–927, 2018.

[23] N. Kaaniche and M. Laurent, "Attribute based encryption for multi-level access control policies," *ICETE 2017 - Proc. 14th Int. Jt. Conf. E-bus. Telecommun.*, vol. 4, pp. 67–78, 2017.

[24] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT," *Comput. Networks*, vol. 133, pp. 141–156, 2018.