Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 56 (2015) 271 – 275

Procedia Computer Science

The 10th International Conference on Future Networks and Communications (FNC 2015)

A Work in Progress: Context based encryption scheme for Internet of Things

Jungyub Lee[a,]*, Sungmin Oh[a], Ju Wook Jang[a]

[a]*Sogang University, 35 baekbeom-ro, Mapo-gu, Seoul, 121-742, South Korea*

Abstract

In current Internet, data owners can provide integrity and authentication when data is generated. However confidentiality is usually implemented by symmetric keys between two corresponding programs in an end-to-end manner. A symmetric key for confidentiality is not suitable for Internet of Things (IoT) environment where there are one producer of data and multiple consumers of data. Further the consumers differ in their qualification about what part of the data is allowed to access under which context. In the paper we describe our work in progress of confidentiality scheme in which the producer encrypts data along with context. We improve Key Policy Attribute Based Encryption (KP-ABE) and Ciphertext Policy Attribute Based Encryption (CP-ABE) to allow consumers to decrypt data as their contexts dictate. We describe briefly our scheme to implement the idea.

Keywords: Internet of Things (IoT), Attribute Based Encryption (ABE), Context.

1. Introduction

Nowadays, as the number of connected devices grows exponentially, excessive data has been generated. On this account, data privacy has become a critical issue in the Internet of Things (IoT). For example, In December 2013 a researcher at Proofpoint, an enterprise security firm, discovered that hundreds of thousands of spam emails were being logged through a security gateway. Proofpoint traced the attacks to a botnet made up of 100,000 hacked

* Corresponding author. Tel.: +82-2-3272-3220; fax: +82-2-3272-3220.
E-mail address: jjang@sogang.ac.kr

doi:10.1016/j.procs.2015.07.208

appliances. As in the example above, since IoT devices have no security capability, security threats of IoT will be growing.

Existing internet, while data owner can provide integrity and authentication when data was generated, confidentiality is usually implemented by symmetric key. Unlike existing internet, IoT data is generated by a large number of devices and delivered multiple users, for that reason symmetric key scheme is hard to use. Therefore, new trust transmission scheme which is suited for use in the IoT should be developed.

In this paper, we introduce a several schemes of KP-ABE (Key Policy Attribute Based Encryption), CP-ABE (Cipher text Policy Attribute Based Encryption), cloud based Attribute Based Encryption Architecture, and then, suggest future direction about data privacy and data access control for IoT environment. In the rest of the paper, Section II introduces a related work of KP-ABE, CP-ABE and Section III introduces working in progress. We discuss about future direction and conclusion in Section IV.

2. Related Work

2.1. Attribute Based Encryption

Sahai and Waters[1] introduced an attribute-based encryption (ABE) method for an access control. ABE can be divided by two types, called KP-ABE[3] and CP-ABE[4].

Fig. 1. illustrates KP-ABE concept. Each Data has attributes (such as Name, Position or Place) and users have keys to an access tree which can distinguish attributes. Through the access tree, data was decrypted only when it satisfies the access tree attributes. For example, an access tree consists of <President OR <Alice AND Seoul>>. Data 1, 2, 3 have three attributes which correspond to Name, Position, and Place respectively. Then, a user can decrypt only Data 3 depending on her position (president). However, KP-ABE has no authority check about data access because the user key includes access tree.

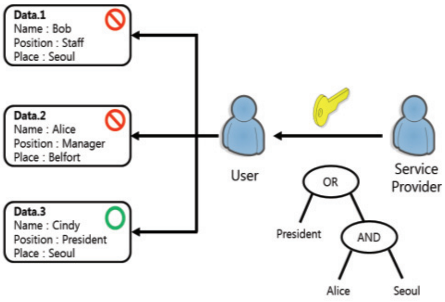

Fig. 1. KP-ABE (Key Policy Attribute Based Encryption)

Unlike KP-ABE, ciphertext includes an access tree and users key includes user attributes such as position, name, and place. If user attribute satisfies the access tree condition in the ciphertext, encrypted data can be decrypted. In addition, data access control is possible since the access tree is in the cipertext. There is an example about CP-ABE in Fig. 2. Each user has some kind of attributes. Only User 3 can decrypt the data since User 3 attributes satisfy the access tree condition in the ciphertext (< President OR < Alice AND Seoul>>). The main difference between KP-ABE and CP-ABE is whether they can data access control or not. In KP-ABE, data include only user attributes, anyone can access data. However, CP-ABE can control the data access since the access tree is in ciphertext.

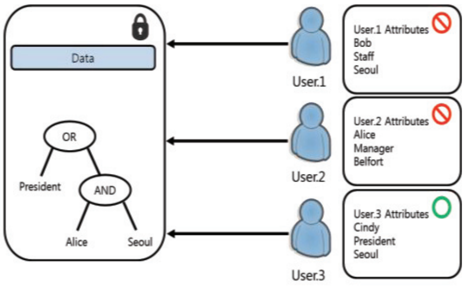

Fig. 2. CP-ABE (Ciphertext Policy Attribute Based Encryption)

2.2. Access Control in Cloud Computing

Shucheng Yu et.al[2] proposed fine-grained data access control in cloud computing. In Yu's scheme, data is composed of a header and body. The header include data encryption key (DEK) based on a set of attributes to encrypt data. The body is the data encrypted by DEK. The data owner creates a data that is combined header with body, and sends the data to cloud service provider. If the user's secret key satisfies a set of attributes of the header, user can receive the DEK and decrypt the data.

Fig. 3. shows the example of access control in cloud computing. In this example, the data owner transmit outsource encrypted data and encrypted DEK to cloud server. When user transmit access request to cloud server, the cloud server transmit the encrypted DEK and encrypted data to user. If the user attributes satisfy the access tree in the header, it can decrypt the DEK. Therefore, user can decrypt data using decrypted DEK.

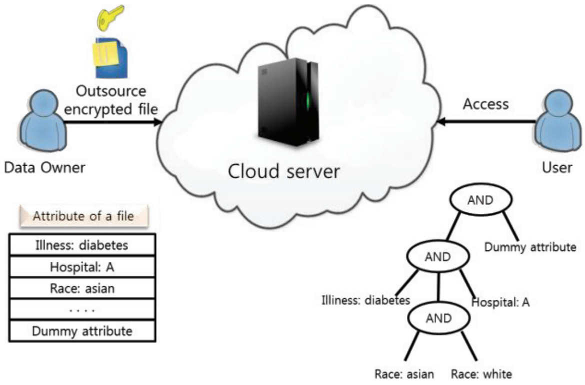

Fig. 3. Example of access control in cloud computing

However, in this scheme, user's context information is not considered. Although Seul-Ki Choi et.al[5] propose the solution of the problem, there is still a problem that the solution is not considered about a huge number of devices as a characteristic of IoT.

3. Working in Progress

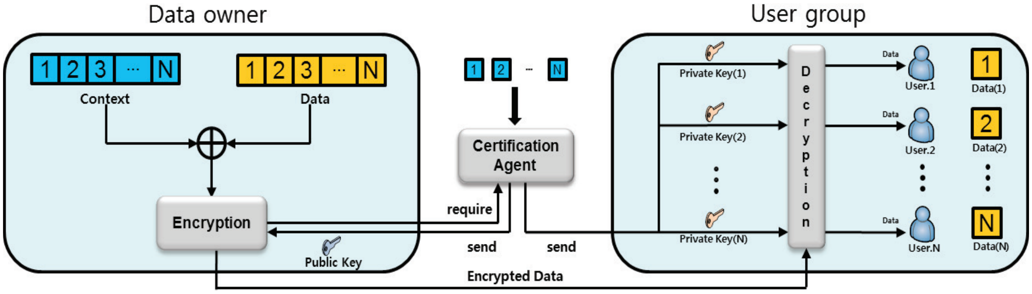

Fig. 4. Context based encryption scheme for IoT

Under the IoT environments, Attribute Based Encryption is more suitable than symmetric key method which is widely used in the existing Internet applications. Since the devices continue to move, the attribute value might change frequently. Previous works on attribute revocation have made some progress but it still remain in a naive level suggests very naive method that uses an expiration date or a revocation list. Therefore, an attribute revocation scheme for IoT devices should be developed.

The contexts related with user or device can be used as an attribute of data when data was encrypted. The contexts are extracted by the detection method based on the user's situations. Therefore, context data can be used as a suitable attribute value although user situation frequently changes.

Fig. 4. shows an example of context based encryption algorithm. Encrypted data is generated by encrypting context and data. Data owner get a public key by a certification agent and data is encrypted by the public key. When data is decrypted, the certification agent creates a private key based on the user's context and provides the private key to each user. A specific user can decrypt only the desired data by the key.

4. Conclusion and Future Work

To enhance the security of Internet applications, some researchers have proposed attribute based encryption method and access controls in cloud computing environments. However, a huge number of devices as a characteristic of IoT was not considered in the existing schemes. In this paper, we have proposed a context based encryption scheme for IoT. Through context extraction based on detection, data owner performs encryption and decryption. In decryption process, each user can decrypt only desired data. Therefore user can receive data in low overhead environment even though there are a large amount of device exists. In the end, access control using context has shown some benefit, but also needs more study about it.

Acknowledgements

"This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2015-H8501-15-1017) supervised by the IITP(Institute for Information & communications Technology Promotion)

References

1. SAHAI, Amit; WATERS, Brent. Fuzzy identity-based encryption. In: Advances in Cryptology–EUROCRYPT 2005. Springer Berlin Heidelberg, 2005. p. 457-473.
2. YU, Shucheng, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing. In: INFOCOM, 2010 Proceedings IEEE. Ieee, 2010. p. 1-9.

3. GOYAL, Vipul, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006. p. 89-98.
4. BETHENCOURT, John; SAHAI, Amit; WATERS, Brent. Ciphertext-policy attribute-based encryption. In: Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007. p. 321-334.
5. CHOI, Seul-Ki; KWAK, Jin. Context-Aware Information-Based Access Restriction Scheme for Cloud Data. International Journal of Multimedia & Ubiquitous Engineering, 2013, 8.6.