Advances in Intelligent Systems Research, volume 163
8th International Conference on Management, Education and Information (MEICI 2018)

Application of Attribute-based Encryption in Internet of Things

Zixuan Wang[1, a], Hao Liu [1, b*] and Hao Ma [1, c]

[1]Information Engineering School Beijing Institute of Fashion Technology

[a]52059676@qq.com,[b]gxymh@bift.edu.cn, [c]gxyliuh@bift.edu.cn

Keywords: Internet of Things; Access control; Anonymity; Attribute-based encryption

Abstract. In the IoT environment, a large amount of personal information and environmental data are collected and processed by the sensing layer, which will contain some private data. Therefore, how to define the user's data access rights becomes a major challenge for the security of the Internet of Things. In addition, mobile users of the Internet of Things interact with the network frequently, and the security of their own information needs to be protected, so anonymous data access becomes another security goal that needs to be achieved. In order to realize the data access control of the Internet of Things and the anonymous data access of users, it is proposed that a Ciphertext-Policy Attribute-based Encryption (CP-ABE)-based access control mechanism. CP-ABE allows data sources to encrypt data while implementing a secure access policy, so only authorized data users with the desired attributes can decrypt the data.

Introduction

The “Internet of Things” is recognized as the third wave of the world information industry after computers, the Internet and mobile communication networks. With the development of wireless technology, more and more items in daily life are connected to wireless communication. Goods in the world which are from computers to mobile phones, from computers to books, from mobile phones to cups, as long as they access to the network, they can exchange information and work together.

In the ideal Internet of Things system, any item can be connected to the network through wireless sensing technology to facilitate people's management and use of items [1]. This feature determines the large number and diversity of IoT terminal devices, making the access control work of massive terminal devices in the Internet of Things different from traditional networks.6 Compared with the Internet, the nodes in the Internet of Things are mostly less intelligent and have poor self-protection capabilities. Compared with wireless sensor networks, the number of IoT terminal nodes is large, diverse, and complex. Most of the IoT-aware nodes are dynamically and decentralized in unsupervised locations, with limited communication range and lack of complex security measures. Attackers can easily capture these devices and use the information contained in these devices to maliciously attack the network. This requires a secure access control policy in the Internet of Things to accurately identify the user's identity and grant access to resources only to reliable nodes.

Traditional access control mechanisms are generally based on identity or role-based coarse-grained access control, and user authorization management is not flexible enough [2]. The number of users and access requirements in the IoT environment will far exceed the traditional single sensor network, requiring a more flexible access control mechanism. In the paper, a ciphertext-based attribute-based encryption-based access control mechanism is proposed for user access control requirements. The mechanism can flexibly set corresponding access rights according to user attributes, and can also realize anonymous access of users to network data.

Attribute-based Encryption Algorithms

In 2005, Sahai and Waterst proposed a fuzzy identity-based encryption scheme to improve the fault-tolerant performance of biometric-based authentication systems and to exploit the difficult problems associated with bilinear pairing[3]. At the same time, the concept of attribute encryption is

proposed by extending and extending the thoughts. Sahai and Waters proposed two attribute-based encryption schemes, attribute-based encryption (CP-ABE) and key-based attribute-based encryption (KP-ABE) based on the size of the complete set of attributes in the system. Similarity, the subject of encryption in the CP-ABE algorithm is ciphertext instead of key, so that the control of encryption is in the hands of the encryptor. This encryption method has better adaptability in distributed networks. This kind of broadcast is similar. The encrypted encryption method can play an advantage in the Internet of Things, and the CP-ABE implementation is simpler. Therefore, the attribute-based encryption system that selects the ciphertext policy is applied to the Internet of Things.

Access Tree Structure

In CP-ABE, the encrypting party does not need to know who is decrypting when encrypting the information. The decrypting party only needs to meet the corresponding conditions to decrypt, and the matching condition is the access tree structure.

The access tree can be extended based on the (K, n) threshold structure. The access control structure described by the access tree which is more complex and multi-layered, and has a stronger expressive power[4]. Each leaf node of the access tree corresponds to an attribute value, representing the input of the access tree, having 0 and 1 states, and the parent node of the tree corresponds to a threshold structure, which may be a (K, n) threshold. It can also be an AND gate and an OR gate, each of which can define the input of its leaf node. Figure 1 shows a typical attribute tree structure in which leaf nodes correspond to attribute values, and the parent nodes can be a K=3 threshold, AND gate, or OR gate, respectively.

The traversal process for the access tree T during access control is as follows: For all leaf nodes x, the definition function att(x) returns the attributes corresponding to the leaf nodes. Let r be the root node of T and node x be the node x

The subtree of the root node is represented as Tx. $(Tx(\omega)=1)$ means that the attribute set ω satisfies the access tree $Tx(\omega)$ and vice versa.

Next, recursively calculate the value of $Tx(\omega)$:

(1) If node x is a non-leaf node, then $Tx(\omega)$ is calculated for each leaf node xn of node x if and only if at least k nodes are satisfied, $Tx(\omega)$ returns 1.

(2) If node x is a leaf node, $Tx(\omega)$ returns 1 if and only if att(x) belongs to ω.

CP-ABE algorithm flow

The flow of the CP-ABE algorithm is shown in Figure 1. It mainly includes the following four parts: initialization of the system, generation of the user's private key, encryption of the ciphertext, and decryption of the user by the private key.

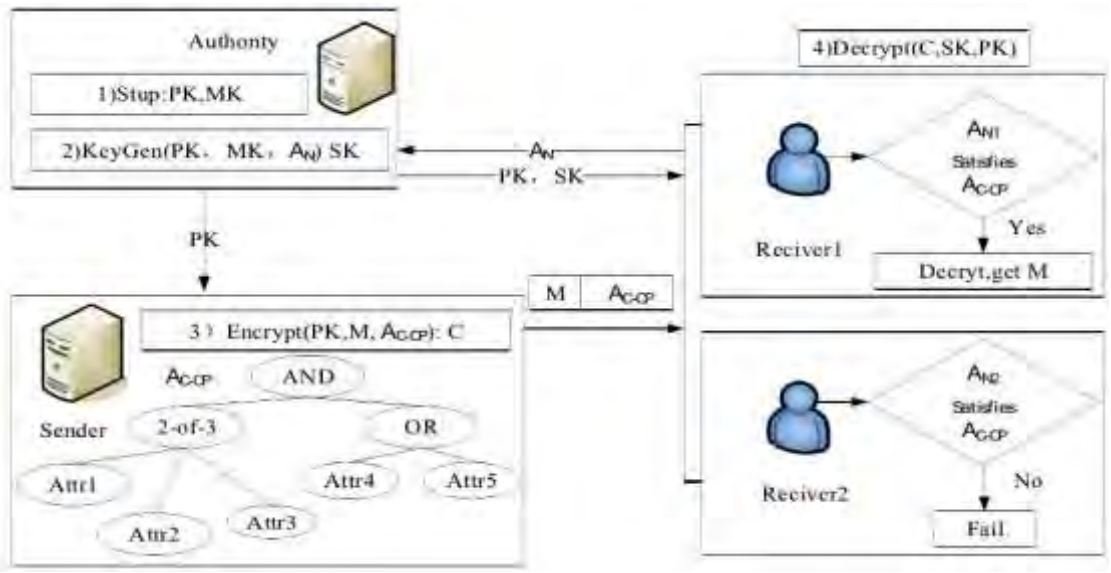

Figure. 1 CP-ABE system

(1) Setup: the initialization function of the system, taking the system security parameter k as input, where k is public in the network, and there are two outputs, namely the system public key PK and the master key MK;

(2) Keygen (MK, S): a key generation algorithm. The key generation is based on the user's attributes. By inputting the master key MK and the attribute set S, a private key SK related to the user attribute set is generated.

(3) Encrypt (PK, M, T): an encryption function. This function uses the system public key PK to encrypt the input message plaintext M according to the specific structure of the access tree. After the encryption is completed, the ciphertext CT is generated.

(4) Decrypt (CT, SK): decryption function, this function will set the user's attribute S and access

All nodes on the tree CT are matched. If S satisfies W, the private key SK can be used to successfully decrypt the CT and obtain the plaintext M.

In the attribute-based encryption scheme of the ciphertext policy, the user's private key is generated according to the user's own attribute set, and each user may have multiple attribute features. At the same time, the encryption and decryption of data in the CP-ABE mechanism is based on the access tree [5]. The ciphertext can be successfully decrypted only if the attribute set of the access requester meets the specific access tree structure.

Performance Analysis

Advantages.(1) Ensure that IoT service providers only allow users with specific attributes to get the entity-related information they need.

(2) When the access control policy changes, it is only necessary to re-encrypt the ciphertext according to the new access control policy, and the key management overhead is small.

(3) Anonymous access is possible

(4) Anti-collusion attack

Challenge.(1) User revocation overhead: When the user revokes from the system, the access policy must be re-established without affecting the access of other users.

(2) Key abuse: The user private key is only related to the user attribute, and has nothing to do with any specific information of the user, and cannot prevent the generation of pirated keys.

(3) The key leakage liability is difficult to define: when a pirated key appears, it cannot be determined whether the user or the authorized authority leaked the private key.

Conclusions

At present, the Internet of Things can be logically divided into a sensing layer, a transport layer, and a processing layer. Since the function of the sensing layer is to fully sense external information and provide information to legitimate users, a reasonable access control mechanism is needed to manage the user's data access rights. Traditional identity-based and role-based coarse-grained access control has many limitations in the large-scale open environment of the Internet of Things. This paper proposes an access control mechanism based on user attributes to achieve fine-grained access control and anonymous data access by users. In this solution, when the user requests access to the sensor node data, identity authentication is not required, and the node selects whether to respond to the user request according to the user attribute and the threshold principle. Different networks can set different thresholds to meet their respective access needs. Although the algorithm can implement access control and anonymous data access, there are also problems such as large user cancellation overhead and key abuse.

Acknowledgements

This research was financially supported by Beijing Institute of Fashion Technology under Grant NHFZ20180104/007and NHFZ20180087/048.

References

[1] Nouha Oualha and Kim Thuat Nguyen:Lightweight Attribute-based Encryption for the Internet of Things [J]. IEEE, 2016

[2] Ren Fang, Ma Jianfeng and Hao Xuanwen: An attribute-based access control mechanism for the Internet of Things perception layer[J]. Journal of Xidian University(Natural Science Edition), 2012, 39(2): 66-72 (In Chinese)

[3] Li Dawei, Yang Geng and Zhu Li: A Verifiable Secret Sharing Scheme Based on Identity Encryption[J]. Chinese Journal of Electronics, 2010,(9): 2059-2065.

[4] FENG HUA-MIN, SUN YI-RU, SUN YING: Private key sharing scheme based on identity authentication encryption and its application[J]. Journal of Computer Applications, 2014,(5):1507-1510.

[5] Su Jinshu, Cao Dan, and Wang Xiaofeng, et al. Attribute-based encryption mechanism [J]. Journal of Software, 2011, (6): 1299-1315.