A Survey on Access Control in Cloud Computing

Yogita Borse[#1], Anushka Chawathe[*2]
[#]Assistant professor, *PG student, Department of Information Technology, K. J. Somaiya College of Engineering, Mumbai, India

Abstract

Cloud Computing is one of the most widely attributed technology. As cloud providers and clients increased in the market, the amount of data also increased. To have a generalised mechanism for accessing this data while making sure there is enough security maintained is the major concern of the service provider. For the purpose of providing services on cloud, there is an access control mechanism. The services made available by the cloud provider are accessed using this mechanism. In this paper, detailed comparison of the access control mechanisms have been discussed.

Keywords

Access control, cloud computing, access control mechanisms, cloud data security.

I. INTRODUCTION

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to public utility. The issues related to data generated by cloud are loss of transparency and control over the data and lack of trust and dependence on cloud provider.

Cloud environment is not static and evolves as more and more clients enter the system. It becomes difficult to manage all these clients. Cloud clients are unaware of their data such as its storage and retrieval. Also the cloud client has trust issues as far as data is concerned. The service provider of cloud thus brings an access control mechanism to ensure the secure handling of data. Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment. Cloud environment has the challenge of access control as it is very scalable and elastic. Following are certain types of access control models which have been discussed as seen in paper [1].

A. Identity-based access control

Identity based access control models like attribute-based, role-based, discretionary access control, mandatory access control are not sufficient to apply directly for cloud environment and so needs to modify before consider for cloud access control.

Disadvantages -

- Any modification or changes made to the resources provided by the cloud service provider in real-time or changes in accessing entities may result in disruption of data integrity.
- There arises the problem of seeking permission from different domains for gaining access. The cloud environment is such that the access-requesting entity may not be known to the access-granting entity. Due to this purpose, identity based access control may not be possible. This is because the identity of the access-requester needs to be known beforehand by the access-granter.
- An authentication of the access-requester needs to be done before availing the services on cloud. This may create a problem of delegation. The resources and their administrators are distributed and so authorization is required to interact with them.

B. *Role-based Access Control(RBAC)*

This model focuses on the functional roles of the user rather than their identity to grant privileges.

Disadvantages - There are minimum number of privileges assigned for every role enhancing security. But, this may result in multiple roles per user. There have been various models proposed to address this limitation such as:

1) Team-based access control

This approach is applied for multiple organizations which collaborate to perform certain task. A team of users with their individual roles makes a better way of accessing resources or entities. There two major contexts assigned which are that of user and objects. User context is the used to identify specific roles assigned to a user within a team.

2) ***Group-oriented Access Control***

It is also called the YGuard model. There is a group which has same privileges assigned to all its members.

3) ***Temporal RBAC***

In this model, the roles may be enabled or disabled based on temporal constraints.

4) ***Location-based RBAC***

The roles are assigned to users based on their geographic location in an organization.

5) ***Spatio-temporal RBAC***

There are spatial and temporal constraints which need to be satisfied.

C. Attribute-based Access Control(ABAC)

In this model, the characteristics of the access requester are used to make an access decision.

Advantages-

- This overcomes the problem of not knowing the identity of the access requester or client. A predetermined set of credentials are required to grant access.
- The rights, responsibilities, qualifications are the general characteristics required in this model.
- To regulate access decisions over the internet, a framework has been proposed. Instead of using a certificate for this purpose, a language is used by the access granter(service provider).
- The requirements to grant access and communicate securely require certain access policies to be defined. There is a policy filtering mechanism used in this framework. The proof carrying authorization is distributed across hosts keeping policies hidden from unauthorized users. A scheme called cryptographic access control is used to protect privacy. This model is scalable in large enterprises and cross-domain or federated situations.

Disadvantages- An attribute may not be required by the access requester to be bound to certain roles or behaviours. This could cause the misuse of access privileges. The model is not dependent on the behavioural characteristics of the client.

D. Risk-Adaptable Access Control(RAAC)

There is a degree of risk and uncertainty associated with making access control decisions.

Disadvantages- However, this model is still in the nascent stages. As a risk model is difficult to create, hypothetically there is no delegation of access control.

E. Trust-based Access Control(TBAC)

Multiple levels of trust is another approach to solve the issues related to the elastic and highly scalable cloud environment. The trust to access privileges is given based on the level of the client.

Disadvantages- This indirectly depend upon the contextual information. Based on the client's trust level, users can assign privileges once a role invoked.

F. Rule-based Access Control

The scripted policy rules are used to make access decisions. The resources which require access control have these rules attached to them.

Disadvantages-For the implementation of these rules, there is no formal model, structure or language. The number of rules assigned increases dynamically as the complexity of the system increases. It becomes difficult to understand if there are any conflicts among these rules. This model may be used to implement dynamic policies. A combination of this model with other compatible models might be a better solution to provide security.

II. LITERATURE SURVEY

The data that is generated by the services provided by cloud has many security issues. The major issue is due to the abstract nature of the cloud architecture. The cloud services are being outsourced for data storage and processing. As there is no way to determine where the data is stored and how it is processed, it poses a threat. If there are more than one organization that are clients of the cloud service provider, any competing organization can wrongfully gain access to data of the victim client. This leads to trust issues for cloud services. Also, there is no proof for the client if there is some incident or problem. These are some of the issues related to cloud services as seen in [2]. Thus, access control needs to be implemented for greater security threat of data breaches.

There are various comparison-based constraints for data access in cloud as seen in [3]. This works on an Attribute-based Encryption mechanism. The attributes describing an outsourced data are used to define access policies. Only the authorized users can decrypt this data. The policies become an inherent part of the data. However, there is no systematic mechanism for constructing a fine-grained access control in cloud. For this particular mechanism, an integer comparison like the Bitwise-comparison operators and AND/OR operators is used. There are certain shortcomings associated with this mechanism. Firstly, there is no support for dual comparative expressions. The range-based comparative constraints are embedded into outsourced files and user's private key. There is no support for efficient cryptographic comparison methods. The Bitwise-comparison has a user key of a large size as the integer must be split into bits. There is a large overhead of running those algorithms due to sophisticated bilinear pairing operations. The

solution to these problems is to construct two new cryptographic functions which are forward and backward deviation functions. A key delegation and dual decryption structure for a cryptosystem will be constructed. This will reduce the computational overheads on lightweight devices. Thus, the majority of decryption operations will be shifted on cloud servers. In paper [3], this structure is proved to be secure against various chosen derivation-key attacks.

The current access control mechanisms rely on trusted host. These are used to mediate access and maintain policies. Traditional models do not support dual comparative expressions (DTE). As these traditional systems do not support current time, a temporal access control is required as seen from [4]. Temporal access control encryption scheme has certain temporal attributes e.g., period-of-validity, opening hours, or hours of service. A license is assigned to each user using certain comparative attributes with many privileges. For the purpose of enforcing valid matches between access policies and user's privileges, a proxy-based re-encryption mechanism. The current time is taken into consideration while implementing this mechanism. This model has many benefits such as flexibility, supervisory and privacy protection, constant size of ciphertext, private-key, depth of policy-tree and nearly linear-time complexity. Even the forward and backward derivation functions are provided.

A new hybrid access control model has been proposed in paper [5]. The computation of risk is combined with access control. The model for access control is attribute-based. The value which is submitted is the attribute. The authority in the organization will then verify this value and give the public key. The user may encrypt his data and store on remote servers. The data can be accessed using public and private keys. This the dynamic attribute-based risk aware access control technique.

In paper [6], the access model for the Personal Health Record(PHR) is discussed. Attribute Authority(AA) is the trusted third party which issues the private keys for medical staff. An assumption about the cloud servers being honest but curious has been made. There might be an issue related to concurrent access. The communication channel through which data is access is considered to be insecure.

The cross-domain access control policy is provided for evaluation of trust in paper[7]. Environment attributes of entities and behaviour are used to generate authorization policies. The credibility evaluation model is implemented. A classification association rule is used for attribute, attribute behaviour, environment and entity to be extracted. An access control policy is defined. This general policy is later integrated into trust management system.

In paper [8], some common concepts such as; secure decryption outsourcing, audibility of decryption, limited and anonymous fine-grained access control and key-leakage resistance have been discussed.

After studying all these papers a comparative study of all these models have been conducted.

III. COMPARATIVE STUDY

As there are two main parts of access control in the form of Authentication and Authorization, the table I gives the first observation in terms of which part is focused in which paper.

If Authentication is the one which is focused, then table II shows the observations in terms of how it is been implemented and security mechanisms used. Whereas if the Authorization is focused the as per table III all solutions are based on authorization through trusted third party.

TABLE I: IDENTIFYING THE ACCESS CONTROL MODEL CONSISTING OF A BASE STRATEGY FOR SECURE ACCESS CONTROL

Paper	Access Control Strategy	
	Authentication	Authorization
2	√	×
3	×	√
4	√	×
5	×	√
6	√	×
7	×	√

TABLE III: IF AUTHENTICATION IS THE BASE STRATEGY FOR ACCESS CONTROL

Paper	Is any key provided to the user	Is communication secure	Encryption Techniques if used	Is any trusted host used
2	Yes	No	CBE Encryption	Yes
4	Yes	Yes	ABE Encryption	No
6	No	No	No	Yes

TABLE IIIII: IF AUTHORIZATION IS THE BASE STRATEGY FOR ACCESS CONTROL

Paper	Is third party based authorization
3	√
5	√
7	×

IV. CONCLUSIONS

An access control policy needs to be implemented which will decrease the risk of an attack such as escalated privileges. For this purpose, an access control mechanism which provides security to the owned data stored on cloud is required. A survey on some of the important access control mechanisms have been carried out. It primarily aims to understand the basic concepts and advantages of these models. After conducting the survey, a unified strategy was chalked out which emphasizes whether authentication or authorization was the basic step to gain access. Certain parameters were compared if the condition was satisfied. Based on these conditions, a model which provides keys for encryption through a secured channel for communication is inferred to be the best. This model should have a trusted host and require a third party for authorization. It could be inferred that such model if created may provide better security.

REFERENCES

[1] Ray I., Ray I. (2014) Trust-Based Access Control for Secure Cloud Computing. In: Han K., Choi BY., Song S. (eds) High Performance Cloud Auditing and Applications. Springer, New York, NY.

[2] Charanya, R., Aramudhan, M.: Survey on access control issues in cloud computing. In: IEEE International Conference on Emerging Trends in Engineering, Technology and Science, pp. 1–4. IEEE (2016)

[3] Y. Zhu, H. Hu, G.-J. Ahn, M. Yu, and H. Zhao, "Comparison-based encryption for fine-grained access control in clouds," in CODASPY, ACM, 2012

[4] Y. Zhu, H. Hu, G. J. Ahn, D. Huang and S. Wang, "Towards temporal access control in cloud computing," *2012 Proceedings IEEE INFOCOM*, Orlando, FL, 2012, pp.2576-2580.

[5] R. Aluvalu and L. Muddana, "A dynamic attribute-based risk aware access control model (DA-RAAC) for cloud computing," *2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Chennai, 2016, pp. 1-5.

[6] W. Li, W. Ni, D. Liu, R. P. Liu, P. Wang and S. Luo, "Fine-Grained Access Control for Personal Health Records in Cloud Computing," *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Sydney, NSW, 2017, pp. 1-5.

[7] H. Xia, "Design and implementation of trust — based access control system for cloud computing," *2017 IEEE 3rd Information Technology and Mechatronics Engineering Conference (ITOEC)*, Chongqing, 2017, pp. 922-926.

[8] M. Ed-Daibouni, A. Lebbat, S. Tallal and H. Medromi, "A formal specification approach of Privacy-aware Attribute Based Access Control (Pa-ABAC) model for cloud computing," *2016 Third International Conference on Systems of Collaboration (SysCo)*, Casablanca, 2016, pp. 1-5.

[9] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma and L. Wei, "Auditable $sigma $ -Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 94-105, Jan. 2018.