International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

Secure Data Access Control with Cipher Text and It's Outsourcing in Fog Computing

Kirti Madhavi[1], Neha Bhutkar[2], Pratiksha Kadu[3], Babita Bhagat[4]

[1,2,3] Student, Computer of Engineering, PHCET College, Maharashtra ,India
[4] Faculty, Computer of Engineering, PHCET College, Maharashtra, India

---

Abstract - *In spite of the abundant advantages of storing data on cloud, Security still remains a major hurdle which needs to be conquered. The subsisting methods of protecting data on cloud have failed in preventing data theft attacks. An altered approach is carried out in our proposed system for securing the data, which is fog computing, in addition to the previous standard encryption mechanisms. The users using the Cloud are monitored and their access patterns are recorded. Every person who is trying to access the data is made to answer the security questions. Also an OTP is provided to avoid shoulder sniffing of password.*

Fog computing is nothing but cloud computing to the extreme of the network security. It provides computation and storage services via CSP (Cloud Service Provider) to end devices in Internet of Things (IoT). Attribute-Based Encryption (ABE) is a public key encryption scheme that allows users to encrypt and decrypt messages based on user attributes, which guarantees data confidentiality and powerful data access control. However, its computational cost for encryption and decryption phase is directly proportional to the complexity of the policies used.

***Key Words*: Access Control, Attribute Based Encryption, Attribute Based Signature, Cipher text-Policy Attribute Based Encryption, Cloud Service Provider, Data Security, Internet of Things, Fog Computing.**

1. INTRODUCTION

Today, cloud computing is considered a promising prototype of computing, since it can provide users with elastic computing resources based on shared computing techniques, virtualization, etc. However, the universality of Internet of Things (IoT) applications is changing the main factor of computing. Centralized computer systems suffer from unacceptable transmission latency and reduced system performance due to the extremely large volume traffic between IoT nodes and the cloud. Cloud computing is an encouraging technology that exploits the prototypes of cloud computing and IoT.

Although the "fog computing" prototype generates many benefits, security issues, including data privacy and access control, are the same as cloud computing and information technology. In addition, they are easier to compromise and unreliable, since fog nodes are distributed at the edge of the network and cost much less than servers in the cloud. Another way to solve these problems is to encrypt user data before uploading. Attribute-based encryption (ABE) is a one-to-many cryptographic technique that meets these requirements. It has tools and techniques that provide access control to the encrypted data through various access policies and attributes referring to private keys and cryptographic texts. In particular, the ABE encryption text policy (CP-ABE) allows the data owner to define the access policy on a universe of attributes that the user must possess to decrypt the encrypted text and apply it to the data. This ensures the confidentiality and control of high-precision data access.

However, existing solutions based on ABE are mainly aimed at managing secure access to data for users, few studies believe that there is no other requirement that the owner of the data you want to authenticate some users to update data encrypted. For example, Alice has outsourced cryptographic data and data to the cloud, and expects only her many friends who are authorized users can renew the cryptography of the initial text. Therefore, the key update is the secure encryption text that the user renews the cipher text must be able to convince the cloud service provider (CSP), which is a valid user. The traditional approach is to sign changed data, which means that CSP should maintain at the same time a list of valid public key users to verify users' identities. However, it would be a big burden to keep the list of keys, if the current number of users and CSP can know the identity of users in this way, revealing the user's privacy. A recent cryptographic technique known as based on study attributes (ABS) can help the CSP to verify if the user is valid. In an ABS system, the user can sign messages with a political request and its attributes. Then, with the signature, the CSP can verify the signer attributes satisfy the affirmation policy without even knowing the signer's identity.

Therefore, the adoption of ABE and ABS can guarantee data privacy, detailed access control and user verification, but at the same time also implies a high computational cost in cloud computing. The encryption, decryption and signature operations of ABE and ABS require a large number of module exponents, which normally grow linearly with the number of attributes in the policies. This is a significant challenge for users who access and modify data on IoT devices with limited resources with limited computing and archiving capabilities.

In this paper, we propose a secure control scheme for accessing data in cloud computing for IoT. The main contributions are as follows:

1]. we propose a detailed data access control scheme with updated cryptography text based on CP-ABE and ABS in fog computing. First, the confidential data of IoT devices are encrypted with multiple policies and then outsourced to the servers in the cloud through the nearby fog nodes. The authorized user whose attributes meet the access policy can decrypt the encryption text stored on servers in the cloud. Secondly, the authorized user can modify the decrypted data and re-subcontract them with his signature. If the user's attributes in the signature match the update policy, cloud servers can renew the encryption text.

2]. We provide a secure outsourcing framework that outsources most encryption, decryption and signature processes from the final IoT devices to fog nodes.

2. RELATED WORKS

Cloud computing is considered as a level in the middle of the cloud and end users are formed by fog nodes, such as routers, switches, etc. hardened. It is immediate for end users that servers in the cloud and some of the workloads and services that the cloud transfers to fog nodes. Fog nodes are semi-independent, as well as nodes in the cloud and data security would cause great concern to users when they store sensitive data on cloud servers through fog nodes. Therefore, a new access control system with cloud, fog and users should be considered, since the network structures and system prototypes are different, in which the fog nodes should serve the user to provide less computing complexity and greater flexibility for users.

ABE is an encouraging cryptographic technique to provide end users with scalable, flexible and fine-grained access control. The concept of ABE was initially proposed by Sahai and Waters as a new method for fuzzy identity based encryption. ABE has two variants, the key to the ABE (KPABE) and CP-ABE policy. In fact, it becomes a powerful mechanism that can be applied to perform access control in many IoT applications. Yu et al. introduced for the first time the problem of controlling access to fine-grained data in wireless sensor networks and adopted KP-ABE to protect data. Unlike KP-ABE, CP-ABE is very suitable for access control in IoT because of its expressiveness in describing the cryptographic text access policy. Hu et al. I designed a secure data communication scheme between portable sensors and data consumers through the use of CP-ABE in wireless networks for body areas. Jiang et al. introduced a CP-ABE scheme against the abuse of key delegation in cloud computing. Yeh et al. proposed a detailed framework for controlling access to health information in the cloud for lightweight IoT devices.

However, the most important drawback of the use of ABE in fog computing is the computational cost in the encryption and decryptions phase that is directly proportional to the complexity of the policy. Fog nodes, the edge of the cloud and closer to end users, are one of the best options for outsourcing proxy, which can be used to make massive calculations to reduce the computational overhead required in IoT devices with limited resources. The main solution of the current schemes is to distribute the calculations of the CP-ABE encryption and decryption phase, so that the limited IoT devices can delegate most of the consumption operations to the nodes of the network. Louniset al. has designed a cloud based architecture for medical WSNs, where sensor nodes outsource cryptographic operations to a reliable gateway that encrypts CP-ABE-based data before sending it to the cloud.

However, this solution adopts a completely reliable entity to perform data encryption that does not achieve the outsourcing of the practical calculation. Zuo et al. They designed a concrete ABE scheme with outsourced decryption for fog computing. Yang et al. proposed a concrete construction with a light computational overhead for the IoT health system, where a semi-reliable computing center is introduced to apply most of the heavy calculations in the data encryption phase. Yang and others have proposed two multiple cloud-based ABE schemes for IoT, which allow receivers to outsource computational decoding to the cloud. However, these schemes can only support outsourced encryption or in-work decryption. Zhang et al. has proposed an access control system for fog computing, which outsources the heavy calculation of cryptography and decoding in fog nodes, so the calculations to encrypt and decrypt are irrelevant to the number of attributes in the access policy.

To perform cryptographic text update services in fog computing, the CSP must be able to verify the user's test before accepting the modified cryptographic text. ABS is an emerging signature algorithm to ensure anonymous user authentication. It was introduced for the first time by Maji et al. Provide authentication without revealing user identities. Based on ABS, Ruj et al. has proposed a new decentralized access control system for the secure reading and writing of data in the cloud, which supports the authentication of anonymous users. In this scheme, the cloud verifies authenticity without knowing the user's identity before storing data. His et al. proposed an expressive scheme of ABS in IoT, which uses an attribute tree to ensure that only a user with the appropriate attributes that meet the access policy can approve the message.

However, in existing ABS works, a large computational cost is needed during the signature phase, which also grows linearly with the size of the predicate formula. Chen et al. they are the first to present two ABS outsourced schemes in which the computational load on the user's side is greatly reduced by outsourcing intensive calculations for CSP that are not reliable. Inspired by this, our schema performs anonymous authentication of the user during the update of the encryption text and delegates most of the signature operations to the fog nodes.

3. SYSTEM MODEL

System Model

1]. Attribute authority. The attribute authority is a fully trusted party which is in charge of generating system parameters as well as secret key for each user.

2]. CSP. The CSP is a semi-trusted party which provides high-capacity and online data storage service. It is also responsible for verifying the signature before accepting the updated cipher text.

3]. Fog node. The fog nodes are also semi-trusted parties which are deployed at the network edge and offer a variety of services. They are in charge of generating part of the cipher text and uploading the whole cipher text to the CSP, and also helping users to decrypt the cipher text from the CSP. Moreover, they assist end users to sign the cipher text update request.

4]. Data owner. The data owner has a great amount of data from the IoT devices to be uploaded to cloud. It is designed to define access and update policies to generate the whole cipher text with the fog nodes.

5]. User. The user is attached to fog nodes and equipped with IoT devices such as smart cameras, medical sensors and smart meters.

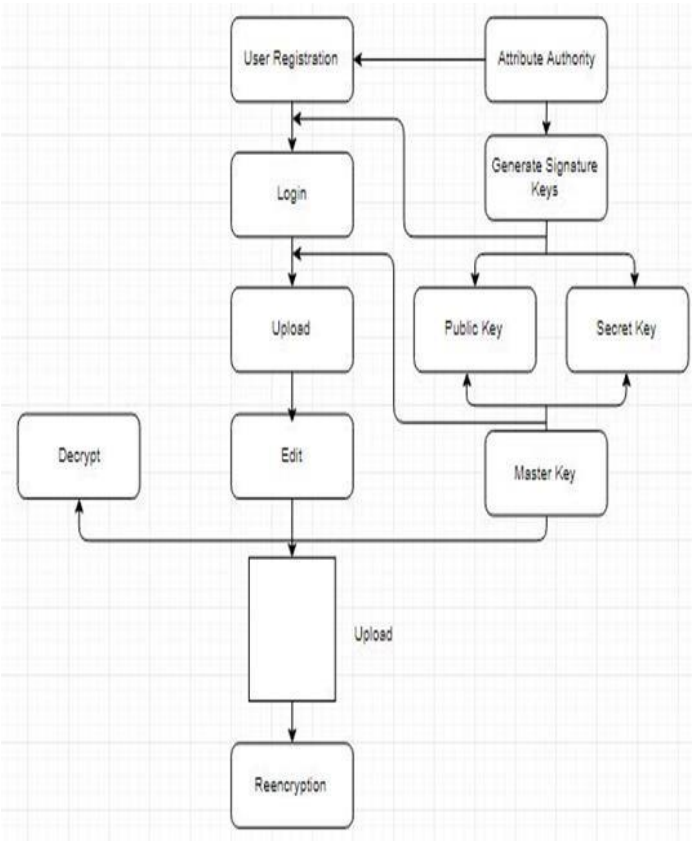

FIGURE 1: SYSTEM MODEL

SYSTEM DEFINITION

We define our proposed scheme by describing the following five phases and nine algorithms.

Phase 1: System setup

1) Setup 1: The attribute authority takes as input security Parameter k, and outputs the system public key (PK) and master secret key (MK).

Phase 2: Key generation

2) Key Gen (PK, MK, S). The attribute authority takes as input PK, MK, a set of attributes S, outputs the secret key SK for the user. And the outsourcing key SK' is sent to fog nodes.

Phase 3: Data symmetric encryption

3) Fog. Encrypt (PK, T). The fog node takes as input PK, an access policy T, outputs a partial cipher text CT'.

4) Owner. Encrypt (PK, M, Tu, CT). The data owner takes as input PK, a data M, an update policy Tu, a partial cipher text CT', and outputs the cipher text CT.

Phase 4: Data decryption

5) Fog. Decrypt (PK, CT, SK'). The fog node takes as input PK, a cipher text CT and a user's SK', and outputs a partial decrypted cipher text T if the attributes satisfy access policy T.

In the cipher text CT.

6) User. Decrypt (T, SK). The user takes as input a partial decrypted cipher text T and SK, then recovers the MK and outputs the plaintext M.

Phase 5: Cipher text update

7) Fog. Sign (PK, U, Tu, SK'). The fog node takes as input PK, a user's cipher text update request U and
SK', update policy Tu. It outputs a partial signature ST' and the global key GK.

8) User. Sign (PK, ST', SK). The user takes as input PK, a partial signature ST' and SK, outputs the signature ST.

9) Verify (Public key, ST, GK). The CSP takes as input PK, a signature ST and a global key GK. It outputs true if ST is a valid signature by the signer whose attributes satisfying Tu.

The workflow of our scheme is shown in the figure. In the initialization phase, the attribute authority uses the configuration algorithm to generate the system parameter. Generating keys with the algorithm, the authority attribute generates secret keys for owners and users of the data. To

achieve high encryption efficiency, the owner enters the data collected first with a random DK applying a symmetric encryption algorithm and defines an access policy and a policy update, the node uses the fog algorithm Encryption to encrypt partially data access policy, and then the data owner uses a proprietary .Encrypt algorithm to terminate the encryption with access to the policy and policy update and stored in the CSP. When accessing data, the fog node first uses the fog algorithm. Decryption to decipher partially encrypted text, the user can use the user. Decryption algorithm to recover data. After modifying the data, the user also uses phase encryption algorithms to encrypt the updated data. Before making the final modification, the user uses the user. Join algorithm to generate the signature with the return of partial signature of fog node. Algorithm of the sign. Then, the CSP uses the Verify algorithm to verify the signature and finally accepts the updated encrypted text if the signature is true. In the end, other users can get the updated data with the decryption algorithms. Therefore, users with Think Internet devices can access and efficiently update sensitive data in fog computing.

4. SYSTEM WORKFLOW

Security Model

In our scheme, cloud servers and fog nodes are curious, they execute the tasks and may collude to get the unauthorized data. Specifically, the security model covers the following aspects.

1) Data confidentiality: The unauthorized users which are not the intended receivers defined by data owner should be prevented from accessing the data.

2) Fine-grained access control: The data owner can custom expressive and flexible policies so that the data only can be accessed and updated by the users whose attributes satisfy these policies.

3) Authentication: If users could not satisfy the update policy in cipher texts, it should also be prevented from updating the cipher texts.

4) Collusion resistance: Two or more users cannot combine their secret and outsourcing keys and get access to the data they cannot access individually.

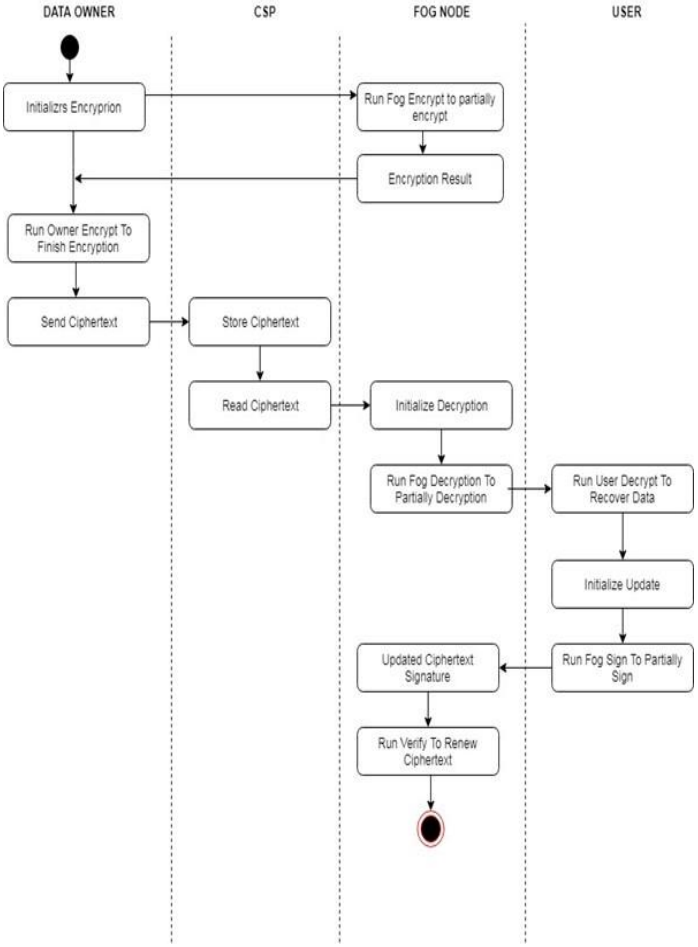

Figure 2: Work flow our scheme

5. CONCLUSION

In this paper, we put forward a secure data access control scheme in fog computing for IoT based on CP-ABE and ABS. The sensitive data of users are first encrypted with both access policy and update policy, and then outsourced to cloud servers via fog nodes. Thus, the users whose attributes meet the access policy can decrypt the cipher text. In order to address the problem of data changes, the CSP will check the signature, to ensure that only the users whose attributes meet the update policy can renew the cipher text. Hence, our scheme attains both fine-grained data access control and secures cipher text update. Also we use decoy information and user behavior profiling to secure data on Cloud. We launch a disinformation attack against malicious intruder using these two technologies thus giving them fake data and keeping the original data safe and intact.

Also, our scheme provides an outsourced encryption, decryption and signing construction by assigning most of the operations to fog nodes. The comprehensive performance analysis and experiments are performed, and the results show that our scheme can easily handle the increasing number of attributes, which is suitable for the resource-constrained IoT devices in fog computing.

6. REFERENCES

[1] Data collaboration in cloud computing," in Proc. IEEE/ACM 21st International Symposium on Quality of Service, Montreal, QC, 2013, pp.195-200.

[2]. F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in Proc. Information Security Practice and Experience - 7th International Conference, Guangzhou, China, 2011, pp. 83-97.

[3]J. Li, M.H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in Proc. 5th International Symposium of Information, Computer and Communications Security, Guangzhou, China,2010, pp. 60-69.

[4]Y. Jiang, W. Susilo, Y. Mu, and F. Guo. (2017, Jan.).Cipher text-policy attribute-based encryption against key-delegation abuse in fog computing. Future Generation Computer Systems. [Online].Available: https://doi.org/10.1016/j.future.2017.01.026

[5]L. Yeh, P. Chiang, Y. Tsai, and J. Huang. (2015, Oct.). Cloud-based fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation. IEEET transactions on Cloud Computing. [Online]. Available: https://doi.org/10.1109/TCC.2015. 2485199

[6]C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji. (2016, Nov.). CCA-secure ABE with outsourced decryption for fog computing. Future Generation Computer Systems. [Online]. Available: https://doi.org/10.1016/j.future.2016.10.028

[7]Y. Yang, X. Zheng, and C. Tang. (2016, Nov.). Lightweight distributed secure data management system for health internet of things. Journal of Network and Computer Applications. [Online]. Available: https://doi.org/ 10.1016/ j.jnca.2016.11.017

[8]A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques Aarhus, Denmark, 2005, pp. 457-473.