International Journal of Engineering & Technology, 7 (2.7) (2018) 20-24

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A Review of fine grained access control techniques

Rakesh Shirsath [1]*, Dr. K. V. Daya Sagar[2]

[1] Research Scholar, Department of CSE,
KLEF Deemed to be University, India
[2] Associate Professor, Department of CSE,
KLEF Deemed to be University, India
**Corresponding author E-mail: rakesh.shirsath@gmail.com*

Abstract

Nowadays cloud computing is most demanding technology where computing resources are availed as per demand through Internet. Cloud computing model also brings many challenges for confidentiality, integrity, privacy of data and data access control. As cloud computing develops vigorously, an increasing number of enterprises and individuals are motivated to upload their data sources to the public cloud server for sharing. It is not entirely credible for enterprises and individuals to transfer data owing to the openness of the cloud server, so they must encrypt data before uploading and also loose direct control of data. Therefore, an elastic access control or fine-grained access control approach for data is urgently required and becomes a challenging open problem. In this paper, the issue of access control is discussed by defining traditional access policies. Attribute based access policy is analysed with its types. Finally, comparison is made among all policies with respect to various parameters.

Keywords: *Attribute based encryption, Cipher text policy, Cloud Computing, Key policy, Hierarchical-ASBE, Security.*

1. Introduction

Currently, one of the issues faced by the organizations is about global access of data irrespective of location. Need of organization or individual to make computing resources and software available whenever required leads towards the idea of cloud computing. Computing resources, software and services are provided through Internet; hence cloud computing is cost efficient [4]. All such needs of end user are represented and fulfilled through service model which constitutes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). SaaS or delivery model enables third party to host different applications to make available for end users over the Internet. PaaS provides a platform for development and management of applications. Services provided by PaaS include database, server, operating system etc. IaaS provides computing resources as a service to the companies and these resources including servers, data centers and networking.

Computing and data storage are the two basic functions of cloud computing infrastructure. Consumers get access to data through Internet and complete the required computation in cloud environment. They are not aware about the location of data and machine which executes the computing task. Next is data storage system which takes care of data protection and security. Security is the primary factor to gain user's trust and successful use of cloud technology. Many techniques related to security or protection of data have been studied in cloud computing. However, data security related techniques need to be enhanced further [1].

On the basis of access scope, cloud is divided into three types: public, private and hybrid cloud. Public cloud can be used in public as a property of service provider and anybody can use the cloud services. Private cloud represents the property of an organization. Authorization plays a major role in private cloud to access the services from the provider. Hybrid cloud is the combined use of public and private cloud. Existing cloud service providing companies are Google, Amazon, and IBM [1].
Security is important area in cloud computing which is provided by the CSPs. Security is all about the confidentiality of data, data integrity, data availability, control over unauthorized access of data, withholding of information and amendment or deletion of information [1]. Expert scientists and developers are continuously trying to improve following security issues,

- Data security
- Access Security
- Network security

Various cloud security algorithms and technologies are currently in use which tries to makes cloud more secure. Security issues and risks prevented businesses from accepting cloud computing infrastructure [2]. Specific security and privacy risks regarding cloud computing respectively arise from the following,

- Authentication
- Access Control
- Shared Resources
- Virtualization
- Outsourced and Distributed Computing
- Mobile Access

Cloud storage is a promising and important service paradigm in cloud computing. Benefits of using cloud storage include greater accessibility, higher reliability, rapid deployment and stronger protection. Despite the mentioned benefits, this model also carries

new security challenges on data access control, which is a critical issue to ensure data security. The data access control in cloud storage environment has thus become a challenging issue. [2]

There is need of access control technique which works dynamically to obtain cross-domain authentication. Access control affects on primary security parameters of information security like data confidentiality, data integrity and data availability. Cloud service provider (CSP) is expected to achieve following objectives for access control:

- Control access of services offered to customer as per predefined policies and the level of service.
- Control access to data of multi-users in multi-tenant infrastructure.
- Control access to all functions of user.
- Maintain the policy of access control and keep up to date information of user profile [3].

Functioning of access control policies guarantees the authorized operations to be performed in the area of information security. Access control mechanisms take care of confidentiality, data integrity and data availability. The access control mechanism defines an object as a computing resource and subjects as an entity initiating the access request. This also presents number of security services namely authentication, authorization and auditing to achieve the desired access protection [5]. Access control models are traditionally classified as: (i.e.) Discretionary access control (DAC) (ii) Mandatory access control (MAC) and (iii) Role based access control (RBAC).

In DAC model, the data owner sets access permissions for other users. DAC is supposed to be the method of "who can access what" [3]. DAC model can be used with legacy applications and it yields management overhead in the multi-tenant environment.

MAC is based on the number of users accessing data. Mandatory access control is mostly based on the protection level. Here entity does not have right to change the access. This model is more adaptable for distributed system as compared to DAC. It abstracts the requirement of resource-user mapping. In MAC model instead of subject, administrator determines the access permissions for data in cloud. MAC mostly will be applied for government and military applications [2].

In RBAC, on the basis of roles and responsibilities assigned in system, user has an access to an object. By considering job authority and responsibilities of the job, permissions are defined and based on these permissions operations are invoked on the object. Objects set or action set which are associated with the subject is considered as role. Assigned role can be changed based on the priority of user and it is managed centrally. At the same instant, this scheme permits to execute multi-roles. This is the better approach to organizations such as cloud computing infrastructure, grid computing and peer to peer system. With comparison to DAC and MAC, and when system is not able to detect end user having fixed identity, this scheme works better [3].

The traditional access control models described above concentrates on an identity of subject only. DAC scheme provides basic security that can be bypassed. MAC scheme is difficult for administration. Hence it can not be utilized in contemporary transaction in distributed IT systems. The RBAC model works well for small size systems, but for large number of roles in enterprises it may become difficult to manage. All such limitations of these access control mechanisms are overcome by the attribute-based access control (ABAC) scheme [5].

Data is accessible only by the authorized user. There is a necessity of such a system, which is capable of securing the data from any known or unknown threats and data breaches. For secured system development, an efficient access control model is required which is based on desired security properties [4]. Developers get more possibilities and able to do better administration using fine grained access control mechanisms. There is a need to take care of authorization problem while providing the file synching-and-sharing service.

Due to multi-tenant property of the cloud, there are possibilities of data leaks and malicious attacks. Hence to keep data privacy and data confidentiality, it is necessary to set robust access control policy. Cloud providers can control data access as they have access to data in cloud. But in this case, it becomes difficult to keep privacy and confidentiality of the data [6].

Table I. Comparative Analysis

Sr. No	Access Control Mechanism	Access Control Owner	Nature of Access Control	Limitations
1	DAC	Data Owners	Trusted Computer System Evaluation Criteria Subject's or Group's identity-based access Explicit Authorization Good Flexibility	Provides basic level of security
2	MAC	Administrator	Limitation by operating system for subject or initiator to access	Difficult to administrate
3	RBAC	Data Owners	Access based on the roles of individual users For Coarse-grain access control	Suits for small size systems. Affects on performance if number of roles for large enterprises exceed.

Attribute based encryption (ABE) is an efficient technique that exploits attributes and access policies which help for fine-grained access control in cloud computing. It can be used to control unauthorized access to the data stored in a dynamic environment. It also supports additional features like scalability, flexibility, diverse type of users and heterogeneity which are required for the current storage platforms [7].

By comparing with existing public-key infrastructure mechanism for data confidentiality and privacy, attribute-based encryption is one better solution. When the identity and public key of the recipient is not known, ABE is useful as it requires only specific attributes of receiver. ABE is extended to Key-Policy based ABE (KP-ABE) and the Ciphertext-Policy based ABE (CP-ABE) scheme. KP-ABE enables senders to encrypt messages under an attribute set and secret key is associated with access tree. The ciphertext is associated with a attribute set. On encryption side, set of attributes are defined for decryption of ciphertext. When user submits the values of attributes to build an access tree then secret key is generated. In KP-ABE, there is no control over access of data. CP-ABE enables senders to encrypt messages using access tree and secret key is associated with an attribute set, the ciphertext is associated with the access tree. On encryption side, policy is framed for decryption of ciphertext. To decrypt the data, attributes of the user must satisfy the policy of corresponding ciphertext [3].

This paper reviews different access control mechanisms for security to data storage, data privacy and data confidentiality in cloud

computing infrastructure. Comparative analysis of the existing methods of data security aspects in cloud computing is presented.

2. Related Work

There are many access control methods based on an ABAC in dynamic, distributed and heterogeneous systems, we will take a closer look at those systems.

2.1 Attribute- based Encryption (ABE)

In the encryption process, confidential data are encrypted to prevent unauthorized access in the cloud infrastructure. Data security, data confidentiality and access control are provided by the different schemes. Attribute based encryption is encryption scheme which depends on authorized person, sender and receiver. Entities involved in this mechanism are authority, sender and receiver. Authority plays a major role in key generation process for data owners and end users for encryption or decryption of data [6]. According to attributes, the authority generates keys and gets it approved by authority. A data receiver completes the decryption process for received encrypted data using private key which is sent by the authority [3]. The user private key and the cipher text both are combined using set of attributes. In ABE scheme, every authorized user has a public key to encrypt data and private key to decrypt data [8]. ABE can be considered as a better choice for protection of privacy and confidentiality of data in a cloud. In ABE scheme, a user is identified using a set of attributes [9].

After satisfying all policy conditions, access is granted to the cloud. The access policy executes the validation process which consists of object, subject, attribute values and the type of operation. Hence access granularity is specifically greater than the traditional access control techniques. Versatility, simplicity and flexibility are the features of ABAC which are helpful for fine-grained access control authorizations applied by centrally managed access control schemes. Therefore, it becomes easy to apply new scheme and update existing schemes by the central policy repository without any effect on the integrated systems [5].
Initially identity-based encryption was proposed in which receiver's identity is described as an attribute set and it is a part of private key. When the distance between the attribute set of receivers and one of the sender is less than a threshold, a receiver is able to decrypt the plaintext correctly. ABE is defined formally by introducing the idea of access tree fine-grained access policy for ABE [10]. Multi-authority ABE scheme with key generation algorithm was proposed [10] which assumed that central authority mentioned in existing multi-authority ABE scheme was semi-trusted, hence it was able to decrypt plaintext irrespective of authorities and user's permissions. Need of the proposed algorithm was, communication between centralized authority and other authorities to generate keys together using individual's secrets key [10].

observed in CP-ABE. Monotonic ciphertext access structure tree and decryption process is associated with a set of key features [1].

Basically, cloud environment can support access control and secrecy. In addition, a set of attributes in the user's private key is a combination of the scheme, so a user can use these set of properties to meet the encrypted data access structure [8]. On encryption side, sender defines access policy for data encryption. Hence CP-ABE keeps confidentiality of data and reliable access control. CP-ABE works well for construction of outsourced data than KP-ABE [10]. The Traceable CP-ABE scheme is proved to be fully secured, highly expressive means it can support any monotonic access structure. CP-ABE is fully collusion resistant and efficient with sub linear overhead. This technique is not adaptively traceable as compared to policy specific black box mechanism. CP-ABE permits the data encryption using an access control policy over attrib-

2.2 Key Policy Attribute-Based Encryption (KP-ABE)

Key-policy attribute-based encryption (KP-ABE) is extended scheme of ABE, in which ciphertext is identified using attribute sets and private key is used to decrypt the structures. Message corresponding to a set of attributes, is encrypted with a public key. KP-ABE is specifically used for one-to-many communications. Sender having set of attributes yields ciphertext which is decrypted using user's private key and this private key is issued by the trusted attribute authority on the basis of key policy. Encrypted data is available with attribute set of data or message by encrypting it with a public key. KP-ABE enables user to control the ciphertext which is associated with access structure. Instead of data attributes, access tree structure is accompanied with user [8]. This scheme works well for structured organizations with the regulation that authorized entity can read particular documents.

The first KP-ABE scheme permitted the access policies to be represented in terms of monotonic technique over encrypted data. This model worked well and also cross-checked for better security using Bilinear Diffie-Hellman algorithm. In another proposed KP-ABE scheme, private keys are described as access formula over an attribute. [12] In KP-ABE scheme, policies are associated with keys and data with attributes. Attributes associated with data need to satisfy the keys associated with policy to decrypt the ciphertext. [5, 6] In this scheme for each encryptor a public key is defined to encrypt data using public key.

The secret key associated with the user plays a major role in access tree structure. Therefore, if data attributes satisfy the access tree structure then user can decrypt the ciphertext. In cloud computing infrastructure to perform efficient revocation, KP-ABE based access control technique and a re-encryption technique can be used [5]. It allows a data owner to reduce most of the computational upstairs to the servers. The KP-ABE scheme provides fine-grained access control. The encrypted data file with the respective set of attributes, the encrypted data and encryption key is stored. Using this stored information, user is able to decrypt data with the help of access tree [3]. KP-ABE has limitations like, encryptor don't have right to decide who can perform decryption for encrypted data. Encryptor need to trust on key distribution center. KP-ABE cannot work well for certain applications. It takes responsibility of user's secret key. It is providing fine grained access but lacking in scalability and flexibility [12].

2.3 Ciphertext Policy- Attribute Based Encryption (CP-ABE)

In ciphertext policy attribute-based encryption, policies which are used to decrypt are associated with the attribute set and secret key with attributes. The secret key is generated on the basis of its features [3]. Generalized identity-based encryption technique is utes, hence users have only rights to decrypt data using attribute set which satisfy the policy. It is also lacking in satisfaction of enterprise requirements like flexibility, access control and efficiency [10].

CP-ABE is limited for specifying policies and management user attributes due to the reasons as: Using cloud computing, data is accessible for user irrespective of time, location and device. Hence, the encryption system is expected to give high performance. Large-scale industry demands a delegation mechanism in the generation of keys inside an enterprise and also a scalable revocation mechanism. Existing CP-ABE mechanism completely depends on attribute authorities and store a heavy database of secret keys. This mechanism also lacks in flexibility and scalability [14]. Secret keys used in CP-ABE mechanism supports a single set of logical organized user attributes, so that users make use of all possible

combinations of attributes present in a single set to fulfil policies [13].

2.4 Hierarchical Identity Based Encryption (HIBE)

The identity-based encryption scheme, such as data and decryption key is encrypted using an arbitrary string. Private Key Generator (PKG) is used to generate and distribute private keys to each user. But in case of large network, PKG has more overhead. To reduce the overhead on PKG, Hierarchical Identity Based Encryption (HIBE) scheme is introduced. This method has selected a ciphertext security at random levels. Time during encryption and decryption, ciphertext size and private key size is directly proportional to the depth of a recipient in the hierarchy [15]. To get better results, Boneh et al. (2005) proposed a HIBE system which works efficiently and it requires ciphertext of fixed-size and a fixed number of bilinear map operations during decryption. With the help of identity-based broadcast encryption with key randomization, fully secured HIBE system was proposed by Gentry and Halevi (2009).

2.5 Hierarchical Attribute Based Encryption (HABE)

Cloud computing system has five entities as a) cloud service provider, b) data owners, c) data consumers, d) domain number and e) trusted authority [2]. The cloud management and storage of data services are provided by the cloud service providers [8]. There is need to combine HIBE scheme and CP-ABE scheme as both are supporting full delegation and fine-grained access control over attributes. HIBE is used to encrypt for exact destined receiver and CP-ABE is designed for encrypting to a set of attributes [15]. In hierarchical attribute-based encryption (HABE), there are four entities as Trusted Third party (TTP), Internal Trusted Third Parties (ITP), User and Cloud Service Provider (CSP). CSP is nothing but the interconnection of more capable servers to store encrypted data of organizations. It also stores replicas of encrypted data over different servers. TTP is used for key generation for end user and CSP. ITP is used to generate key user and maintain dynamic hierarchical structure of organization [15].

3. Comparative Analysis

After the review of various attribute-based techniques, we showed a comparison in the below table on the basis of different parameters. This table clearly indicate the behavior of different techniques on different parameters and provide a review that which technique is more efficient. It has been observed that there is need of such technique which avails the fine grained and multi-authority authorized access with less overhead, prevents data against anomalies and traces the traitors.

Table II. Comparative Analysis

Mechanisms / Parameters	ABE	KP-ABE	CP-ABE	HIBE	HABE
Fine grained access control	Low	Low, High for re-encryption technique	Average realization of complex access control	Lower than CP-ASBE	Good Access control
Access Structure	Monotonic	Monotonic	Monotonic	Hierarchical	Hierarchical
Collision Resistant	Average	Good	Good	Good	Good
Computational Complexity	High	Computational Overhead	Average computational overhead	Most computational overheads	Average
Efficiency	Average	Average, High for broadcast type system	Average, not efficient for modern enterprise environment	Better, Lower as compared to ABE schemes	Flexible and scalable
Reliability	Good	Poor	Poor	Good	Good
Scalability	Good	Poor	Poor	Good	Good

4. Conclusion

Data security and data privacy are major hurdles towards the development of cloud computing as an emerging technology. End user or organization is looking for trust of data security to transfer their data to cloud. Researchers have proposed techniques for data privacy, data confidentiality and data protection. Existing techniques can be strengthened to make it favorable by the cloud service providers. This paper surveyed different techniques about data access control concentrating on fine grained access control mechanisms. We surveyed different attributes based encryption (ABE) schemes used in cloud infrastructure for providing access to data on cloud. Many encryption schemes like KP-ABE, CP-ABE, HIBE, and HABE are discussed by taking various parameters and finally we conclude that all the algorithms are efficient on different domain. In Attribute based encryption, attributes are associated with two things which are “secret key” and “ciphertext”. Both are important concepts in terms of providing the security in cloud using encryption. On the basis of comparison table summary is presented which leads towards the need of most scalable, efficient and secure algorithm to provide security in cloud computing.

References

[1] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu, “Review Article Data Security and privacy in Cloud Computing,” International Journal of Distributed Sensor Networks, Volume: 10 Issue: 7, 2014.

[2] Priya G, Kavitha BR, Ramya G, Kumaresan P, Feslin Anish Mon, “An Access Control Models in Cloud Computing: A Review”, International Journal of Pure and Applied Mathematics, Volume 116 No. 24, 539-548, 2017.

[3] Meghanathan, Natarajan, “Review of Access Control Models for Cloud Computing”, Computer Science & Information Technology. 3. 77-85, 2013.

[4] Joseph K. Liu, Man Ho Au, Xinyi Huang, Rongxing Lu, and Jin Li, “Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services”, IEEE Transactions on Information Forensics and Security, Vol. 11, No. 3, March 2016.

[5] Erkan Yalcinkaya, Antonio Maffei and Mauro Onori, “Application of Attribute Based Access Control Model for Industrial Control Systems” *I. J. Computer Network and Information Security,* 2017, 2, 12-21.

[6] Jun Shao, Rongxing Lu and Xiaodong Lin,"Fine-Grained Data Sharing in Cloud Computing for Mobile Devices",Institute of Electrical and Electronics Engineers (IEEE),2015.

[7] Jiaye Shao, Yanqin Zhu, Qijin Ji, "Privacy-Preserving Online/Offline and Outsourced Multi-Authority Attribute-Based Encryption",Institute of Electrical and Electronics Engineers

(IEEE),2017.

[8] Etti Mathur, Manish Sharma, "A Review of Attribute based Encryption Technique for Security in Cloud Computing", International Journal of Computer Applications, Volume 159 – No 3, February 2017

[9] B Sankaraiah, D. Bhadru, G Shravan Kumar, "A Review on Different Access Control Mechanism in Cloud Environment", SSRG International Journal of Computer Science and Engineering, Special Issue, April 2017.

[10] Guofeng Lin, Hanshu Hong, and Zhixin Sun, "A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing", IEEE, pp. 9464 – 9475, 2017.

[11] Parmar Vipul Kumar J, RajaniKanth Aluvalu, "Key Policy Attribute Based Encryption (KP-ABE): A Review", International Journal of Innovative and Emerging Research in Engineering, Volume 2, Issue 2, 2015.

[12] Changji Wang1,2,3 and Jianfa Luo1,2 "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length" Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2013.

[13] John Bethencourt, Amit Sahai, Brent Waters "Ciphertext-Policy Attribute-Based Encryption" Supported the US Army Research Office under the CyberTA Grant No. W911NF-06-1-0316.

[14] Guojun Wang, Qin Liu, Jie Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services", 17th ACM conference on Computer and communications security, Pages 735-737, 2010.

[15] Shashikant Govind Vaidya, Shailesh Kisan Hule, Gaurav Balvant Dagade, Sharad Arjun Jadhav, "HABE (Hierarchical Attribute Based Encryption) Model for Supporting Dynamic structure of organization", Second International Conference on Advances in Computing, Control and Communication (CCN), 2012.

[16] Guojun Wang, Qin Liu, Jie Wu, Minyi Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Computers & Security, Vol:30, Issue:5, Page:320-331,2011.