Conceptual Framework for Lightweight Ciphertext Policy-attribute based Encryption Scheme for Internet of Thing Devices

Jasni Mohamad Zain[1*], Norhidayah Muhammad[2]
[12]Faculty of Computer & Mathematical Sciences, Universiti Teknologi Mara, 40450, Shah Alam, Selangor, Malaysia

Keywords: Cryptography, ABE, CP-ABE, Lightweight Cryptography, Internet of Thing.

Abstract: The paper proposes a conceptual model for data security in the Internet of thing devices. Estimated by Jumoki in early 2018 to 2022, there will be about 18 billion devices connected IoT. Therefore many issues concern in IoT devices especially in data security. Cryptography with lightweight features is one of focus area by researchers to develop a powerful cryptography scheme for IoT devices. Lightweight cryptography scheme has been discussed and proposed widely recently. There are AES, PRESENT, Hash algorithm declared as a lightweight algorithm under consideration in ISO/IEC 29192 "Lightweight Cryptography". Unfortunately these lightweight algorithm is one-to-one communication cryptography technique. This algorithm is suitable to be implemented for individual or for small group communication. It is however not suitable to be implemented in a big company as it involves many users and become a bottleneck. Therefore we propose a lightweight Ciphertext Policy-Attribute Based Encryption (CP-ABE) algorithm to implement in IoT devices. CP-ABE algorithm is one-to-many technique suitable for secure grouping communication, but this algorithm is not a lightweight features. Therefore this paper proposes a lightweight CP-ABE algorithm for IoT devices.

1 INTRODUCTION

Cryptography was known as encryption become an important thing in data security, especially enabling safe internet communications in cloud computing. In cryptography, lightweight issues have long been identified and many studies have been conducted in producing more lightweight cryptography methods especially for constrain device such as IoT device. Lightweight cryptography was standardized with the properties of lightweight cryptography discussed in ISO/IEC 29192 (Katagi & Moriai, 2008). In ISO/IEC 29192, lightweight properties are described based on target platforms.

Cryptographic algorithm tailored with constrained resources including RFID tags, sensors, contactless smart cards, health-care devices and so on. Figure 1 show IoT devices role was connected today. In hardware implementations, chip size and/or energy consumption are the important measures to evaluate the lightweight properties. In software implementations, the smaller code and/or RAM size are preferable for the lightweight applications. Security solutions need to consider the efficiency and lightweight requirements if they want to produce a method that can be used on lightweight devices to ensure that it does not increase the processing time (Yang et al., 2016).

AES was known as lightweight cryptography if compared to RSA because AES is a symmetric key cryptography, it's using a small size of keys and only has one key for both encrypting and decrypting processes. Similarly with IBE, many researchers have developed IBE which is more lightweight and suitable for implementation in constraint devices. But all of these algorithms are for one-to-one communication, it is better suited for communication between individuals and small groups that do not involve many users. To meet the security requirements in the cloud system, one-to-many communication is required to facilitate data sharing and to ensure data security.

Previously people familiar with some well-known cryptography algorithms such as AES, RSAs are commonly used to ensure data security, but it provides problems for users to share data or ciphertext and requires a lot of steps to share data with many users because those algorithm is one-to-one communication encryption technique (Yuan, 2016).

Zain, J. and Muhammad, N.
Conceptual Framework for Lightweight Ciphertext Policy-attribute based Encryption Scheme for Internet of Thing Devices.
DOI: 10.5220/0010043303790383
In *Proceedings of the 3rd International Conference of Computer, Environment, Agriculture, Social Science, Health Science, Engineering and Technology (ICEST 2018)*, pages 379-383
ISBN: 978-989-758-496-1

Figure 1: Role of IoT devices (Agarwal, 2015)

In one-to-many technique, one ciphertext can be accessed by many users as long as it meets the access policy specified in the ciphertext. This makes it easy for the data owner because it does not have to send one by one the same ciphertext to different users. This method is very efficient for a large company that has many users (Vaanchig et al., 2016). Goyal first person who introduced the concept of grouping by developing an Attribute based encryption (ABE). Then Sahai and Waters (2005) introduce (CP-ABE) more efficient because users have the right to determine who is eligible to access the ciphertext.

Many encryption algorithm can offer short decryption keys. For example, identity-based broadcast encryption (Delerablée, 2007), identity-based encryption with traitor tracing (Guo et al., 2012), multi-identity single-key decryption (Guo et al., 2013). Unfortunately, a few researcher in attribute-based encryption scheme offers short decryption keys. CP-ABE Instead of decryption key, ciphertext is also have problem with the size because it's depend on number of Boolean in access policy. Therefore key design criteria in a CP-ABE scheme should include constant size secret key and constant size ciphertext, as well as a cost efficient mechanism for encryption and decryption.

2 RELATED WORK

Sahai and Waters (2005) made some initial steps to improve the primitives existing encryption scheme with one-to-one communication features by introduced the concept of Attributed-Based Encryption (ABE). The idea of ABE is grouping technique, means that user or decryptor will be scale in group. Therefore, one ciphertext can be decrypted by one group of users with certain attribute, stated in access policy by encryptor. ABE scheme has obvious advantages in terms of efficiency and is fit for large scale network environment, such as cloud systems. In an ABE system, a user's keys and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key.

The ABE scheme is allowed for decryption when at least k attributes overlapped between a ciphertext and a private key. While this primitive was shown to be useful for error-tolerant encryption with biometrics, the lack of impressibility seems to limit its applicability to larger systems. Attribute-based encryption (ABE) enforces encrypted data to be decrypted with a secure access control mechanism that the assigned attributes must satisfy the access policies associated with ciphertext and private keys. ABE has become a promising cryptographic primitive providing one-to-many encryption.

2.1 Ciphertext Policy-attribute based Encryption

After the notion of Attribute-based Encryption (ABE) was introduced by Sahai and Waters (2005), After that Goyal, Pandey et al. (2006) has proposed the first KP-ABE system, in which ciphertexts are associated with attributes, and secret keys are associated with access policies. Then BSW (Bethencourt, Sahai et al. 2007) has proposed CP-ABE scheme contrast with KP-ABE where attribute is associated with private key and access policy is associated with ciphertext and become better than Key Policy-Attribute Based Encryption (KP-ABE) based on specification of CP-ABE provide fine-grained access control, CP-ABE scheme in which the data owner hold direct control on access policy and decide who should or should not have access to the ciphertext. Then, Cheung and Newport (Cheung & Newport, 2007) proposed another CP-ABE in which the access structures are AND gates. Both scheme is based on bilinear map and pairing based cryptography practically implementing fine grained access control for data owner to control deep security and very usable in cloud system (Zain, 2010).

Table 1 show previous research focuses on constant ciphertext and a constant private key. The proposed algorithm is focused on one either private key or ciphertext. Schemes with constant size ciphertexts (Zhang et al., 2014), (Emura et al.,

2009),(Herranz et al., 2010) and constant size secret keys (Emura et al., 2009),(Guo et al., 2014) with an expressive access structure based on bilinear maps have been proposed. According to (Zheng et al., 2015) and (Li et al., 2014), the schemes based on bilinear maps, which is significantly more costly than schemes based on conventional cryptosystems. Besides that, even though Emura makes the size is constant, but it uses the structure (n, n) threshold. Where the threshold property is the number of attributes in the access structure and the user attribute in the private key must be the same. Thus, designing a cost efficient and expressive access structure CP-ABE with the constant size secret keys and ciphertexts using conventional public-key cryptosystems remains a research challenge (Liew et al., 2013).

Table 1: CP-ABE scheme with constant private key and constant ciphertext

Author	Size	
	Private Key	Ciphertext
BSW(Bethencourt et al., 2007)	(2|A| + 1) G	(2|P| + 1) G + G_t
(Herranz et al., 2010)	(n + |A|) G	2G + G_t
(Emura et al., 2009)	2G	2G + G_t
(Zhang et al., 2014)	(n +1) G	2G + G_t
(Guo et al., 2014)	2G	(n - |P| + 2) G + G_T + L
(Odelu et al., 2017)	2G	3G + L

2.2 Proposed Conceptual Model

The weakness of CP-ABE is in terms of size decryption key and ciphertext, because it's growing linearly with the number of attributes, if the number of attributes is more, then the size key will be bigger because attribute combined with the key. And this will be a barrier to constrain devices such as IoT. Each device has a different number of attributes. The challenge is to produce a constant size ciphertext, and making the size ciphertext is not dependent on the number of boolean in the access policy (Odelu et al., 2017). As well as the challenge for generating a size private key that is constant and independent of the size attribute. This is because the attribute will be combined with the user private key and it should match the boolean in the access policy (Ambrosin et al., 2016). Thereby enabling the process decryption to succeed.

As shown in figure 2, this is theoretical framework proposed. Four important component involved in this framework. The first is the key authority or key center. The key center will generate a public key and also a private key for the user. It also has the power to verify the user's status by ensuring that the attribute used by the user is correct. Therefore the key authority plays a very important role in ensuring data security. The second is data owner. The data owner is the individual who will encrypt the data and he also will determine who has the right to access the data. The group of user that has access to the data will be specified in the access policy, and the access policy will be merged together with the ciphertext.

Third component is cloud, after data owner encrypts the data and put the ciphertext to cloud. Cloud is a storage that gathers thousands of servers and provides client service storage according to user requirements. Data security needs to be emphasized in cloud storage to ensure data security as data intrusion can occur easily. The forth is IoT devices. IoT devices become a new phenomenon today and forward. IoT devices are used today such as sensors for safety, medical, and so on systems. These devices have a lack of resources such as a battery, memory size, and processor. Therefore it requires a lightweight algorithm and a small size of data.

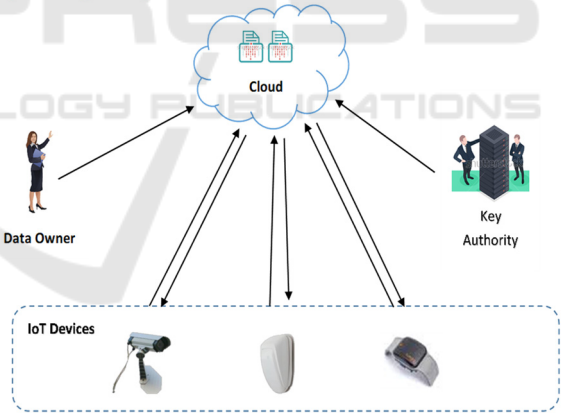

Figure 2: Conceptual Framework for CP-ABE algorithm in IoT devices

As shown in picture 3, there are four algorithms in the CP-ABE scheme. The first is setup algorithm, master public key and master secret key will be generated. Master public key will be used in encryption algorithm, keygen and also decryption algorithm. While the master secret key will be used to generate a private key in the algorithm keygen.

The second algorithm is encryption. After the master public key is generated, the data owner can apply from the key authority and can encrypt the data

using the master public key that is given and also defines the access policy for the ciphertext. Only the attributes mentioned in the access policy that will successfully access the ciphertext.

The third algorithm is keygen. Keygen algorithm operates to generate decryption key or private key for the user to decrypt the ciphertext. The key authority will validate user attribute and then use the master secret key and combined with user attribute to create user private key.

The fourth algorithm is decryption. In this algorithm, the user or IoT device will use the private key that has been generated in the keygen algorithm to decrypt the ciphertext. If the attribute contained in the private key match with the attribute in the access policy then the process decrypt will succeed.

3 CONCLUSIONS

This paper proposes a framework to produce a lightweight CP-ABE algorithm for IoT devices. The proposed algorithm allows one message or ciphertext placed in the cloud to be accessed by many IoT devices as long as it meets the policy set in the access policy. Expected output that will be obtained from research analysis later is size decryption key and size ciphertext that will not increase with the number of user attribute. Besides the small size, it is also constant. This is because the big challenge in CP-ABE is to make sure attributes embedded in a private key do not influence the size of keys, as well as boolean in access policy will not affect the size of ciphertext.

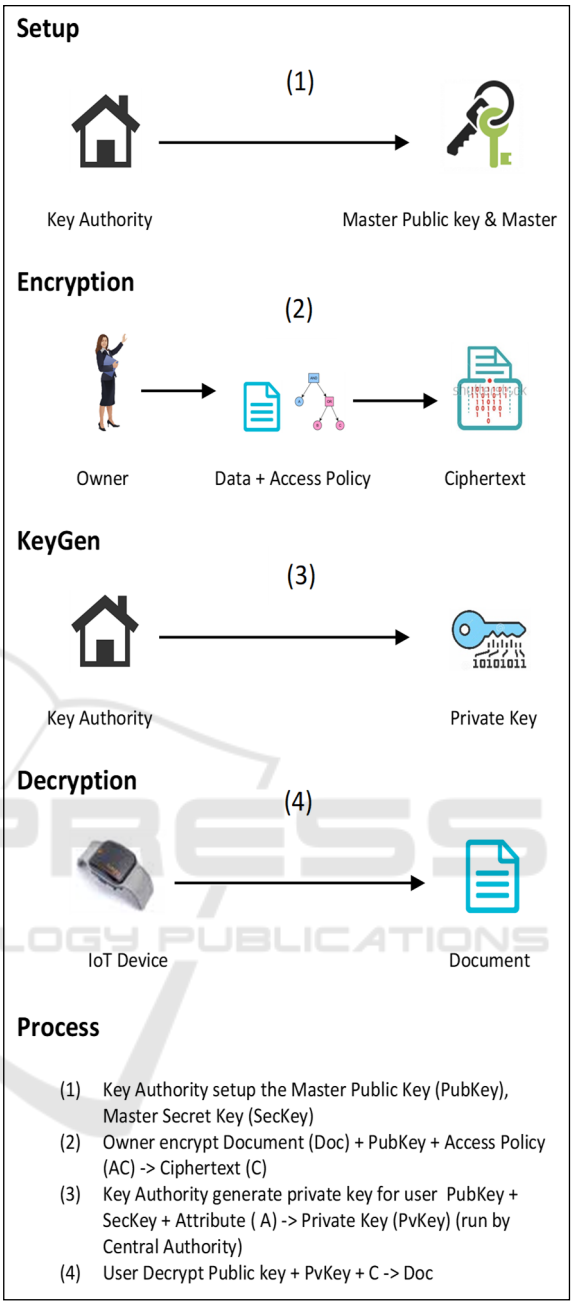

Figure 3: Four Algorithm in CP-ABE cryptography scheme

REFERENCES

Agarwal, M. 2015. "Role of IOT devices and servcies in the development of smart cities." from https://www.slideshare.net/mayankagarwal51/role-of-iot-devices-and-servcies-in-the-development-of-smart-cities.

Ambrosin, M., A. Anzanpour, M. Conti, T. Dargahi, S. R. Moosavi, A. M. Rahmani and P. Liljeberg. 2016 "On

the feasibility of attribute-based encryption on internet of things devices." *IEEE Micro* 36(6), 25-35.

Bethencourt, J., A. Sahai and B. Waters. 2007 "Ciphertext-policy attribute-based encryption". *IEEE Symposium on Security and Privacy*, IEEE.321-334

Cheung, L. and C. Newport. 2007 "Provably secure ciphertext policy ABE". *Proceedings of the 14th ACM conference on Computer and communications security*, ACM.456-465

Delerablée, C. 2007 "Identity-based broadcast encryption with constant size ciphertexts and private keys". *International Conference on the Theory and Application of Cryptology and Information Security*, Springer.200-215

Emura, K., A. Miyaji, A. Nomura, K. Omote and M. Soshi. 2009 "A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length". *ISPEC*, Springer.13-23

Guo, F., Y. Mu and W. Susilo. 2012 "Identity-Based Traitor Tracing with Short Private Key and Short Ciphertext". *ESORICS*, Springer.609-626

Guo, F., Y. Mu, W. Susilo, D. S. Wong and V. Varadharajan. 2014 "CP-ABE with constant-size keys for lightweight devices." *IEEE Transactions on Information Forensics and Security* 9(5), 763-771.

Guo, H., C. Xu, Z. Li, Y. Yao and Y. Mu. 2013 "Efficient and dynamic key management for multiple identities in identity-based systems." *Information Sciences* 221, 579-590.

Herranz, J., F. Laguillaumie and C. Ràfols. 2010 "Constant size ciphertexts in threshold attribute-based encryption". *International Workshop on Public Key Cryptography*, Springer.19-34

Katagi, M. and S. Moriai. 2008 "Lightweight cryptography for the internet of things." *Sony Corporation*, 7-10.

Li, H., X. Lin, H. Yang, X. Liang, R. Lu and X. Shen. 2014 "EPPDR: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid." *IEEE Transactions on Parallel and Distributed Systems* 25(8), 2053-2064.

Liew, S.-C., Liew, S.-W., Zain, J.M. 2013. "Tamper localization and lossless recovery watermarking scheme with roi segmentation and multilevel authentication". *Journal of Digital Imaging*, 26 (2), pp. 316-325.

Odelu, V., A. K. Das, M. K. Khan, K.-K. R. Choo and M. Jo. 2017 "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size Keys and ciphertexts." *IEEE Access* 5, 3273-3283.

Sahai, A. and B. Waters. 2005 "Fuzzy identity-based encryption". *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer.457-473

Vaanchig, N., W. Chen and Z. Qin. 2016 "Ciphertext-Policy Attribute-Based Access Control with Effective User Revocation for Cloud Data Sharing System". *International Conference on Advanced Cloud and Big Data (CBD)*, IEEE.186-193

Yang, Y., H. Cai, Z. Wei, H. Lu and K.-K. R. Choo.2016 "Towards Lightweight Anonymous Entity Authentication for IoT Applications. Information Security and Privacy": *21st Australasian Conference, ACISP 2016,* Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I. J. K. Liu and R. Steinfeld. Cham, Springer International Publishing, 265-280.

Yuan, W. 2016 "Dynamic Policy Update for Ciphertext-Policy Attribute-Based Encryption." *IACR Cryptology ePrint Archive*, 457.

Zain, J.M. 2010 "Strict authentication watermarking with JPEG compression (SAW-JPEG) for medical images". *European Journal of Scientific Research*, 42 (2), pp. 232-241.

Zhang, Y., D. Zheng, X. Chen, J. Li and H. Li. 2014 "Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts". *International Conference on Provable Security*,

Zheng, M., Y. Xiang and H. Zhou. 2015 "A strong provably secure IBE scheme without bilinear map." *Journal of Computer and System Sciences* 81(1), 125-131.