A Review on a Novel Trust Based Access Control Model for Cloud Environment

Deepak Kumar [1], Rahul Kumar Chawda[2]
[1] Student of 6 th Sem MCA Department , Kalinga University, Raipur
[2] Assistant Professor, Department of Computer Science, Kalinga University, Raipur
rahul.chawda3@gmail.com [2]

Abstract- Cloud computing is a service oriented technology which offers the services (IaaS, PaaS, and SaaS) as a utility over the Internet. Since cloud computing is one of the most popular form of internet application, the resources and services in cloud environment is more vulnerable to security threats and attacks in order to protect the cloud environment from malicious users.

Keyword- Authorization, Access Control, SLA parameter, Cloud Computing

I. INTRODUCTION

Cloud can be broadly classified into two parts: front end and the back end. Client part of the cloud computing system is referred as front end which consists of the applications and interfaces that are needed for accessing cloud computing services, e.g., Web Browser, mobile aopps. Back end part provides different types of services to the user, e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a service (SaaS). Figure 1.1 shows the complete architecture of cloud computing. The architecture is composed of five layers. The first layer is the physical infrastructure which is composed of all hardware resources such as computing, storage, networks. In the second layer, the virtualization technolgy i.e, hypervisor is used to virtualize the cloud resources in order to serve the multiple n users at a time. The infrastructure as a service (IaaS) is the third layer of cloud computing architecture and bottom layer of the service delivery model or service stack. In this layer, the resources such as computing, storage, networks are present in form of image or virtual machine. The platform as a service (PaaS) provides the runtime environment or development tools in which the user can build the application and execute in it. The software as a service (SaaS) is the top most layer of cloud architecture. This layer provides the application or software as a service such as CRM, google docs, game. The cloud user can access all these services through web browser or mobile apps over the Internet.

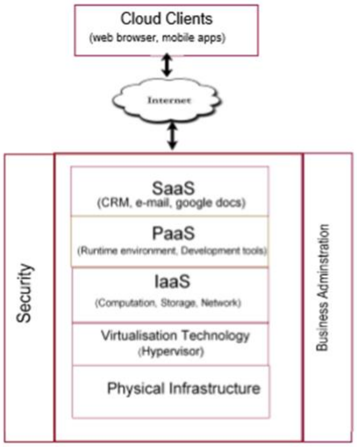
Cloud Clients
(web browser, mobile apps)
Internet
SaaS
(CRM, e-mail, google docs)
PaaS
(Runtime environment, Development tools)
IaaS
(Computation, Storage, Network)
Virtualisation Technology
(Hypervisor)
Physical Infrastructure
Security
Business Adminstration

Figure 1.1: Cloud Architecture

Security Issues and Goals in Cloud Computing

Cloud computing is one of the most popular form of Internet application, which faces a lot of security threats and attacks. There are several vulnerabilities present in the cloud environment by which the attacker and malicious user can get a chance to introduce the attacks. Since cloud computing provides on-demand and scalable services, the environment are highly dynamic. The traditional security mechanism cannot fulfill all the security requirements of cloud computing. There are four security goals of cloud computing:

- Confidentiality
- Integrity
- Availability
- Accountability

We address the different vulnerabilities present in cloud environment and different types of threats and attacks that can be made to violate the above security goals. shows the ecosystem for cloud environment i.e, four security goals and privacy. This ecosystem can be applied to any computer or network systems.

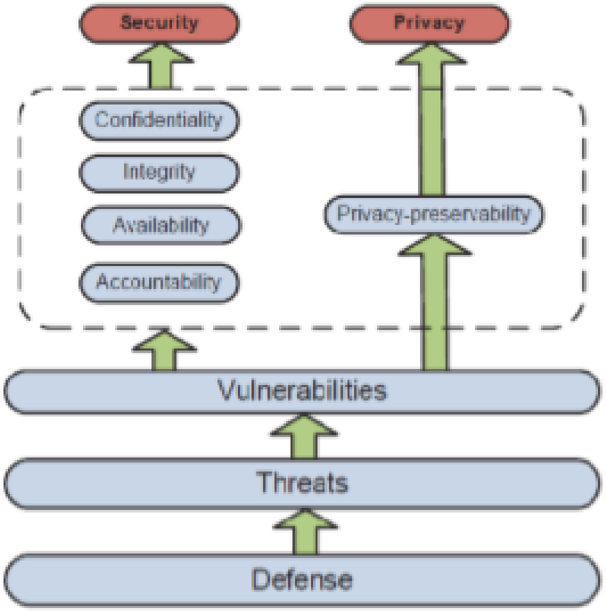

Figure 1.2: Ecosystem of Cloud Security and Survey

II. LITERATURE REVIEW

Abraham Yarn et al. Cloud computing is one of the most popular form of internet application, which faces a lot of security threat and attacks. There are several vulnerabilities present in the cloud environment by which the attacker and malicious user can get chance to introduce the attacks. Since cloud computing provide the on-demand and scalable services, hence the environment is highly dynamic. Therefore, the traditional security mechanism cannot satisfy the security requirements of cloud computing. One of the most fundamental and important key technique that can meet the security requirements in cloud environment is the access control technology

Srikanth Kandula et al. explain the main goal of designing access control model for cloud environment is to protect the users' data and computation, cloud resources by controlling access to the resources and the system itself. Access control model decides which user (subject) has previlege to access the resources (object) and which type of operation can be performed by the user on a particular resource. In cloud computing, access control model takes various actions such as identification, authentication, and authorization before actual accessing the resources. There are two types of access control model which can be applied to traditional Environment and cloud environment.

- Identity based access control modelˆ
- Trust based access control model

Matt Blaze et al. Say that since cloud computing is very popular form of Internet application, the number of users is very large and the user behaviour is always uncertain and dynamic. So, there is more risk of affecting cloud resources. The above model cannot be applied to the cloud environment. Some researcher introduce the concept of trust mechanism and applied this trust mechanism into cloud environment. The trust based access control model takes the user behaviour parameter for access control decision. There are several parameters is to be defined in order to evaluate the trust value. The trust value is evaluated for both users and cloud resources before they interact with each other.

In attribute access control model, the users attribute is considered in order to make access control decisions. The users attribute may be the location, age, data of birth, role or all of them. Amittai Aviram et al.Each attribute take unique and discrete values. This model checks the users attribute against the predefined policy of a particular systems or organisation in order to make allow or deny access. Since there are large number of users in cloud computing, it would be very complex task to decide large number of attributes.

Paul Manuel et al.proposed a trust model based on Quality of Service (QoS) parameter. The objective of this model evaluates the trust value intrems of Qos requirements such as reliability, availability, turnaround time, and data integrity. This model also explains how the resource is selected for the user base on trust and its capabilities.

David F Ferraiolo et al. in cloud computing, the number of user access to cloud service is huge. If any user performs any malicious activity or introducing any attack to the cloud server, then the resources will affected. As a result, the performance of cloud server will be degraded. if the cloud provider is unable to meet the users service level agreement, then the user may not be trust on the cloud provider. So this model can not be applied in cloud environment because there is no point of checking users malicious activity done by the users.

III. CONCLUSION

Trust based access control model is one of the efficient mechanism for the security in cloud computing. In this thesis, we proposed a novel trust based access control model for cloud environment. The main goal of this model is to authorize the user and select the most trusted resource for the user. The user is authorized based on their trust value.

References

1. Abraham Yaar, Adrian Perrig, and Dawn Song. Fit: fast internet traceback. In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, volume 2, pages 1395–1406. IEEE, 2005.
2. Americas Headquarters. Cisco data center infrastructure 2.5 design guide. 2007.
3. Amittai Aviram, Sen Hu, Bryan Ford, and Ramakrishna Gummadi. Determinating timing channels in compute clouds. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop, pages 103–108. ACM, 2010.
4. David F Ferraiolo, John F Barkley, and D Richard Kuhn. A role-based access control model and reference implementation within a corporate intranet. ACM Transactions on Information and System Security (TISSEC), 2(1):34–64, 1999.
5. Giuseppe Ateniese, Roberto Di Pietro, Luigi V Mancini, and Gene Tsudik. Scalable and efficient provable data possession. In Proceedings of the 4th international conference on Security and privacy in communication netowrks, page 9. ACM, 2008.
6. Peter Mell and Tim Grance. The nist definition of cloud computing. 2011.
7. Srikanth Kandula, Dina Katabi, Matthias Jacob, and Arthur Berger. Botz-4-sale: Surviving organized ddos attacks that mimic flash crowds. In Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2, pages 287–300. USENIX Association, 2005.
8. Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security, pages 199–212. ACM, 2009.
9. Zhifeng Xiao and Yang Xiao. Security and privacy in cloud computing. Communications Surveys & Tutorials, IEEE, 15(2):843–859, 2013.