CP-ABE Protocol for Iot with Cloud

Vishwesh J
Assistant Professor, Department of CSE
GSSSIETW, Mysuru

Dr. S. Meenakshi Sundaram
Professor & Head, Department of CSE
GSSSIETW, Mysuru

***Abstract*— the main requirement of any cloud-based platform for the deployment of Internet of Things applications is security. Cipher text policy Attribute-based encryption (CP-ABE) is a viable solution, particularly for cloud deployment, as an encryptor can ``write'' the access policy so that only authorized users can decrypt and have access to the data. However, most existing CP-ABE schemes are based on the costly bilinear maps, and require long decryption keys, ciphertexts and incur significant computation costs in the encryption and decryption (e.g. costs is at least linear to the number of attributes involved in the access policy). The Attribute-based encryption scheme fulfils the requirements for secure data retrieval. The concept is Cipher text Policy ABE), it gives an appropriate way of encryption of data. The encryption includes the attribute set that the decryption needs to possess in order to decrypt the cipher text. Hence, many users can be allowed to decrypt different parts of data according to the security policy.**

I. INTRODUCTION

Society is moving towards an “always connected” paradigm, where the Internet user is shifting from persons to things, leading to the so called Internet of Things (IoT). In this respect, successful solutions are expected to embody a huge number of smart objects identified by unique addressing schemes providing services to end-users through standard communication protocols. Accordingly, the huge numbers of objects connected to the Internet and that permeate the environment we live in, are expected to grow considerably, causing the production of an enormous amount of data that must be stored, processed and made available in a continuous, efficient, and easily interpretable manner. Cloud computing can provide the right technologies to implement the infrastructure that meets these requirements and can integrate sensors, data storage devices, analytic tools, artificial intelligence, and management platforms. Additionally, the pricing model on consumption of cloud computing, enables access to end-to-end services in an on-demand fashion and in any place. At the same time, service-oriented technologies, web services, ontologies, and semantic web allow for constructing virtual environments for application development and deployment [1].

As it is discussed in the following section, we still believe that to fully exploit the potentialities of the IoT paradigm, there is a strong need for further advancements in the design of platforms that: make easier the communications among objects; help the developers in creating new applications on top of the available objects’ services; allow the users to have complete control of their own data and objects; are reliable and efficient to support the interaction of billions of objects.

In the literature, several identity-based encryption schemes [2] to [4] with constant size secret keys and ciphertexts have been proposed. Attribute-based encryption (ABE), an extension of identity-based encryption, scheme was first introduced by Sahai-Waters [5] and has two variants, namely: Key-Policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, ciphertext is associated with the attribute set and the secret key is associated with an access policy. The ciphertext can be decrypted with the secret key if and only if the attribute set of ciphertext satisfies the access policy of secret key. On the contrary, in

CP-ABE, the ciphertext is associated with an access policy and the secret key is associated with an attribute set. The ciphertext can be decrypted with the secret key if and only if the attributes of the secret key satisfies the ciphertext access policy. As CP-ABE enables the data encryptor to choose the access policy and decide who can access the data, it is more suited for access control applications as compared to KP-ABE schemes.

II. LITERATURE REVIEW

Since the introduction of ABE in implementing fine-grained access control systems, a lot of works have been proposed to design flexible ABE schemes. There are two methods to realize the fine-grained access control based on ABE: KP-ABE and CP-ABE.

They were both mentioned in [6] by Goyal et al. In KP-ABE, each attribute private key is associated with an access structure that specifies which type of cipher texts the key is able to decrypt, and cipher text is labeled with sets of attributes.

In a CP-ABE system, a user’s key is associated with a set of attributes and an ecrypted cipher text will specify an access policy over attributes. The first KP-ABE construction [7] realized the monotonic access structures for key policies. Bethencourt et al. [8] proposed the first CP-ABE construction. The construction is only proved secure under the generic group model. To overcome this weakness, Cheung and Newport [7] presented another construction that is proved to be secure under the standard model. A store-and-forward approach has been already been implemented for delivering messages in disruption tolerant networks. Recently, several approaches have been proposed for unicast routing in disruption-prone networks.

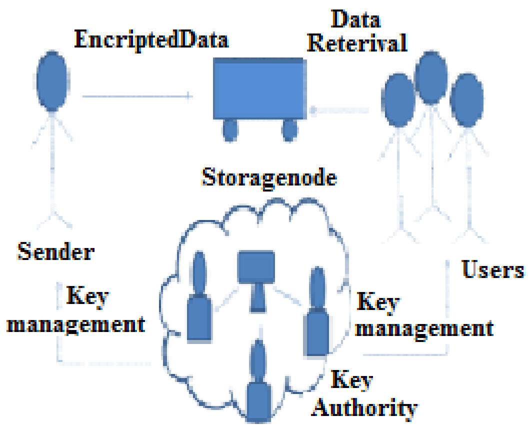

Fig 1: System Architecture

A. Attribute based encryption (ABE):-

Sahai and Waters [9] first introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this can be achieved only when user and server are in a trusted domain. But what if their domains arenot trusted or not same? So, the new access control scheme that is 'Attribute Based Encryption (ABE)' scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered.

In ABE scheme both the user secret key and the ciphertext are associated with a set of attributes. A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher-text and user secret key. Different from traditional public key cryptography such as Identity-Based Encryption, ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system.

Attribute-Based Encryption (ABE) in which policies are specified and enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy
ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CPABE) scheme.

B. Key Policy Attribute Based Encryption (KP-ABE):-

To enable more general access control, *V. Goyal, O. Pandey, A. Sahai, and B. Waters* [10] proposed a key-policy attribute-based encryption (KP-ABE) scheme. It is the modified form of classical model of ABE. Exploring KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications. In this scheme, data is associated with the attributes for which a public key is defined for each. Encrypter, that is who encrypts the data, is associated with the set of attributes to the data or message by encrypting it with a public key. Users are assigned with an access tree structure over the data attributes. The nodes of the access tree are the threshold gates. The leaf nodes are associated with attributes.

The secret key of the user is defined to reflect the access tree structure. Hence, the user is able to decrypt the message that is a ciphertext if and only if the data attributes satisfy the access tree structure. In KP-ABE, a set of attributes is associated with ciphertext and the user's decryption key is associated with a monotonic *access tree structure.* When the attributes associated with the ciphertext satisfy the access tree structure, then the user can decrypt the ciphertext.

C. Expressive Key Policy Attribute Based Encryption:-

In KP-ABE, enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure. Access tree structure specifies which all the ciphertexts the key holder is allowed to decrypt.
Expressive key-policy attribute-based encryption (KPABE) schemes allow for non-monotonic access structures. Non monotonic access tree structures are those may contain negated attributes and with constant cipher-text size. This is more efficient than KP-ABE.

D. Cipher Text Policy Attribute Based Encryption:-

In CP-ABE scheme, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. CP-ABE works in the reverse way of KP-ABE. In CP-ABE the ciphertext is associated with an access tree structure and each user secret key is embedded with a set of attributes. In ABE, including KP-ABE and CP-ABE, the authority runs the algorithm Setup and Key Generation to generate system MK, PK, and user secret keys. Only authorized users (i.e., users with intended access structures) are able to decrypt by calling the algorithm Decryption.

In CP-ABE, each user is associated with a set of attributes. His secret key is generated based on his attributes. While encrypting a message, the encryptor specifies the threshold access structure for his interested attributes. This message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP ABE technique, encrypted data can be kept confidential and secure against collusion attacks.

CP-ABE scheme consists of following four algorithms:

1. ***Setup :*** This algorithm takes as input a security parameter κ and returns the public key PK as well as a system master secret key MK. PK is used by message

senders for encryption. MK is used to generate user secret keys and is known only to the authority.
2. ***Encrypt :*** This algorithm takes as input the public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT.
3. ***Key-Gen :*** This algorithm takes as input a set of attributes associated with the user and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.
4. ***Decrypt :*** This algorithm takes as input the ciphertext CT and a secret key SK for an attributes set . It returns the message M if and only if satisfies the access structure associated with the ciphertext CT.

In CP-ABE depends how attributes and policy are associated with cipher texts and users’ decryption keys. In a CP-ABE scheme, a ciphertext is associated with a monotonic tree access structure and a user’s decryption key is associated with set of attributes.

Limitations of CP-ABE:-

However, basic CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP-ABE has limitations in specifying policies and managing user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies.

For realizing complex access control on encrypted data and maintaining confidential-ability, CP-ABE can be used. Encrypted data can be kept confidential even if the storage server is un-trusted; moreover, our methods are secure against collusion attacks. KP-ABE uses attributes to describe the encrypted data and built policies into user’s keys. In other hand CP-ABE, attributes are used to describe a user’s credentials. Data encryptor determines a policy for who can decrypt.

III. CONCLUSION

In this paper we have overviewed different attributes based encryption (ABE) schemes that can be used in cloud systems for flexible, scalable and fine grained access control.

In ABE scheme, there are both the ‘secret key’ and ‘ciphertext’ are associated with a set of attributes. ABE is further modified into KP-ABE that provides fine grained access control. In KP-ABE, attribute policies are associated with keys and data is associated with the attributes. Keys associated with the policy that is satisfied by the attributes can decrypt the data. Moreover, we have explored CP-ABE.

The CP-ABE scheme differs from KP-ABE in such a way that in CP-ABE, ciphertext is associated with an ‘access tree structure’ and each user ‘secret key’ is embedded with a ‘set of attributes’. Attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data.

REFERENCES

[1] L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” Industrial Informatics, IEEE Transactions on, vol. 10, no. 4, pp. 2233–2243, 2014.
[2] M. Zheng, Y. Xiang, and H. Zhou, ``A strong provably secure IBE scheme without bilinear map," *J. Comput. Syst. Sci.*, vol. 81, no. 1, pp. 125_131, 2015.
[3] C. Delerablée, ``Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Advances in Cryptology_ASIACRYPT*. Kuching, Malaysia: Springer, 2007, pp. 200_215.
[4] F. Guo, Y. Mu, andW. Susilo, ``Identity-based traitor tracing with short private key and short ciphertext," in *Computer Security_ESORICS*.Kuching, Malaysia: Springer, 2012, pp. 609_626.
[5] A. Sahai and B. Waters, ``Fuzzy identity-based encryption," in *Advances in Cryptology_EUROCRYPT*. Pisa, Italy: Springer, 2005, pp. 457_473.
[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.
[7] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.
[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
[9] J.Bethencourt, A. Sahai, and B. Waters. “Ciphertext-Policy Attribute- Based Encryption.” In Proc. of SP’07, Washington, DC, USA, 2007.
[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters. “Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data”. In Proc. of CCS’06, Alexandria, Virginia, USA, 2006.