ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse370942020.pdf
https://doi.org/10.30534/ijatcse/2020/370942020

Secure Scalable Attribute Based Access Control (SS-ABAC) in Cloud Environment

Rudragoud Patil[1], R. H. Goudar[2]
[1]Department of CSE, Gogte Institute of Technology, VTU-RRC, Belagavi, (Karnataka), INDIA, rspatil@git.edu
[2] Dept. of CSE, VTU, Belagavi, (Karnataka), INDIA, rhgoudar.vtu@gmail.com

ABSTRACT

In cloud computing environment access policies will define certain restrictions on the behavior of cloud users which are part of the cloud ecosystem. With rapid development in recent technologies like cloud computing, Internet of things, grid computing many cooperating processes which are belonging to different enterprises need to exchange their data as well as services. So in this regard, security and privacy are the major concerns in developing such communications. We need to develop appropriate secured access policies to keep user data safe which is there on the cloud server. This paper implements access control model based on cloud user attributes and roles. SS-ABAC (Secured Scalable Attribute Based Access Control) is proposed where to access or to perform operations on the object is based on roles and attributes of the subject entity as well as environmental condition and simulation of experimental result shows that our model will reduce unauthorized access to cloud data and also minimizes access to services hosted by the cloud service provider.
.

Key words: SS-ABAC, data privacy, and security, roles, attributes, subject, object, environment condition.

1 INTRODUCTION

In recent years cloud computing technology gas gained more popularity and ease of using cloud services has made customers happier. This technology hosts storage, software, platform, etc like many various types of services and these are used by many customers pay-as-you-go method on demand. However it also brings more concerns like user authorization, access policies, security, privacy, multitenancy. Once user data is outsourced to cloud service providers, the privacy of user data cannot be guaranteed due to curious learners in the domain of cloud service providers. The cloud services delivery models are classified into three categories.

Software as a Service: A cloud service provider offers approved licensed software to the end customers on demand. Here customers don't have any control over the software but only run the software in his machine. Multitenancy concept is used when delivering services to customers using virtualization. Overall the end customers don't have any burden of purchasing, maintaining and updating the software whenever it is required. The best example of SaaS is Google docs.

Platform as a Service: In this end users have more control and management of all the resources provided at the system level by the cloud service provider. The resources like applications, operating systems are maintained by CSP at the hardware level. CPU, Network and memory are allocated to users based on the needs. Google Cloud Platform is an example of PaaS.

Infrastructure as a Service: A user rents software infrastructures where different hardware facilities such as CPU, Storage, Networking capabilities are provided as services to users. Based on customer needs services can be scaled. Google Storage, Amazon S3 are examples of IaaS.
The various cloud services are deployed in Private, Public, Hybrid, Community deployment models.

In such an environment where already existing cloud users and cloud service providers first both should come to an agreement with respect to SLA (Service Level Agreement) and QoS (Quality of Services).But still, there can be some violations of rules which are made during agreement. In such a scenario a proper access control methods should be framed to protect the privacy of user data. Nowadays, in cloud environment communication of data and services between user and service providers on demand has created a dynamic ecosystem. This said process involves the number of stakeholders such as cloud users and cloud service providers. Before using any services from CSP users should a) Select appropriate service provider. b) Have a service level agreement for future monitoring.

In cloud computing access control mechanisms are divided into the following categories.

1.1 Discretionary Access Control

In Discretionary access control, each user in a system has control over their own data. In DAC, each resource object has an ACL (Access Control List) associated with it as shown in Table 1. It contains a list of users and groups who are authorized to access the objects and also certain security levels are defined for certain groups. Let User set is represented as U, set of all objects are represented as O and set of all possible permissions are denoted as P. So the policy of form

$$f: U \times O \rightarrow P$$

a function f(U, O) decides the list of allowable permissions on object O by Users U. The following table gives an example of ACL policies. (Where P1-Read, P2-Write, P3-Delete)

Table 1: Sample List of ACL

Users/Objects	O1	O2	O3
U1	P3, P1	P1	P1
U2	---	P2	P1,P2,P3
U3	P1	P3	P3,P2

1.1 Mandatory Access Control

In cloud computing access security, mandatory access control gives the most suitable defined type of access control mechanisms, where the operating system has controls all the resources of a system. The MAC models are generally suitable for a multi-cloud system where the entire responsibility of granting access permission lies with the system administrator. Here in practice, we refer people or machines and files or directories for subjects and objects respectively. All objects and subjects are defined with some attributes and roles. Whenever any subject tries to perform operations on an object, an access rule is examined by the operating system against attributes of both subject and objects and decision is taken whether to grant permission to access the object. MAC is also suitable to DBMS where objects are tables, views, procedures etc. In MAC based on the levels of security objects are categorized into Top secret, Secret, Classified, and Unclassified. Bell LaPadula that recommends the "no-write-down" and "no-read-up" rules, where write operation indicates data flowing from subject to object and read operation indicates data flowing from object to subject respectively for data access to maintain confidentiality.

1.2 Role-Based Access Control

Role based access control is developed because most of the sensitive data is owned by the organization not by the users and to allow the user to access the data is done based on the user roles are. This is the best method to restrict access. The organization not necessarily authorize and revoke the access for an individual person one at a time, they can do it based role assigned. Here even multiple roles can be assigned to a single person based on the organization requirement. Although RBAC is used by many companies nowadays, we cannot assign any role to the user before he joins the company based on certain parameters. As the access permissions are assigned to user roles not to the objects and operations. So we can restrict access to actions but not to data. In this way, a role represents an intermediate layer between subjects and permissions and as the complexity of policy specification and administration is reduced, it brings scalability. When a person joins or leaves the program, all that has to be changed is the ties between the user and their associated roles.

1.3 Attribute Based Access Control

NIST define as" It is a method of an access control system in a cloud environment where policies are well defined instead of user roles and whenever any subject (User or Machine) willing to perform any operation on the object (File or Programs) is granted permission only on the basis of well-defined policies which are examined based on attributes of all the entities of a system like subject, object, environment condition". The different components of this access control system are Subject, Object, Attributes, Operation, Policy and Environment conditions will be the components of the system. This is a valid access control model as it takes decisions dynamically by evaluating attributes, rules or policies and environmental conditions each time a request is made. The major components [10] of enterprise ABAC are Enterprise ABAC Policy, Attribute Management, and Access Control Mechanism. The Access Control Mechanism of Enterprise ABAC contains functional points such as Policy Enforcement Point, Policy Decision Point, Policy Information Point and Policy Administration Point.

1.3.1 Attributes

Attributes are the unique features of all the entities of an access control system like subject, object, or environment conditions. Attributes information collected and stored in the form of name-value pair.

1.3.2 Subject

Subjects can be any customer, clients or computer system which gives access permission to apply any operations on objects. One or more attributes are defined or identified for all the subjects of a system. In our implementation user is assumed as subject those are synonymous.

1.3.3 Object

In ABAC cloud system resources that are accessed are managed such as hardware devices, software programs networks, processes. On all these resources access permission can be given based on the access policies defined in the system. Based on the subject entity attributes operation are to be performed.

1.3.4 Operation

Operations are the execution of action on the object based on user requests. Following are few operations like read, write, edit, delete, copy, execute, and modify.

1.3.5 Policy

Based on the need of enterprise, in ABAC set of policies or rules are defined. Access or to perform an operation on any object is given to any subject based on evaluating the policies against attributes values of the subject, object, and environment conditions.

1.3.6 Environment conditions

These are passive entities play a very important role in access management. Environment conditions values are independent of all the remaining components of the system. Possible environment values may be the current time, geographical location of user, date, security level. Table 2 gives advantage and disadvantage of all access methods discussed so far.

Table 2: List of Access Control Models

Access Models	Advantage	Disadvantage
DAC	• Implementation is easy • Scalable & Flexible	• Not Scalable • Possibility of ACL Explosion • Can be some Mistakes
MAC	• Security is more • Scalable	• Rigid Policies • More administration overhead
RBAC	• Scalable • Flexible • Less admin overhead	• Roles need to be maintained • Possibility of roles expansion • Not possible in a real-time scenario
ABAC	• Dynamic and Fine-grained Access control • Scalable • Considers Environmental Condition • Easy administration	• Attributes need maintenance • Possibility of attributes expansion • Difficult for analysis •

2 LITERATURE SURVEY

This section provides a detailed survey on work carried out on attribute-based access control.

In [1] authors have implemented an XML based framework which combines attribute-based control and policy decision system. This provides fine-grained and scalable secure access to the services which are hosted by any cloud service provider. This framework includes a large number of entities and their attributes. This work can be extended to build ABAC architecture for intrusion detection.

In [2] authors used the user's attributes and roles to develop a composite access control model. Existing problems in RBAC can be resolved by this model by simplifying access permissions and policy management.

In [3] they have implemented a fuzzy attribute-based access control scheme, which is best suitable for the existing cloud environment. It is more flexible and having the best time efficiency compared to existing standard ABAC. It uses a fuzzy evaluation of users and objects. This work can be extended to deep learning techniques by using a neural network.

Cloud users and providers have to trust upon each other in such a dynamic cloud ecosystem. [4] Have implemented an efficient and flexible Role-based access control to provide privacy and security of all communication between user and provider. In this scheme, all users are assigned with some roles by using less privilege access rules to operate on any object. This scheme supports both active and passive workflow of the system.

One of the major concerns of the cloud system is authentication and access control to cloud services, especially when it comes to data access. Implementation of MLBAAC [5] gives the best solutions using a double breaker to provide secured access solutions but with some overhead in execution time.

In [6] implemented a new attribute rule ABAC, based on the security level. Users are allowed to access the object based on the attributes and roles. It works based on the evaluation of the attributes of all the entities involved in the cloud system like subject, object and environment condition. It also caters to all the mandatory requirements of an access mechanism.

The role expansion problem is addressed by implementing RABAC [7] without making any changes in the existing RBAC. Here it combines user roles and attributes in a more flexible method. The filtering component is added to RBAC model.

In this [8] authors have included trust as one of the attributes in implementing the ABAC mechanism. To evaluate a degree of trust, previous information and observation of users are used. Based on the outcomes of trust degree access permissions are granted to the user for different objects. An

XACML is used to implement policies of the healthcare domain which is part of this work.

In [9] presents an implementation of ᵠRBAC model by the code generator to access the data which is there on the cloud. This model uses the concept of attributes and roles. This model is having two phases like the testing phase and the transformation phase.

Revocable identity based signatures scheme [11] is proposed in which during updating of all the user keys, different computational workload are transferred to the cloud revocation agency. Security analysis shows that the proposed scheme is not vulnerable to chosen identity attacks.

The scheme [12] implemented using cryptography is more suitable as it uses XOR operation which will reduce less resource. Another system is developed to guarantee security and privacy of the user data stored in the cloud which includes access policy, encryption and decryption algorithms.

The proposed privacy-preserving solution [13] in which encrypting the user health data before outsourcing to the cloud storage and also provided a keyword search scheme to retrieve files from the cloud.

The proposed work [14] implements Curtmola SSE scheme using AES algorithm to perform encryption and decryption of user data. It also gives all implementation module and workflow used to encrypt the data before sending to the cloud servers. This work also enhances the search operation by providing the user to conduct a search operation over the encrypted cloud data. The user does not need to manage the encrypted file name list, as the application maintains a database for each file that the user uploads. The index is dynamically updated each time a user uploads a new file to the cloud server.

3 IMPLEMENTATION OF PROPOSED SCHEME

Our proposed model consists of the following sets of entities: Subject, Object, Environment, Roles and Permission. An attribute-based access control every subject is consisting of attribute-value pair, as well as object, is consisting of an attribute-value pair. Here any access permission policy is identified by a triplet (S, P, O) where any Subject performs Operation on an Object.

An example policy can be represented as follows.

Policy→(S, P, O)→(Sa=Sv ,Op, Oa=Ov)----------(1)

Attributes values can have different types of values as text, numeric, alphanumeric. To evaluate the rule there is a need to use logical and relational operators. A student subject S has age 22 is allowed to view his scorecard Object with id 10.

Policy→(S, P, O)→(Sage <=22 ,View, Oid=10)----------(2)

3.1 Proposed Algorithm

Algorithm: SS-Attribute Based Access Control

Input:$Subject_{attr}$,$Object_{attr}$,Env_{attr}
Output: Permission Granted/Not for Performing Operation

1. Read the request from a user with
   a. Subject attribute, Object attribute, Env attribute
2. PIP checks the attributes in databases along with Environment conditions.
3. Evaluate Access Request (For Operations)

```
If(AG==1)
{
   Fetch the Object
   Return the Object to the Subject
   User will perform the Operation on Object
    goto step 4
}
Else
{
  Send the Exception to the administrator(as
   violation of rules)
}
```

4. Stop the Algorithm

4 RESULTS AND DISCUSSION

To verify our SS-ABAC model for its correctness, we implemented the proposed model in Intel Core i5 CPU, 2.86 GHz with 8GB RAM Memory, and Windows OS. During result analysis, we compared standard ABAC and our proposed model SS-ABAC in the same execution environment.

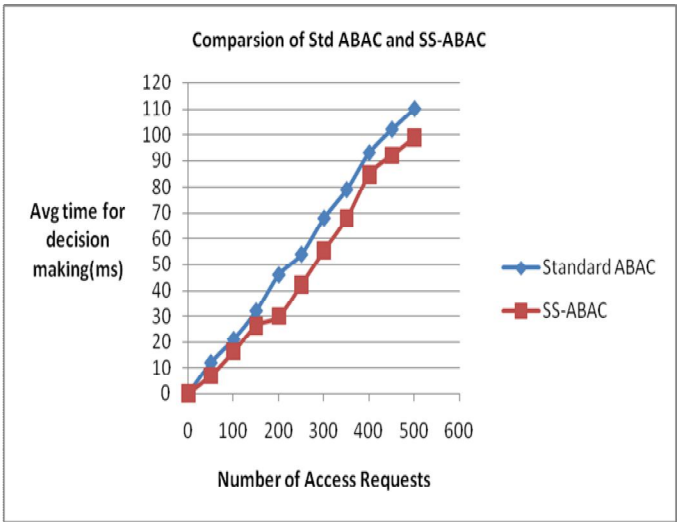

Figure 1: Result analysis

To build a simulation environment, we have used the cloudsim3.0.3 tool. Around 500 policies are designed for object access by the subjects. Randomly access request is made by the number of users and we calculated the time required for decision making for both models. The resulting graph shown in Fig 1 indicates that our proposed model takes less time in decision making without any flaws. So we have more accuracy and better access control mechanism by designing the SS-ABAC model

To build a simulation environment, we have used the cloudsim3.0.3 tool. Around 500 policies are designed for object access by the subjects. Randomly access request is made by the number of users and we calculated the time required for decision making for both models. The resulting graph shown in Fig.1 indicates that our proposed model takes less time in decision making without any flaws. So we have more accuracy and better access control mechanism by designing the SS-ABAC model.

5 CONCLUSION

In this paper, we have designed a new access control mechanism SS-ABAC based on the attributes and roles of users and objects. It also solves the problems which are existing in standard ABAC. The main goal is to write proper access policies so that the time required for decision making on any policies will be reduced. But still, there is scope for improvement by increasing the number of attributes which are belonging to subject, object, environment condition and also designing more complex access policies will make better access control to the resources of the cloud environment.

REFERENCES

1. Vibha Bhardwaj, Sushil Sharma **, "An XML Based Framework For ABAC As A Service Based On Policy Machine Architecture"** International Journal of Computer Sciences and Engineering vol-7,Issue 3,2019. https://doi.org/10.26438/ijcse/v7i3.461469
2. Jing-yu WANG et.al, **"A Composite Access Control Model Based on Attribute and Role"** 2nd International Conference on Computer Science and Technology (CST 2017) ISBN: 978-1-60595-461-5.
3. Yang Xu et.al, **"A Feasible Fuzzy-Extended Attribute-Based Access Control Technique"** HindawiSecurity and Communication Networks Volume 2018, 11 pages. https://doi.org/10.1155/2018/6476315.
4. Shilpi Harnal, R.K. Chauhan **"Efficient and Flexible Role-Based Access Control (EF-RBAC) Mechanism for Cloud"** EAI Endorsed Transactions on Scalable Information Systems, doi: 10.4108/eai.13-7-2018.161438
5. Amit Wadhwa and Vinod Kumar Gupta, **"Proposed Framework with Comparative Analysis of Access Control & Authentication based Security Models Employed over Cloud"**, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017) pp. 15715-15722.
6. Khaled Riad et.al **"AR-ABAC: A New Attribute Based Access Control Model Supporting Attribute-Rules for Cloud Computing",** 2015 IEEE Conference on Collaboration and Internet Computing DOI 10.1109/CIC.2015.38.
7. Jin X., Sandhu R., Krishnan R. (2012) **"RABAC: Role-Centric Attribute-Based Access Control. In: Kotenko I., Skormin V. (eds) Computer Network Security**." MMM-ACNS 2012. Lecture Notes in Computer Science, vol 7531. Springer, Berlin, Heidelberg https://doi.org/10.1007/978-3-642-33704-8_8
8. Abirami G, Revathi Venkataraman, **"Attribute Based Access Control with Trust Calculation (ABAC-T) for Decision Policies of Health Care in Pervasive Environment".** International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-7, May, 2019
9. Ghotbi S.H., Fischer B. (2013) "**Fine-Grained Role- and Attribute-Based Access Control for Web Applications. In: Cordeiro J., Hammoudi S., van Sinderen M. (eds) Software and Data Technologies."** ICSOFT 2012. Communications in Computer and Information Science, vol 411. Springer, Berlin, Heidelberg.
10. V.C. Hu et al. **"Guide to Attribute Based Access Control (ABAC) Definition and Considerations"** NIST Special Publication 800-162, USA, pp.4-14, 2014.
11. Pragya Mishra *et al.*, **"Revocable Identity Based Signature Scheme with Outsourced Cloud Revocation Authority"** International Journal of Advanced Trends in Computer Science and Engineering, 8(4), July- August 2019, 1537 – 1544. https://doi.org/10.30534/ijatcse/2019/76842019
12. Dhanjaya. V *et al.*, **"Design and Analysis of high securityECC based Cryptography by Holomorphic and data storage in Cloud",** International Journal of Advanced Trends in Computer Science and Engineering, 9(2), March - April 2020, 1720 – 1728. https://doi.org/10.30534/ijatcse/2020/124922020
13. S. J. Nadaf and R. Patil, **"Cloud based privacy preserving secure health data storage and retrieval system,"** 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, 2016, pp. 1-6.
14. Rudragoud Patil and R. H. Goudar **"Implementation of User-Centric SSE for Privacy-Preserving and Enhancing Searching Efficiency in Cloud Environment",** International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-10, August 2019. https://doi.org/10.35940/ijitee.J9625.0881019