Journal of Advanced Computing and Communication Technologies ***(ISSN:* 2347 - 2804*)***
Volume No.1 Issue No. 1, August 2013

SECURITY CONCERN ON CLOUD BASED ON ATTRIBUTES: AN SURVEY

By

Munmun Sharma Pahare
California State University East Bay,USA

Munmun.kinshuk@gmail.com

ABSTRACT

The Cloud computing is the way of using a network of remote servers hosted on the Internet to store, process and manage data, rather than on to the local server. Security is the most important concern in the cloud computing because the user data is transferring through the insecure medium i.e. Internet. In this paper, we present an overview of existing issues related to the cloud security and algorithms for finegrained access control and data security in the cloud environment. All these algorithms are described more or less on their own. Cloud security is a very popular task. We also explain the fundamentals of sequential rule mining. We describe today's approaches for cloud security. From the broad variety of efficient algorithms that have been developed we will compare the most important ones. We will systematize the algorithms and analyze their performance based on both their run time performance and theoretical considerations. Their strengths and weaknesses are also investigated. It turns out that the behavior of the algorithms is much more similar as to be expected.

Keywords

Cloud Security,Remote Control,Sequential rule mining,Fine grained access Control.

1. INTRODUCTION

More recently, Lots of schemes have been already proposed to achieve flexible and fine-grained access control. Unfortunately, these schemes are only applicable to systems in which data owners and the service providers are within the same trusted domain. In cloud computing, the data owner and Service providers are usually in different domain, a new access control scheme utilizing attributed-based encryption is proposed, which adopts the so-called key-policy attribute-based encryption (KP-ABE) to enforce fine-grained access control. This scheme has some drawbacks such as flexibility in attribute management and lacks scalability in dealing with multiple-levels of attribute authorities.

Over the last few years, cloud computing has evolved as one of the most effective domain in the IT Industry and has lulled and grabbed attention from both academic and professional world. Cloud computing holds the promise of providing computing as the fifth utility [1] after the other four utilities (water, gas, electricity, and telephone). The cloud computing provide scalability, flexibility, cut down the cost and capital investment and increased operational efficiency, and so on as its benefits. Different service-oriented cloud computing models have been proposed, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Numerous commercial cloud computing systems have been built at different levels, e.g., Amazon's EC2 [2], Amazon's S3 [3], and IBM's Blue Cloud [4] are IaaS systems, while Google App Engine [5] and Yahoo Pig are representative PaaS systems, and Google's Apps [6] and Salesforce's Customer Relation Management (CRM) System [7] belong to SaaS systems. These different cloud computing systems provides benefits to enterprise users by cut down the cost of hardware/software or no need to hire IT professionals to maintain this systems, on the other hand, utilities supplied by cloud computing are being offered at a comparatively low price in a pay-as-per-use style.

The benefits bring by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security becomes the serious problem in cloud computing, will prevent cloud computing extensive applications and usage in the future. One of the most important security issues is data security and privacy in cloud computing due to its Internet- based data storage and management. Cloud users have to give their data to CSP's (cloud service provider) for storage and business uses, while the CSP's are commercial enterprise which cannot be trustworthy. For any organization, data is very important. If the confidentiality of the data is disclosed to their competitors or to the public, the enterprise will face a big problem. Thus the cloud user need the assurance that the confidentiality of

their data is not going to be reveal in front of outsiders, including cloud providers and their competitors. This is the basic data security which is required. Other than that, flexible and fine-grained access is also desired in cloud computing environment.

2. RELATED WORK

The literature review is divided into two sections. In first section we describe the cloud securities general overview and in second section we describe and compare the different algorithms for Attribute Based Encryption.

In paper [1] the authors define the cloud computing and provide the architecture for creating cloud by using technologies such as Virtual Machines (VMs). It also explains the market strategy for resource management including both customer-driven service management and computational risk management to sustain Service Level Agreement (SLA)-oriented resource allocation. Moreover, it highlights the difference between High Performance Computing (HPC) workload and Internet-based services workload.

The state-of-the-art Cloud technologies have limited support for market-oriented resource management and they need to be extended to support: negotiation of QoS between users and providers to establish SLAs; mechanisms and algorithms for allocation of VM resources to meet SLAs; and manage risks associated with the violation of SLAs. Moreover, interaction protocols needs to be extended to support interoperability between different Cloud service providers. In addition, we need programming environments and tools that allow rapid creation of Cloud applications.

In this paper [8], the authors shows the security policies and with different methods and their limitation. This model defines policy as the collection of interdependent statements of provisioning and authorization. Each statement identifies context-sensitive session requirements. A reconciliation algorithm attempts to identify a policy instance compliant with the stated requirements. We define and prove the correctness of an efficient two-policy reconciliation algorithm, and show by reduction that three or more policy reconciliation is unmanageable. It also identifies several heuristics for detecting and combating intractable provisioning policy reconciliation, and shows that reconciliation of (many) reasonable authorization policies can be efficient.

Policy in our model defines interdependent statements of provisioning (session configuration) and authorization. We show that the general problem of provisioning policy reconciliation is unmanageable. By restricting the language, we show that reconciliation of two policies becomes manageable. However, reconciliation of three or more policies under this restriction remains unmanageable. The design and implementation of the Ismene policy language is based on the Policy Model. The Ismene language and supporting infrastructure is built on top of previously designed algorithms.

In paper [9], the authors described the different security issues and challenges in accepting cloud computing model. Usually the data services provided by the cloud are delivered by the third party provider who owns the infrastructure. The challenges related to cloud computing are based on the users authenticity. IDC conducted a survey in 2008 for knowing the challenges due to which the organizations feared to adopt cloud computing.

The challenges are as follows: Security, Costing Model, Charging Model, Cloud Interoperability Issue and Service Level Agreement [SLA].

In this paper [10], the authors discussed issues related to security with Cloud Based Computing and Cloud Operating Systems. In recent time, the Cloud computing experienced a remarkable increase in popularity as major companies such as Google and Microsoft have started to release cloud based products, denote the use of the cloud, and even release an open source Cloud OS. As the popularity of cloud computing increases the demand for security will increase. In this the authors try to figure out specific security concerns for cloud computing as well as shared security issues between cloud and other computing. It also propose a method for allowing the user to select specific security levels of security for items and make a list of security items that all users should be aware of before opting to use cloud based services.

There are lots of security issues related to cloud computing. Few of them are as follows.XML signature [11], Flooding [11], Browser Security [11], Reputation fate Sharing [12], Loose Control over Data, dependence of Internet and many more.

This section shows the algorithms based on Attribute based Encryption.

Attribute Based Encryption (ABE) is one of the encryption schemes, which is a novel domain where such policies are magnified and glorified 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 (CP-ABE) scheme. In KP-ABE scheme, attribute are associated with keys and data is associated with attributes. The can be decrypted only when the keys associated with the policy that is satisfied by the attributes associating with data. In CP-ABE schemes, 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. The scheme proposed in the paper [13] is based on the KP-ABE, tries to provide the fine grained access control. But this current work not provides the fine grained access, data confidentiality and

scalability simultaneously. The different algorithms are as follows:

A. Key-policy Based Attribute Based Encryption

Key-policy Attribute Based Encryption scheme is public key cryptography that is for one-to-many communication. In this data are associated with attributes for which a public key is defined. The encryptor associates the set of attributes to data by encrypting it with public key. Access structure is defined as access tree over the data with attributes which is assigned to users. The secret key is defined to show the access structure. The user is able to decrypt the data or message, if and only if the ciphertext satisfy the access structure.

KP-ABE [13] is access control mechanism, which works with re-encryption techniques for efficient user revocation in cloud computing. This scheme permits a data owner to reduce most of the computational overhead to cloud servers. The KP-ABE encryption scheme is used to provide 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 corresponding to a set of attributes in KPABE, which is generated corresponding to an access structure. The data file that is encrypted is stored with the corresponding attributes and the encrypted DEK. Only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a users key, then the user is able to decrypt the encrypted DEK, to decrypt the file or message.

The problem with this scheme is that the encryptor is not able to decide who can decrypt the encrypted data except choosing descriptive attributes for the data, and has no choice but to trust the key issuer.

B. Expressive Key Policy Attribute Based Encryption

Among the encryption methods in clouds Attribute-based Encryption (ABE), allows fine- grained access control on encrypted data. In the Key Policy Attribute Based Encryption, Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key corresponding to a set of attributes in KPABE, which is generated corresponding to an access structure. This expressive key-policy attribute based encryption (KP-ABE) schemes allowing for non-monotonic access structures (i.e., that may contain negated attributes) and with constant cipher-text size. Towards achieving this goal, show that a certain class of identity-based broadcast encryption schemes generically yields monotonic KP-ABE systems in the selective set model. A new efficient identity-based revocation mechanism, when combined with a specific instantiation of our general monotonic construction, provides rise to the first truly expressive KP-ABE realization with constant size ciphertext. The drawback of these new constructions is that private keys have quadratic size in the number of attributes. On the opposite side, they reduce the number of pairing evaluations to a constant that seems to be a novel feature among expressive KP-ABE schemes.

C. Ciphertext-policy Attribute Based Encryption

In lots of decentralized systems users should only able to access the data if a user own certain set of attribute. The only way to apply such policies is to employ a trusted server to store the data and mediate access control. If server compromises the stored data, then the secrecy of the data is also compromised. For complex access structure, a new system is designed on encrypted data that known as CP- ABE [14]. Data secure by using this encrypted techniques even if the storage server is untrusted. Previously defined Attribute-Based Encryption systems based on key attributes to describe the encrypted data. Data encrypted by user private key which are specified by a set of attributes and decrypt by a specific policy over these attributes specifying which users are able. In this system, 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. This policy conceptually near to former access control method such as Role-Based Access Control (RBAC).

This system is based on how attributes and policy are associated to ciphertext and users' decryption key. In CP-ABE scheme, a monotonic structure is associated with the ciphertext, and set of attributes associated with users' decryption key. Unlike KP-ABE, the roles of ciphertext and decryption key are switched in CP-ABE. The encryptor chooses the tree access policy to encrypt the data, and set of attributes are used to create decryption key. If the set of attributes associated with decryption key satisfy the tree access policy associated with the ciphertext, and then the key can be used to decrypt the ciphertext.

The CP-ABE scheme is not good enough to support access control in modern enterprise environment. Because it requires flexibility and efficiency in specifying policies and user attributes. In this scheme, the key used for decryption supports only user attributes organized as a single set, so user can use all possible sets of attributes in a single set issued with keys to satisfy policies.

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

Cipher Text Policy Attribute Set Based Encryption is a new variant of CP-ABE, unlike existing CP-ABE schemes that represent user attributes as a single set of keys, organizes the user attributes into a recursive set based structure and allows

user to impose dynamic constraints on how those attributes may be combined to satisfy the policy.

In CP-ASBE, uses recursive set structure is denied to maintain users' attributes unlike CP-ABE which uses single set of attributes to satisfy the policies.

In CP-ABE Scheme, user attributes are organized as the single set for decryption key, the user can use all possible set of attributes in a single set issued in their key to satisfy policies. To solve this problem, new scheme introduced known as Cipher text Policy Attribute Set Based Encryption. It is extended form of CP-ABE which manages user attributes into a recursive structure.

CP-ASBE allows, the user attributes to allow in recursive set and policies that can selectively restrict decryption user to use attributes from within a single set or allow them to combine attributes from multiple sets. CP-ASBE can support compound set of attributes without scarifies with the flexibility to easily specify the policies involved in singleton attributes. It also supports multiple numerical assignments for a given attribute by placing each assignment in separate set.

3. Conclusion

Cloud computing offers different advantages for organizations and individuals. There are certain issues related to the security and privacy of the user data. Cloud security is the major issue in cloud computing. We studied different security issues and different type of algorithms of encryption for fine grained access control and security of user data. We will try to improve the mechanism of single set of attributes present in the previous work by using hierarchical attributes set of users.

4. REFERENCES

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput. Syst., vol. 25, pp. 599–616, 2009.

[2] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/

[3] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws. com/

[4] R. Martin, "IBM brings cloud computing to earth with massive new data centers," InformationWeek Aug. 2008 [Online].Available:http://www.informationweek.com/news/hardware/data_centers/209901523

[5]Google App Engine [Online]. Available: http://code.google.com/appengine/

[6] K. Barlow and J. Lane, "Like technology from an advanced alien culture: Google apps for education at ASU," in Proc. ACM SIGUCCSUser Services Conf., Orlando, FL, 2007.

[7] B. Barbara, "Salesforce.com: Raising the level of networking," InfoToday, vol. 27, pp. 45–45, 2010.

[8] P. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2002.

[9] Kuyoro S. O., Ibikunle F. & Awodele O. ,"Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011

[10] J. C. Robert II, W. Al- Hamdani "Who Can You Trust in the Cloud? A Review of Security Issues Within Cloud Computing", Information Security Curriculum Development Conference 2011, October 7-9, 2011, Kennesaw, GA, USA.

[11] Jensen, M., Schwenk, J., Gruschka, N., and Iacono, L. 2009.On technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing.

[12] Y. Chen, V. Paxson, and R. Katz.What's New About Cloud Computing Security? Technical Report UCB/EECS-2010-5, Berkeley, 2010

[13] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542.

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption" in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.