ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(42), DOI: 10.17485/ijst/2016/v9i42/90536, November 2016* ISSN (Online) : 0974-5645

A Review on Access Control Issues in EHealth Application in Cloud Computing

R. Charanya[1*] , M. Aramudhan[2] and Ra. K. Saravananaguru[1]

[1]VIT University, Vellore - 632014, Tamil Nadu, India; charanyame@gmail.com, saravanank@vit.ac.in
[2]PKIET, Karaikal - 609603, Pondicherry, India; aranagai@yahoo.co.in

Abstract

Personal Health information is highly confidential. The Main objective is to find out the techniques to protect the health care data from unauthorized user in cloud. Due to privacy concern the personal data are need to be protected from third party and also from unauthorized user. In existing work they used cryptographic techniques like KP-ABE, Attribute based encryption, CP-ABE, etc. This paper addresses the challenges in each access control techniques, and its pros and cons. Future work is to overcome the challenges in existing techniques by using Keyless signature algorithm by using hash function.

Keywords: Access Control Models, Encryption Techniques

1. Introduction

Cloud computing is booming techniques, which enables on flexible, on demand service on computing resources. It relieve from organization burden to invest and manage the own IT infrastructure. Individuals can also use the cloud services to reposit the large volume of information in cloud[1]. For the financial benefit, untrusted server use the data, it lead to huge loss for the data owner. In December2010, Microsoft stored the data in BPOS, that has been gathered by unauthorized user[2]. This is the first major data lose happened in Microsoft. Access control and data security are one of the main security problem in cloud. The users stored the sensitive data like health information, in the cloud servers. All medical data's are stored electronically, so people can easily get the medical services at anytime and anywhere.

Its one of the important techniques to secure the data from network and also it allow authorized user to access the resources based on the privileges. Its mainly concentrate on security of the confidential information, and also provide most important basic security mechanism in the computer system. Personal health record is confidential information, only authorized user can able to access the data.

Access control model is mainly divide into three types, i.e., Discretionary Access Control model (DAC), Role Based Access Control Model (RBAC) and Mandatory Access Control (MAC).The following discussion describe about pros and cons of each models. Here it's divided into three domain namely subject, action and object. The entities are called as Subject, which make request to take resources on the object. The object means resources a subject to access. Action means activity performed by the subject.

2. Existing Models

Its one of the popular techniques to secure the data from network and also it allow authorized user to access the resources based on the privileges. It's mainly concentrate on security of the confidential information, and also provide most important basic security mechanism in the computer system. Personal health record is confidential information, only authorized user can able to access the data.

* *Author for correspondence*

2.1 Classification of Access Control Models

2.1.1 Discretionary Access Control (DAC)

Patient can pass the permission to other users to access the data, access control is done by a centralized authorities. Based on the identity of the User (Doctor, nurse, research dean, etc.,) access control is enforced. In this techniques each resources is associated with set of users, only particular user are authorized to performed action on the object. If user requested data matched with the access list then request permission granted else not. For example: Each doctor have unique id, based on that they are allowed to access the patient data. All doctor cannot access the patient file, if doctor request matched with access list then he can access the patient data. Advantage are 1. Easy to implement 2. No Technical Infrastructure needed. Disadvantage are 1. If access request is initiated then ACL of each resources must be checked.

2.1.2 Mandatory Access Control (MAC)

It's restricted to access by central authority. Administrators have control to access the data by means of two security labels such as sensitivity levels and category[3]. Sensitivity levels are classified into public, confidential, sensitive, top secret, secret and so on. The category indicates the organization or area. Example army, military, commercial systems, research and so on. If user tries to access the resources, in each attempt administrator check the two secure labels, if it condition satisfies then access permission is granted. Main advantage is single location Administration and disadvantage is 1. Central location fail, then couldn't access the resources. 2. Overhead has occurred.

2.1.3 Role based Access Control (RBAC)

The access permission is accepted or rejected based on the user role. The user must be the members in more than one group. The users have different role and responsibility in each group. Depends on role and privileges they are allowed to read the information. For example in E-health system, Patient has full control to access the file. Doctor he is working in more than one hospital, in one hospital he is doctor and in another he may be a research dean. Same person have different role in different hospital. So depends on role, access permission is granted. The Advantage of RBAC is 1. Scalable 2. Minimum cost 3. User is a member in more than one group. Disadvantage is 1. Distinguish each individual in group is unmanageable.

2.1.4 Attribute based Access Control (ABAC)

It's proposed by A. Sahai and B. Waters. Access control means it allows the user to read the information, if the conditions are satisfied. Attribute based access control is a fine grained access control mechanism[4]. Attribute based access control is not only used for access control but also it's used for hiding the information from the unauthorized user. Patient encrypts the personal data with set of attributes and stores the encrypted information in the cloud. In this techniques the user (doctor, nurse, etc) can access the personal data or any data if and only if attributes satisfies the access policy[5]. The attributes are given by the user and trusted authority issues the private key. If attributes are matched then user can decrypt the data.

3. Existing Solutions

3.1 Identity based Encryption

Identity based scheme is like mail system, If I know someone name and id, then I can send message to the particular person, that will be read only by that person[6]. When come to cryptographic concepts, ram want to send message to Sam, he sign it with secret key with his smart card, Ram encrypt the message with Sams name and Sams network address and send it to Sam. While decryption the message using secret key, then Sam verifies the signature by using sender's name and address as a verification key. In health system if doctor knows his patient id then automatically he can view the particular patient details.

3.2 Role based Access Control Encryption

The Data owner encrypt the information, depends on the role the user can decrypt the information. Role based scheme deals with role hierarchies, where each role inherits his role permission from other role. In RBAC model, each user are assigned with set of roles, roles are mapped to access permission[7]. Based on the roles the access privileges are given. It provides flexible control management system to user so it's used in many systems. The data owner encrypted his personal data and stored in the cloud, now user can access the data from then on, no need to re-encrypt the data. The user leaving the group,

then he/she is not authorized to see the encrypted data. Encryption and decryption time are adequate in client side but decryption time at the cloud can be reduced.

3.3 Attribute based Encryption

It allows users to encrypt and decrypt messages based on attributes and access structures[19]. Using Attribute based encryption technique we can achieve scalable and fine grained access control for PHR file. In this technique divide the user into different security domain that reduces the key management complexity for patients and users[8]. Under emergency scenario dynamic change of access polices or file attributes, support on demand[9] User/ attribute revocation. Still some drawback of ABE and MA-ABE in PHR systems. For Example Scenarios like work flow based access control, access rights based on identity rather than attributes. So ABE technique is not efficient. In MA-ABE also have limitation it support only conjunctive policy across multiple AAs.

There are two types of attribute based encryption called as Key-Policy Attribute based encryption (KP-ABE) and Ciphertext Policy Attributes based Encryption (CP-ABE).

3.4 Key-Policy Attribute based Encryption

The patient encrypted the file and stored in cloud, the ciphertext is joined with set of attributes and private key which is given by trusted authority and is joined with access structure like a tree, which describe user identity. For eg., in health record system, personal information are stored in the cloud and encrypt with set of attributes such as, {Doctor, Pharmasist, Nurse, Research Dean, ABC Hospital Centers, Mangers, ABC Hospital}. For each person the access policy is different. Ram is a doctor in ABC hospital, so the access policy is {Doctor ^ABC Hospital}. Sam is a doctor in ABC hospital and also he is a is a research dean in ABC Health center, so the access policy for Sam is {Doctor ^ABC Hospital} OR {Research Dean ^ABC Health Center}[10] . All the information is not visible to everyone, depends on role datas will be visible. In Decryption process, the user decrypt the ciphertext if private key is satisfied by the attribute in the ciphertext. Main disadvantage is data owner have limited control over who can decrypt the data. When re-encryption occurs, the private keys need to be re-issued to all the users, so as to gain access to the re-encrypted files, this creates problem in implemention.

3.5 Ciphertext Policy Attribute based Encryption

The user is described with set of attribute and private key is given by authority[11]. The user credential is described by attributes, and encryptor specifies the policy based on that that can decrypt the data. The data owner encrypts the data before transfer the file in cloud. The data owner associates the access policy with the ciphertext. During decryption if the attribute of a user satisfy the access policy of the ciphertext, then the user can decrypt the ciphertext[12].

3.6 HASBE: A Hierarchical Attribute Set-based Encryption

Hierarchical attribute set based encryption is extension of CP-ABE with hierarchical structure of users. This scheme support inherits flexibility and fine-grained access control in compound attributes of ASBE. It consists of trusted authority, multiple domain authorities, data owners and data users. The root master key and system parameter are generated and distributed by trusted authority. Domain authority is answerable for distributing key to next level users. Key structure is assigned with each user and attributes are joined with user's decryption key. Main advantage of this techniques, it support compound attribute, efficient user abrogation because of multiple value assignment of attributes[13].

3.7 Capability based Cryptographic Data Access Control

Heavy computational overhead is the major problem in existing cryptographic technique on both data owner and as well as CSP. Diffie-Hellman key exchange protocol is used by both CSP and user confidentially share a symmetric key for secure data access. The system composed of owner, user and CSP[14]. Only registered user can access the file in cloud. The new user send registration request to data owner. When owner comes to online the new user registration request is approved and sends the updated capability list to cloud service provider. Now user send file request to CSP, capability list is updated by CSP and sends a acknowledgement to user. Here double encryption is performed. Data owner send data file and capability list to the CSP. Now the encrypted file is unable to read by the CSP because symmetric key available between data owner and user. The main advantage is Data

owner securely outsource the file to cloud. Drawback behind in this scheme is computation overhead to cloud.

3.8 A Task-Attribute based Workflow Access Control Model

Task-attribute- based data entry control model achieves system security, flexibility and versatility. It's a combination of tasks based data entry control and attribute based access control model. In this technique task and attributes are the main concept of task attributes based access control. The basic idea behind in this task described by attributes, attributes is associated by task, task is joined with privileges, and privileges are joined with task. The relationship between task and attributes, status and task, privileges and status are described by two dimensional matrix. Data access security is improved by using this techniques[15].

3.9 Multi-authority Cloud Authority

In main problem in existing CP-ABE Schemes is attribute abrogation. In revocable data entry control for Multi-authority Cloud Storage systems, where each authorities issue attribute individually The attribute abrogation method support both forward security and backward security[2,16]. The Certificate authority is a global authority; it accepts all users and AAs in the system. CA generate public key for the user and assign global unique user identity to it. According to user roles or identity, entitling and revoking user attributes is done by attribute authority. The public key and secret key for each user attribute is generated by each attribute authority. Main advantage is it supports efficient attribute revocation using abrogation multi-authority CP-ABE scheme.

3.10 SPoC: Protecting Patient Privacy for E-Health Services in the Cloud

Single point of contact provides functionality like secure login privileges for E-health system. It mainly protects patient data in e-health application by providing proper secure authentication and authorisation[17]. It Provide secure path between E-health service and clients. SPoC mainly support authentication and authorization. It plays different role in different situation. It's able to issue Security tokens and authenticate internal users and approve the attributes that the user has. SpoC provide information about external user who don't have account in local domain.

3.11 MTBAC: A Mutual Trust based Access Control Model in Cloud computing

In this approach trust computation is introduced into access control model. Here trust is enhanced between user and cloud service through trust mechanism. This techniques control the uncertainty and vulnerability risks caused by authorization. The trust calculation is performed based on trust degree and user role information. Confidentiality, Integrity and Reputation are the three main trust attributes[18]. The commonly used parameter to obtain user behaviour in cloud such as service availability, application vulnerability, and user access frequency, time, unauthorized operation, environmental conditions and resource utilization rate. Operation like success rate, mean time to failure self-protection capability and error repair rate. It provides secure communication between user and cloud service.

3.12 DAC-MAC

CP-ABE is effective technique to encrypt data. In multiauthority cloud storage system, user may get the attributes from multiple authorities. In existing CP-ABE scheme cannot be used to construct the access control. In data access control for multi-authority cloud storage (DAC-MACS) scheme[16,20]. Here they proposed efficient token based decryption method and effective immediate attribute revocation using DAC- MACS scheme.

3.13 A Trust based Context Aware Access Control Model for Web-Services

In this approach secure access control incorporates context aware models and reliance on capability based access control scheme. This is trust enhanced version which support XML-based role based access control framework[21].

4. Conclusion

Access control security issues are one of the major problems in cloud[22]. Good access control model secure the important information from unauthorized user.

Access control security is very important in Ehealth system. Patient wants to protect the health information from unauthorized user. In this paper we discussed about the survey on access control security issues in cloud computing. The existing solutions are identity based encryption. Role based encryption, hierarchical attributes based encryption, and attribute based encryption. Task attribute based access control and trust based context aware access control. Still the existing solutions are not efficient to trust the cloud service provider. Future plan is to use keyless signature using hash function to protect the health care data.

5. References

1. Mohan K, Aramudhan M. Ontology based access control model for healthcare system in cloud computing. Indian Journal of Science and Technology. 2015 May; 8(S9). DOI: 10.17485/ijst/2015/v8iS9/53617.
2. Yang K, Jia X. Expressive, efficient, and revocable data access control for multi-authority cloud storage. IEEE Transactions on Parallel and Distributed Systems. 2014; 25(7):1735–44.
3. Samaratil P, Vimercat SDCD. Access control: Policies, models, and mechanisms. ACM Computing Survey. 2002; 2171:137–96.
4. Hur J. Improving security and efficiency in attribute-based data sharing. IEEE Transactions on Knowledge and Data Engineering. 2013; 25(10):2271–82.
5. Hur J, Noh DK. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems. 2011; 22(7):1214–21.
6. Shamir A. Identity-based cryptosystems and signature schemes. Berlln Heldelberg: Spnnger-Verlag; 1985. p. 47–53.
7. Zhou L, Varadharajan V, Hitchens M. Achieving secure role-based access control on encrypted data in cloud storage. IEEE Transactions on Information Forensics and Security. 2013; 8(12):2381–95.
8. Suhendra V. A survey on access control deployment. Germany: Springer-Verlag; 2011. p. 11–20.
9. Li M, Yu S, Zheng Y, Ren K, Lou WL. Scalable and secure sharing of personal records in cloud computing using attribute based encryption. IEEE Transactions on Parallel and Distributed Systems. 2013; 24(1):131–43.
10. Han J, Susilo W, Mu Y, Yan J. Privacy-preserving decentralized key-policy attribute based encryption. IEEE Transactions on Parallel and Distributed Systems. 2012; 23(11):2150–62.
11. Microsoft cloud data breach heralds things to come. PC World. Available from: http://www.pcworld.com/article/214775/microsoft_cloud_data_breach_sign_of_future.html
12. Zhou Z, Huang D, Wang Z. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption. IEEE Transactions on Computers. 2015; 64(1):126–38.
13. Wan Z, Liu J, Robert H, Deng D. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Transactions on Information Forensics and Security. 2012; 7(2):743–54.
14. Hota C, Sanka S, Rajarajan M, Srijith K, Nair N. Capability-based cryptographic data access control in cloud computing. Int J Advanced Networking and Applications. 2011; 3(3):1152–61.
15. Yi L, Kel X, Junde S. A task-attribute-based workflow access control model. IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing; china. 2013. p. 1330–4.
16. Yang K, Jia X, Ren KK, Zhang B, Xie R. DAC-MACS, effective data access control for multiauthority cloud storage systems. IEEE Transactions on Information Forensics and Security. 2013; 8(1):1790–801.
17. Fan L, Lo O, Buchanan W, Thummler EEC, Uthmani O, Lawson A, Sharif T, Sheridan C. SPoC: protecting patient privacy for e-health services in the cloud; UK. 2012. p. 1–7.
18. Guoyuan L, Danru W, Yuyu B, Min L. MTBAC, a mutual trust based access control model in cloud computing. China Communication. 2014; 29(2):154–62.
19. Hur J, Noh DK. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems. 2011; 22(7):1214–21.
20. Anbarasan P, Hariharan K, Parameshwaran R. Design of gain enhanced and power efficient Op- Amp for ADC/DAC and medical applications. Indian Journal of Science and Technology. 2016 Aug; 9(29). DOI: 10.17485/ijst/2016/v9i29/90885.
21. Bhatti R, Bertino E, Ghafoor A. A trust-based context-aware access control model for web-services. Proceedings of the IEEE International Conference on Web Services ICWS; 2005. p. 83–105.
22. Charanya R, Aramudhan M, Mohan K, Nithya S. Levels of security issues in cloud computing. International Journal of Engineering and Technology. 2013; 5(2):1912–20.