International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Impact Factor (2018): 5.426

A Survey on Data Centric Access Control with Role Based Proxy Re-encryption in Cloud Environment

Akhila Raj[1], Dr. K.S. Angel Viji[2]

[1] Post Graduation Student, College of Engineering Kidangoor

[2]Associate Professor, College of Engineering Kidangoor

Abstract: ***The security solutions currently available are based on perimeter security. However, cloud computing breaks the organization perimeters. At the point when data resides within the cloud, they reside outside the structure bounds of an organization. Users may loss control over their data and it raises reasonable security issues that block the adoption of cloud computing. Those issues includes questions like: Is that the cloud service provider(CSP) a truthful person or he accessing the data? Is it genuinely apply the access control policy defined by the user? In this research paper we present a survey and analysis of different methods that are used for protection of data over cloud and also for making data accessing easy as possible. A novel identity-based and proxy re-encryption techniques are used to protect the authorization model. In this, data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider' s access or misbehavior.***

Keywords: Authorization, Cloud computing, Data-centric security, Role-based access control

1. Introduction

Cloud computing is a large-scale distributed computing paradigm [1]. A large amount of convenient services such as Google Gmail, Amazon EC2, Facebook and Dropbox, have been provided with the arrival of cloud computing. Even though, many organizations must trust the security policies and mechanisms provided by cloud service providers. There are some security requirements, such as data encryption, key management, identity authentication, and access control [2]. Cloud service providers should satisfy those requirements.

Cloud computing technology involves the use of computing resources that are conveyed as a service over a network. In cloud computing model users have to give access to their data for storing and performing the desire business operations. Hence, cloud service provider should give the trust and security, as there is huge amount of valuable and sensitive data stored on the clouds. Not only the cloud services and its utilization increases gradually but also there are complaining about the non-competitive security aspects of the cloud by critics and security analysts. This trade-off can be compensated by introducing newer, efficient and effective cloud security solutions like good access control techniques and competent encryption/ decryption algorithms.

Access control technique sets the control and limitations to the actions done by several users over the data on the cloud. It processes the capability to allow or deny access to a resource on the cloud based on certain constraints and protocols followed extensively for all the users. The access control algorithm sets the abstraction level to the data for the cloud users thereby achieving confidentiality, integrity, availability and scalability.

Recently, a number of researchers have proposed various hierarchical architectures for the key management of cloud computing. These schemes have provided some of encryption, authentication, and access control mechanisms, but not all them together. However, these schemes also have a number of disadvantages. First, the computation costs of encryption and decryption are high. Second, they lack the integration of key management, encryption, authentication and access control mechanisms. Thus, the primary issue researched in this study is how to develop efficient encryption, authentication, and access control mechanisms.

2. Literature Survey

Cloud computing technology consists of the use of computing resources that are delivered as a service over a network. In cloud computing model users have to give access to their data for storing and performing the desired business operations. Hence cloud service provider must provide the trust and security, as there is valuable and sensitive data in huge amount stored on the clouds. There are concerns about flexible, scalable and fine grained access control in the cloud computing. For this purpose, there have been many of the schemes, proposed for encryption.

2.1 Attribute based encryption (ABE)

Sahai and Waters [3] 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. 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 [4], 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. 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.

Limitations: The cipher text and the users secret key are related with the set of attributes and these set of attributes act as a access policy. Only when there is a match between the attributes of the decryption key and cipher text, the users will be capable of decrypting the cipher text. The number of pairing operations increases with the increase of complexity of access policy. There is also possibility for the malicious users to leak the key to others without knowing the seriousness of traceability.

2.2 Key Policy Attribute Based Encryption(KP-ABE)

To enable more general access control, V. Goyal, O. Pandey, A. Sahai, and B. Waters [3], [5] 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.
In the cloud computing, for efficient revocation, an access control mechanism based on KP-ABE and a re-encryption technique used together. It enables a data owner to reduce most of the computational overhead to the servers. The KP-ABE scheme provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key, that is corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access tree structure.

The encrypted data file is stored with the corresponding attributes and the encrypted DEK. If and only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK. That can be used to decrypt the file or message.

Limitations: The data owner is not sure about who can decrypt the cipher text apart from choosing a collection of attributes which describes the data. The data owner is in a situation to fully trust the key issuer and also the scheme couldn't express the negative attributes because it has adopted a monotonic structure pattern for expressing access structure.

2.3 Cipher Text Policy Attribute Based Encryption (CP-ABE)

Sahai et. al[6] introduced the concept of another modified form of ABE called CP-ABE that is Ciphertext 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. 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 en crypting 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. 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.

In this scheme, the roles of ciphertexts and decryption keys are switched as that in KP-ABE. The ciphertext is encrypted with a access tree policy chosen by an encryptor. And the corresponding decryption key is created with respect to a set of attributes. As the set of attributes of a decryption key satisfy the access tree policy associated with a given ciphertext, the key can be used to decrypt the ciphertext. CP-ABE is conceptually closer to traditional access control models such as Role-Based Access Control (RBAC) [6] as users' decryption keys are associated with a set of attributes.

Hence CP-ABE is more natural to apply instead of KP-ABE, to enforce access control of encrypted data.

Limitations: 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.

2.4 Cipher Text Policy Attribute-Set Based Encryption (CP-ASBE)

As compared to CP-ABE scheme in which the 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.

To solve this problem, ciphertext-policy attribute-set based encryption (CP-ASBE or ASBE for short) is introduced by Bobba, Waters et.al [7] ASBE is an extended form of CP-ABE which organizes user attributes into a recursive set structure. Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) is a modified form of CP-ABE. It differs from existing CP-ABE schemes that represent user attributes as a monolithic set in keys. It organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. The CP-ASBE consists of recursive set of attributes.

Limitations: The challenge in constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key. There is challenge for preventing users from combining attributes from multiple keys.

2.5 Identity Based Encryption (IBE) and Hierarchical Identity Based Encryption (HIBE)

In an identity-based encryption scheme, data is encrypted using an arbitrary string as the key and for decryption; a decryption key is mapped to the arbitrary encryption key by a key authority. Hierarchical Identity Based Encryption (HIBE) is the hierarchical form of a single IBE [8]. The concept of HIBE scheme can help to explain the definition of security. In a regular IBE (1-HIBE) scheme; there is only one private key generator (PKG) that distributes private keys to each users, having public keys are their primitive ID (PID) arbitrary strings.

A two-level HIBE (2-HIBE) scheme consists of a root PKG, domain PKGs and users, all of which are associated with PIDs. A users public key consists of their PID and their domains PID (in combine, called an address). In a 2-HIBE, users retrieve their private key from their domain PKG. Domain PKGs can compute the private key PK of any user in their domain, provided they have previously requested their domain secret key-SK from the root PKG. Similarly, is for number of sub-domains. There also includes a trusted third party or root certificate authority that allows a hierarchy of certificate authorities: Root certificate authority issues certificates for other authorities or users in their respective domains. The original system does not allow for such structure. However, a hierarchy of PKGs is reduces the workload on root server and allows key assignment at several levels.

2.6 Hierarchical Attribute-Base Encryption (HABE) and Hierarchical Attribute Set Based Encryption (HASBE)

This scheme Hierarchical attribute-based encryption (HABE) is derived by Wang et.al [7]. It is designed to achieve fine-grained access control in cloud storage services.

It is a combination of HIBE and CP-ABE. In the HABE scheme, there are multiple keys with different usages. Therefore, we first provide a summary of the most relevant keys to serve as a quick reference. HASBE scheme is proposed and implemented by Zhiguo Wan et.al . The cloud computing system consists of five types of parties: a cloud service provider, data owners, data consumers, a number of domain authorities, and a trusted authority. The cloud service provider manages a cloud and provides data storage service.

Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority.

A domain authority is managed by its parent domain authority or the trusted authority. The trusted authority is responsible for managing top-level domain authorities. It is root level authority. For example, for an IT enterprise, employees are kept in the lowest domain level and above that there is department and above that there is top level of domain we call it as a trusted domain. It generates and distributes system parameters and also root master keys. And it authorizes the top-level domain authorities. A domain authority delegates the keys to its next level sub-domain authorities. Each user in the system is assigned a key structure. Key specifies the attributes associated with the users decryption key.

Zhiguo Wan et. al [7] given a HASBE scheme for scalable, flexible, and fine-grained access control in cloud computing.

The HASBE scheme consists of hierarchical structure of system users by using a delegation algorithm to CPASBE. HASBE supports compound attributes due to flexible attribute set combinations as well as achieves efficient user revocation because of attributes assigned multiple values. Thus, it provides more scalable, flexible and fine grained access control for cloud computing.

HASBE combines the functionalities of HIBE and ASBE. HASBE scheme seamlessly incorporates a hierarchical structure of system users. It uses a delegation algorithm to ASBE. Out of these schemes, the HASBE scheme provides more scalable, flexible and fine-grained access control than any other schemes in cloud computing.

2.7 Secure Role-Based Access Control (Sec:RBAC)

Perez et.al [9] propose a novel approach based on role based access control. A data-centric access control solution for self-protected data that can run in untrusted CSPs and provides extended Role-Based Access Control. This authorization solution provides a rule-based approach following the RBAC scheme, where roles are used to ease the management of access to the resources. This approach can help to control and manage security and to deal with the complexity of managing access control in Cloud computing.

Role hierarchy and object hierarchy capabilities provided by SecRBAC cannot be achieved by current ABE schemes. In SecRBAC, a single access policy defined by the data owner is able to protect more than one piece of data, resulting in a user-centric approach for rule management.

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 and CP-ASBE [10]. 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.

3. Conclusions

Different encrypted and data accessing methods were studied. A data centric authorization solution has been already proposed for the secure protection of data in the cloud, among which SecRBAC allows managing authorization following a rule-based approach and provides enriched role-based expressiveness including role and object hierarchies. Re-encryption key is used as cryptographic token to protect data against CSP misbehavior. Role hierarchy and object hierarchy capabilities provided by SecRBAC cannot be achieved by other ABE schemes. SecRBAC is a better method for data access and secure data.

References

[1] Shawish, A., and Salama, M., 2014. “Cloud computing: paradigms and technologies”. In Inter-cooperative collective intelligence: Techniques and applications, Springer, pp. 39–67.
[2] Huang, J.-Y., Chiang, C.-K., and Liao, I.-E., 2013. “An efficient attribute-based encryption and access control scheme for cloud storage environment”. In International Conference on Grid and Pervasive Computing, Springer, pp. 453–463.
[3] Bethencourt, J., Sahai, A., and Waters, B., 2007. “Ciphertext-policy attribute-based encryption”. In Security and Privacy, 2007. SP’07. IEEE Symposium on, IEEE, pp. 321–334.
[4] Yu, S., Wang, C., Ren, K., and Lou, W., 2010. “Attribute based data sharing with attribute revocation”. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ACM, pp. 261–270.
[5] Goyal, V., Pandey, O., Sahai, A., and Waters, B., 2006. “Attribute-based encryption for fine-grained access control of encrypted data”. In Proceedings of the 13th ACM conference on Computer and communications security, Acm, pp. 89–98.
[6] Wang, G., Liu, Q., and Wu, J., 2010. “Hierarchical attribute-based encryption for fine-grained access control in cloud storage services”. In Proceedings of the 17th ACM conference on Computer and communications security, ACM, pp. 735–737.
[7] Bobba, R., Khurana, H., and Prabhakaran, M., 2009. “Attribute-sets: A practically motivated enhancement to attribute-based encryption”. In European Symposium on Research in Computer Security, Springer, pp. 587–604.
[8] Wan, Z., Liu, J., and Deng, R. H., 2012. “Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing”. IEEE transactions on information forensics and security, 7(2), pp. 743–754.
[9] Perez, J. M. M., Perez, G. M., and G´omez, A. F. S., 2017. “Secrbac: Secure data in the clouds”. IEEE Transactions on Services Computing, 10(5), pp. 726–740.
[10] Sahai, A., and Waters, B., 2012. “Attribute-based encryption for circuits from multilinear maps”. arXiv preprint arXiv:1210.5287.

Author Profile

Akhila Raj, She is a post graduation student in College of Engineering Kidangoor. Specialization in Computer and Information Science. She received the graduation in computer science and engineering from Caarmel Engineering College, Ranny.

Dr.K.S. Angel Viji, is currently working as Associate Professor, Department of Computer Science and Engineering, College of Engineering Kidangoor. She is having 12 years of teaching experience and 8 years of research experience. She did her BE and M.E in computer science and engineering under Anna University

Chennai. She did her Ph.D in Noorul Islam university. Her area of interest includes medical image processing and network security. She is a member of IEEE. She is having more than 40 national and international conference and journal publications.