International Journal of Electrical and Computer Engineering (IJECE)
Vol. 3, No. 4, August 2013, pp. 504~508
ISSN: 2088-8708

Enforcing Multi-user Security Policies in Cloud Computing

Shubhada P. Mone, Sunita S. Dhotre
Departement of Computer Engineering, Bharati Vidyapeeth University, Pune.

Article Info

Article history:

Received May 10, 2013
Revised Jun 25, 2013
Accepted Jul 10, 2013

Keyword:

Cloud computing
Policy based system
Firewall
Cryptographic method
Fine grained data access control

ABSTRACT

The user can access data from any server with unlimited data with the security. Multi-user tendency will cost lesser than the expected cost in the single user environment. While dealing with cloud computing, confidential data can be secured from the unauthorized access and internal threats. Cloud servers use smart techniques for achieving this requirement like encryption and decryption of data. The database is stored in the encrypted format on the server & a complex query can be fired on it. Cloud server will maintain the access control policies to reveal the data from the database that are in the encrypted format. In the access control policies, we use KMA (Key Management Authority) which provides the keyset for encryption & decryption of the database. The attributes entered by the user will create one public key which is cipher text based. So this technique is called as cipher text based technique. This key is used for encryption. While registering, user will choose the policy and select the attributes on which security policy is based. Because of this it is called as cipher text policy attribute based encryption (CP-ABE). To achieve this complex encryption, we can use many algorithms like AES or DES encryption algorithms with CPABE algorithm. This scheme allows making SQL-like queries on encrypted database in multiuser environment while at the same time, the database owner assign different access rights to users that defines a specific policy for the database. The major use of this encryption is privacy, access control and data confidentiality and multi-user access control.

Corresponding Author:

Shubhada Parashar Mone,
C-53, Shama-Prasad society, near sawant vihar,
pune-satara road, katraj, Pune.
State- Maharashtra, Country-India.
Email: shubhadamone@mmcoe.edu.in

1. INTRODUCTION

Now a days, Cloud computing is popular because of multi user ability & virtualization facilities which provides scalability for business enterprise. Instead of sharing any software with one user, it is more beneficial to access it by many users. In this case, we should take a consideration of many issues like, security, fine-grained access control, and unauthorized use of cloud resources and services in terms of attacks. For achieving secure, scalable and fine-grained data access control in cloud computing, traditional method that is assuming the data owner & the servers storing data in the same trusted domain is not much effective because in this case, servers are responsible for enforcing access control policies only for the same domain but if the information is asked by another domain, we have to do another setting for that. Again another issue is if the data owner & cloud servers are in different domains, the data resources are not physically under the full control of the owner, or any single cloud server. The existing solutions to these problems are either applying cryptographic methods or encrypt the data & disclose keys to authorized users [1]. The cryptographic methods are so complex that normal user can not recognize how to apply it. If we think about the second solution that is encryption of data, it causes heavy computation overhead on the data owner for a key distribution and data management. To overcome these difficulties user can either use

services for data security and access control for data on cloud servers. For this, user defines & enforces access policies based on data attributes. Also user can delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disabling the data. Another approach to overcome the prescribed difficulties is data re-encryption & user secret key update to cloud servers without disclosing data contents or user access privilege information. This can be achieved by key policy Attribute-Based Encryption.

For implementing the security, Hadoop Distributed File System (HDFS) which is default back end for the hadoop Map/Reduce framework is used for maintaining security [5]. The main threats in HDFS arise from the lack of user-to-service authentication, service-to-service authentication & the lack of encryption when sending & storing data. Moreover, even if typical user does not have a full access to the file system, HDFS is vulnerable to various attacks that it can not detect, such as Denial Of service. We always have aim of providing high security mechanism for cloud storage services, as data access operations are vulnerable against a wide range of security attacks which cause to damage the system and to affect its overall data access performance and response time. In high level architecture of the security management framework is described in such a way that it provides greater security [5].

A proxy-based re-encryption mechanism is useful for constructing a temporal access control. In this re-encryption mechanism, cryptographic integer comparisons are obtained successfully which predicts efficient benefits, such as flexibility, supervisory, and privacy protection [6].

2. SECURITY & SECURITY RISKS

In any company, end to end application security can be achieved by isolation. In case of isolation, we want cloud providers to isolate as well as isolate components & users within each user's application. Each cloud user provides one or more services and it can be converted into multi-users. While accessing all these services, we want to ensure that user's data should remain private. Even if we use multi-threading, it should share a service's address space. Thus cloud users guarantee that their user's data is safe from leakage to unauthorized recipients. For this reason, cloud providers therefore need to offer their users strong but usable isolation support. Mainly security risk is from hacker's sites. Security service should be available to protect number of sites that all are accessing our application service in the cloud. Second security risk is to build a cloud intelligent network. It gives a challenge to cloud computing to securely connect remote sites to Infrastructure-as-a-service (IAAS) cloud. Third security risk is to apply strategies for enforcing consistency policies to protect against web-based threats. Fourth security risk is to secure the connection to the cloud. To solve or if possible to avoid these security risks, a good policy-based cloud should be enforced which achieves all these preventions. That means event though you are the architect of great technology, but if you have a password problem, or if you are not following procedures, it will be all in vein!!!

To improve the security, following tasks can be performed-

1. Perform routine backups of your operating system, programs, applications and all data files.
2. Separate the back-up network from main traffic or main work area. But do not back-up secured data over a network that everybody uses. Restricting access to back-up network will allow you to more effectively control access to back-up equipment & applications.
3. We have to make sure that all back-up equipments should keep in a secure area.

Other major security problems are authentication, identity management, access control and policy integration. In case of access control issue in cloud computing, that is more related to the customers [1]. This customer can be an individual or group of people, organizations. This leads to the major security risk that cloud infrastructures are usually operated by commercial service providers that are outside of the trusted domain of the user, even in another country with a different environment. Thus insecure information flow occurs in cloud computing with high risks and this should be avoided in the network. With the growth of web applications and web services deployed on the Internet, the use of policy based approach is useful for providing security requirements covering large, open, distributed and heterogeneous computing environments [8].

3. NEED OF POLICY BASED SYSTEM

Use of policy-based client-server system is the best solution to achieve all these criteria. A policy based networking approach helps to find the goals such as providing access to authorized users from certain locations or using specific devices, routing all traffic from point-of-sale systems in branch locations using encryption & a guaranteed quality of service, providing priority to customers during peak network traffic periods and blocking employee access to non-business social networking sites during business hours. Many companies have implemented the policy-based cloud which defines their respective goals. Policies must

focus on user activities of all authenticated & unauthenticated users inside the firewall. The users can be customers, partners, employees, or inside intruders. Most policy violations can be done by the insiders not outside hackers in the companies. We should not forget to detect events in real-time applications. We should keep checking log-files daily always after some hours or days or in a week, so that any unauthorized activity can be stressed and stopped in time. Also policy based response process should be established [1]. While designing a policy-based cloud, we should consider the information flow in cloud computing. It may happen that when one user communicate with the server for accessing the information, that information should be told to any another user [2]. If any another user requires to access the information, which can be accessed by the server only. In this case, server can't control to a specific user for disclosing the confidential information but can provide confidentiality while accessing by another user. This can be most obvious in case of Infrastructure-as-a-service (IAAS).

Another issue is to check whether the data owner and cloud server are in same domain or different! [7]. If both are in same domain then it is very easy to share the information and the possibility of attack is very less. But if both are in different domain, it will increase the possibility of unauthorized access for the critical data. Policy-based computing handles complex system properties by separating policies from system implementation. In distributed, heterogeneous and web-oriented computing, the increasing complexity of policy based computing demands strong support of different techniques [8]. Without analysis, most benefits of policy-based and declarative policy languages may be in vein.

While defining security policies, the policy management module has to meet certain requirements that are-

1. The format used to describe the security policy should be much flexible and it should be much more expressive enough to allow the system administrator so that he can translate any type of attack into a policy that can be understood by the policy management module.
2. The security policy management module should be extensible. Many specific attacks needs an enriched policy format according to particular events that are observed by the previous activities.
3. As the process of writing the security policies is very difficult task so this process has to be automated by using any another software which is compatible with the security environment.

Thus to achieve these above requirements a good policy based environment should be achieved by the cloud server and owner [5]. It doesn't matter of the domain limits.

4. ARCHITECTURE

Always in cloud computing, user always hopes for the security. The critical data should be secured from the unauthorized users. For this reason encryption while accessing data is achieved. The database owner of the database stores the information from the cloud provider. The database owner is responsible for user management deciding who is authorized to access the data. The owner can assign to each user a different access policy. The database owner maintains a table with each user's access to different attributes of the database. According to the access specification, the value is maintained in the database table for each attribute. User can have access to limited attributes or all attributes, that is not known to any user. To apply these complex queries can be applied on the database. We encrypt the table name & the names of the attributes the user wants to access with specific function & a key. We transform the WHERE clause of the query into the tree where each condition is represented by AND and OR gates. The encrypted code will depend on this newly created tree for each query. Key Management Authority (KMA) is responsible for generating & revoking keys. KMA will generate the key-set with the support of cloud server for all authorized users. The user is an entity that wishes to encrypt or decrypt the data. Any user can retrieve the data from the database & encrypt it. According to the policy decided by the user, KMA will generate the key-set. By using this key set, the attributes in the database gets encrypted by using KP-ABE. These encrypted records are stored in the database. This technique hides not only the data but even attributes names of the table from the cloud server & other unauthorized users. For encrypting the values of the attributed, the searchable data Encryption (SDE) scheme can be used [4]. This scheme can be used for the string encryption at a time. Cloud server is a part of the infrastructure provided by the cloud provider. A cloud server stores the encrypted data in the database and performs encrypted searches according to the user's request. According to the encryption of cipher texts on sets of attributes, users are associated with access policies. These access policies describe about the key of decryption of cipher text. Applications of this attribute-based encryption are like property based Broadcast Encryption & attribute based Access Control (ABAC, used in SOA). In many cases, Distributed Attribute-based Encryption is applied for managing attributes independently. That includes different algorithms & use of variety of keys. In our algorithm we are going to use this KP-ABE for to encrypt the data. In many cases, it happen that cloud users themselves are cloud providers [7]. They publish data on cloud servers for sharing and need fine-grained data access control and at the same time the

data owner will stores the abundant information which will be provided to other users. This is more helpful foe efficiency and to maintain the good economy.

KP-ABE is a public key used for multi-user access ability module. In this encryption, data are associated with attributes for each of which is a public key. The encryption associates the set of attributes to manage by encrypting it with the corresponding public key components [7]. A KP-ABE scheme is composed of four algorithms such as setup, encryption, key generation and decryption. Proxy-re-encryption can be also applied on the encrypted data. This is semi-trusted proxy which is able to convert a cipher text encrypted under the public key into another cipher text that can be opened by another user's private key without knowing actual data. If we deal with the web access control policies, these are often error prone due to lack of logical and formal foundation [3]. As in the web we cannot maintain a uniform structure as well as a uniform policy so when access control policies will not achieve the security to critical data that we have the goal about it.

5. KEY POLICY-ATTRIBUTE BASED ENCRYPTION

Key-policy attribute based encryption is very useful for achieving fine grained access control on encrypted data. Actually attribute-based encryption is of two types- Key policy- Attribute based encryption (KP-ABE) and cipher text policy-Attribute based encryption (CP-ABE). The KP-ABE scheme with constant size cipher text allows many expressive policies. In this scheme, first identity-based broadcast encryption will be applied and then it yields KP-ABE scheme via generic transformation. It preserves cipher text size & provide guarantee about security of the database.

The time complexity provided by such same size cipher text KP-ABE scheme will be O(1), which is the best access time complexity. Without compromising in the efficiency of the KP-ABE method, we can reduce the extra load of encryption by using identity based revocation method.. In this revocation method, the set of allowed attributes are only revoked for encryption which reduces the size of cipher text. In case of attribute based encryption, there are two major schemes- dual policy based ABE and mixture of KP-ABE & CP-ABE method. To obtain KP-ABE scheme with compact cipher text , requires much more efforts on it. According to this encryption method, first the setup algorithm builds the master public key and master secret key. Key management authority (KMA) handles these keys and when any user requires accessing the database, it provides the master public key. This master public key constitutes the selected attributes from database file which is the minimum requirement to match for encryption or decryption. Before providing public key to any user, KMA checks whether the user is already registered. The owner of the database have the list of users those can access the database file, including selected attribute list. For better security, this access-list file is also stored in the encrypted format. While checking for the valid user, KMA take the help of this access file. Even though any hacker will be able to crack the security of KMA but the encrypted access-list file will be the next challenge! Server stores the database files with different attributes. The server use the encrypt algorithm which require master public key, message and cipher text index number as input and provides the encrypted format of database file as cipher text 'C'. The server stores this encrypted file. When any third party wishes to access this encrypted database file and send a request to server, KMA first check his name in the access list file. If it is already registered with the KMA and owner, server can provide access. The master secret key is already provided to all authorized users. By using this key and key index value, every authorized user will generate private key. This generation of private key can be done by keyGen algorithm. By using this private key, third party user can decrypt the encrypted database file. Cipher text has set of attributes and user also has set of attributes. If more than k attributes match, third party user can decrypt the data. User can decrypt if and only if attributes from cipher text can satisfy the key policy so this scheme is called as key policy- attribute based scheme. In the key policy, many AND and OR gates are used. The main application of this scheme is biometrics. Main aim behind this scheme is to avoid collusion.

Secret key sharing can be possible while dealing with this scheme. We can map a tree structure with AND and OR, which replicate secrets for OR's and split secrets for AND's. This checks all public parameters against the list of all possible attributes. It select certain selected attributes and combine with original message, yields cipher text. While decrypting, any combination of attribute with the private key reconstruct the original message. The security can be provided by Diffie-Hellman algorithm.

6. CONCLUSION

In this scheme, we try to keep the database in encrypted format up to the lowest level. The encryption of every value in the attributes as well as every name of the attribute also is encrypted by using KP-ABE. In this case when any user wish to acquire the data from the database which is on the cloud server, the complex query with the complicated functions which are in the form of AND and OR gate can be used.

This gives the user the better encryption of the data. KMA provides the key-set for multiuser searches but these multi-users should have the same access rights. By representing queries as a tree access policy, this is possible to support any type of query. By encrypting the data with KP-ABE, we allow the database owner to assign different access rights to users. Hence, user is able to read the database field values if it is decrypted and allows reading field names also. But the user is unaware about total number of the fields in the database and their names. We can achieve the encryption by using four algorithms of KP-ABE scheme.

REFERENCES

[1] Ruoyu Wu, Gail-Joon Ahn, Hongxin Hu, Mukesh Singhal. "Information flow control in cloud computing". *IEEE international ljournal*. 2010.
[2] Allison Lewko, Tatsuaki Okamoto, Amit sahai, Brent Waters. "Fully Secure Functional Encryption: Attribute-based Encryption and inner product encryption". 2009.
[3] Sascha Miller, Stefan Katzenbeisser, Claudia Eckert. "Distributed Attribute-based encryption". 2010.
[4] Rohit Ranchal, Bharat Bhargava, Anya Kim, Myong Kang, Lotfi Ben Othmane, Leszek Lilien, Mark Linderman. "Protection of Identity Information in cloud computing without Trusted Third Party". *29th IEEE International Symposiumon Reliable distributed Systems*. 2010.
[5] Cristina Basescu, Catalin Leordeanu, Alexandra Carpen-Amarie, Gabriel Antoniu. "Managing Data Accesss on clouds: A generic Framework for enforcing security policies". *International conference on advanced Information Networking And Applications*. 2011.
[6] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijing Huang, and Shanbiao Wang. "Towards Temporal Access control in cloud computing". *The 31st annual IEEE International conference on computer communications*. 2012.
[7] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. "Achieving secure, scalable, and fine-grained data access control in cloud computing". *IEEE INFOCOM*. 2010.
[8] Gail-Joon Ahn, Hongxin Hu, Joohyung Lee and Yunsong Meng. "Representing and Reasoning about Web Access Control Policies". *34th annual IEEE computer software and Application Conference.*
[9] Changji Wang, Guangzhou, China Yang Liu. "A Secure and Efficient Key-Policy Attribute Based Key Encryption Scheme". *Information Science and Engineering international conference*. 2009.
[10] Bethencourt J, Pittabusburgh PA Sahai A, Waters B. "Cipher text Policy-Attribute Based Encryption". *Security and Privacy*. 2007.