A Novel Trust Based Access Control Model for Cloud Environment

Pratap Kumar Behera

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769 008, India

A Novel Trust Based Access Control Model for Cloud Environment

Dissertation submitted in partial fulfillment of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

by

Pratap Kumar Behera

(Roll No. : 213CS2159)

under the supervision of

Prof. Pabitra Mohan Khilar

Assistant Professor

Department of Computer Science and Engineering, NIT Rourkela

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

Dedicated to my family...

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

May 30, 2015

Certificate

This is to certify that the work in the thesis entitled ***A Novel Trust Based Access Control Model for Cloud Environment*** by ***Pratap Kumar Behera***, bearing Roll Number ***213CS2159***, is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of ***Master of Technology*** in ***Computer Science and Engineering Department*** with specialisation in ***Information Security***. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Dr. Pabitra Mohan Khilar
Assistant Professor
Dept. of CSE
NIT Rourkela

Acknowledgment

First and foremost I would like to thank my guruji Sri Sri ravishankar for his blessing and advice to move on whatever we get in our life. I am thankful to my guruji for giving me the strength to complete my thesis.

I would like to express my deep sense of respect and gratitude towards my supervisor Prof. Pabitra Mohan Khilar, who has been the guiding force behind this work. I want to thank him for introducing me to the field of cloud computing and security and giving me the opportunity to work under him. Without his guidance and support it would not have been possible for me to complete this thesis. I am greatly indebted to him for his constant encouragement and invaluable advice in every aspect of my academic life.

I thank our H.O.D. Prof. Santanu Kumar Rath and Prof. Bansidhar Majhi for their constant support in my thesis work. They have been great sources of inspiration to me and I thank them from the bottom of my heart.

I would like to thank all the faculty members, ph.d research scholar, and friends at National Institute of Technology Rourkela for their regular cooperation and encouragement during my thesis work.

I must acknowledge the academic resources that I have got from NIT Rourkela. I would like to thank administrative and technical staff members of the Department who have been kind enough to advise and help in their respective roles.

At last but not the least I am in debt to my parents, all of my family members for their unlimited support and keeping faith on me. Without their dedication and support, even i could not have pursued my M.Tech degree at National Institute of Technology Rourkela.

Pratap Kumar Behera

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. Inorder to protect the cloud environment from malicious users, we proposed a novel trust based access control model. This model authorize the user based on user trust value, before accessing the cloud resources. The user must be trusted before accessing the resources and the resources must be trusted before providing the service to the user. In this thesis, we evaluate the trust value of both user and cloud resources. The user trust value is evaluated based on the user behaviour parameter and resource trust value is evaluated based on the Service Level Agreement (SLA) parameter. If the trust value of both user and cloud resource are more than their trust threshold value, then they are considered to be trusted. Simulation results shows that proposed model performs better than QoS models in terms of Rate of Successful Transactions (RST) and correctness of result (COR).

***Keywords*:** Authorization, Access Control, SLA parameter, Cloud Computing

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Cloud computing is a form of utility computing, which provides the services such as computing, storage, network and appllication as a utility on pay-per use basis over the Internet. Most of the users adopt to cloud computing due to the lack of physical resources such as storage, large computing power, high network bandwidth and high cost software. There are many definitions of cloud computing presented by many authors.

Gartner defines cloud computing as a "style of computing which provides the scalable and IT-enabled capabilities that can be delivered as a service to external customers over the Internet".

According to NIST [3] *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*. This definition was published in 2009 widely accepted by the various industry.

1.2 Essential Characteristics

The five important characteristics of cloud computing is presented as follows:

- **On-demand self-service:** A user can provision the cloud services such as computing , storage, network, and application automatically as needed without user interaction with each cloud service provider.
- **Broad network access:** Cloud services or capabilities are available over the network and accessed from the client such as laptop, tablet, mobile phones, PDA and workstations.
- **Resource pooling:** The cloud computing resources are pooled together to serve multiple users using the multi-tenant model. The virtual resources can assigned and re-assigned to users dynamically acording to their demands. Example of such type of resources is storage, network, computing and network.
- **Rapid elasticity:** The resources capabilities can automatically scale up and scale down according to users demand. Resources often to be available unlimited and accurate quantity at any time.
- **Measured service:** The resources in cloud environment can be monitored, controlled and providing the transparency to the users.

1.3 Cloud Computing Models

The cloud computing model is divided in to two types:
1) Service models
2) Deployment models

1.3.1 Service Models

- **Infrastructure as a Service (IaaS):** This is the first layer in cloud computing service models. It provides the service such as processing, storage, memory, network bandwidth to the users. The users can run or deploy any application or operating systems on the underlying cloud infrastructure.

- **Platform as a Service (PaaS):** This is the second layer in service delivery models. This layer provides the platform for building and executing the application on cloud environment. For example, Google App engine provides the environment for the user to build and deploy their application. This layer is build above the infrastructure layer of cloud environment.

- **Software as a Service (SaaS):** This is the top most layer of cloud service delivery models. In this layer, application software such as Google Docs, game, e-mail etc. are provided as a service over the Internet. Users are unable to purchase high cost application for their personal use. So, the cloud computing provides application in a few cost to the users. Users does not need to maintain the underlying cloud infrastructure.

1.3.2 Deployment Models

- **Private cloud**: In private cloud, the services can be available within a particular organisation. The users who belongs to that organisation is able to access the service. The private cloud can be managed by the organisation itself or any other third party.

- **Public cloud:** In public cloud, the services is available for the public use over the Internet. It can be owned, managed by any business, academic or government organisation.

- **Community cloud:** The community cloud is combination of several organisations from a specific community with common concern. It can be

hosted either internally or externally.

- **Hybrid Cloud:** The hybrid cloud model is combination of two or more cloud model that may remain unique entities. This model bound to offer the benefits of multiple models.

1.4 Cloud Computing Architecture

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 virtualisation technolgy i.e, hypervisor is used to virtualise the cloud resources in order to serve the multiple 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.

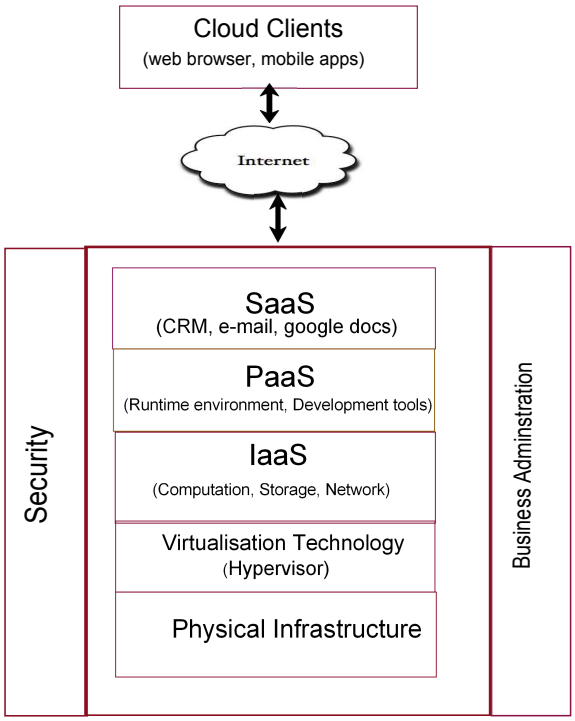

Figure 1.1: Cloud Architecture.

1.5 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 provide on-demand and scalable services, the environment is highly dynamic. The traditional security mechanism can not fulfill all the security requiremnets 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. Figure 1.2 [1] shows the ecosystem for cloud environment i.e, four security goals and privacy. This ecosystem can be applied to any computer or network systems.

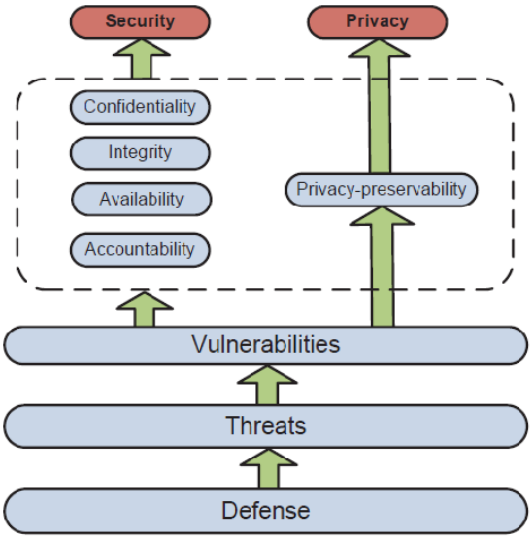

Figure 1.2: Ecosystem of Cloud Security and Survey [1]

1.5.1 Cloud Vulnerabilities

Vulnerability is a weakness present inside the cloud environment by which the attacker can get a chance to exploit this for his own personal gain. The weakness may be present either in hardware or software or network part. The vulnerabilities of cloud computing is explained as follows:

- **VM co-residence**: The VM co-residence can be defined as the multiple independent users can be present in same physical infrastructure. The

virtual machines belongs to different users share the same physical instances. However, the mechanism of VM co-residence may have raised certain security issues such as cross-VM attack [4] and malicious SysAdmin [5].

- **Loss of Physical Control**: In cloud computing, the users store their data in remote cloud server and outsources their computation to the cloud data center. As a result, the cloud users lose the control over their data and computation. So there may be chances of modified, lost or deleted of their outsources data and computation. Users are unable to resist certain type of attacks due to the loss of physical control [1].

- **Bandwidth Under-provisoining**: In cloud computing, the traditional DOS/DDOS attacks is also present and its solution is given in prior researches [6] [7]. But there is also a new type of DOS attack can be made in cloud computing. According to cisco design guide [8], the actual network capacity in a data center is much less than the aggregate capacity of the host located in the same subnet.

- **Cloud Pricing Model**: The billing process of cloud users is determined based on the service they use such as storage, bandwidth, and server hour. But if the attacker manipulate the billing process then the users would be financially responsible for this situation.

1.5.2 Cloud Confidentiality

Confidentiality means the users data and computation should not be disclosed to any other users. Since users outsource their data and computation to the cloud server, confidentiality is one of the major concern in cloud computing.

Threats Cloud Confidentiality

- **Cross VM attack via side channels**: In cloud computing, the same physical infrastructure is shared by multiple users by using the multi-tenancy model. The VM belongs to different users can be present in same physical instances. There are two step process to implement such attacks.

  Placement: In this step, First the malicious VM is to be placed on the targeted server where the target client VM is present. The adversary can identify the location by using the network probing tools such as nmap, hping, etc.

  Extraction: After the placement of malicious VM is complete, the victims VM and malicious VM co-resided with same physical instances. So, the malicious VM can able to access the common resources they use such as CPU pipelines, branch predictors, etc.

- **Malicious SysAdmin**: This type of attack is made by the privilege sysadmin. SysAdmin can directly access to users memory at run time by running user level process.

1.5.3 Cloud Integrity

In cloud computing, data integrity implies that users data on cloud server should not be modified, lost or compromised. Computational integrity means user programs are executed without any modification. If the data or programs are modified by any malicious user or due to adminstartive error by cloud provider then incorrect result will be detected.

Threats to Cloud Integrity:

- **Data loss/manipulation**: In cloud computing, application is delivered storage as a service. The user stores huge amount of data on cloud servers. The

users data may be modified or lost maliciously or accidentally. So, the cloud servers are distrusted in terms of both security and reliability [9]. Due to some adminstrative error (backup, restore, migration and changing membership in P2P systems [10]) data may be lost or modified. Since, users loss the physical control over their data, the attacker may take advantage to initiate the attacks.

- **Dishonest computation in remote servers**: In cloud computing, it is very difficult to judge whether the users outsourced computation is executed with high integrity or not. Since, the computational activity is not transparent enough to cloud users, cloud provider may not follow the honest model and the incorrect result may returned to cloud users. Computation that requires huge amount of computational resource, there may be chances the cloud to be "lazy" [11]. There is another case for dishonest computation, if the cloud provider uses the outdated technology, vulnerable code or any mis-configured policies on their cloud server.

1.5.4 Cloud Availability

In cloud computing, availability is defined as the resources that must be available or accessible when the user wants to access. Availability is one of the core function in cloud computing environment. If the cloud provider is unable to meet the users service level agreement then the user may lose the faith on cloud service provider.

Threats to cloud Availability

- **Flooding Attack via Bandwidth Starvation**: In flooding attack, huge number of nonsensical or malicious request are sent to cloud server in order to hinder the server working properly. There are two basic types of flooding attacks [12].

  Direct DOS- In direct DOS, the attack is intiated after the determination of target VM and the availability of targeting cloud service is fully lost.

Indirect DOS- This is two step process: i) all machine hosted in the same physical machine affected along with victim machine; ii) the attack is initiated without a specific target.

1.5.5 Cloud Accountability

In cloud computing, Accountability is defined as taking the responsibility for providing the required service, security and performance as mentioned in the service level agreement (SLA).

Threats to Cloud Accountability:

- **SLA Violation**: In cloud computing, there are several factors present which may causes SLA violation. i) The machine can be mis configured or defective which causes the loss of data and return incorrect result; ii) The cloud provider can allocate the insufficient resource to user which degrade the performance of the users service and then violate the SLA; iii) An attacker can embed a malicious code in to users data inorder to steal the valuable data or to take over the users machine for DOS attack; iv) The user may not access the data because of cloud server crash or simply data is unavailable at a particular time.
- **Inaccurate billing of resource Consumption:** The cloud users outsources their data and computation to the cloud server. Due to the black box view and dynamic nature of cloud computing, users are unable to verify the billing process. Since this is pay per use model, users only pay according to their utility. The cloud provider may bill the additional cost more than the resource consumption [13].

1.5.6 Cloud Privacy

In cloud computing, privacy is one of the important concern. Privacy is defined as the appropriate use of the information or data. Since the users stored their confidential data on cloud server, there is a huge risk that data may be disclosed to third party.

Threats to Cloud Privacy:

Privacy is violated if the cloud admin or any staff publish the users data (health record, financial details, profile information) to any other person or organisation. There are two types of cloud privacy: data privacy and computation privacy.

1.6 Motivation

In many cases, users turning to the cloud computing because they need to use the services to meet operational demands like high computing capability, network bandwidth, memory speed and huge amount of data storage. Since most of the users adopt to cloud computing, so they loss their physical control over data storage and computation. If the resources in cloud environment gets affected as a result, it is unable to provide the quality of service according to the service level agreement. Therefore, we have to protect both users data and computation as well as cloud resources in order to provide the quality of service. So we allow only those user who are not involved in any malicious activity and we select the resources which can provide the proper quality of services.

The traditional security mechanism can not fulfill all the security requirements for the cloud computing. One of the most fundamental and important key technique that can meet the security requirements for cloud computing is access control technlogy [14]. Many access control model have been designed so far to implement in cloud computing. Role based access control model [15] is an access control technolgy which authorize the user based on the predefined roles and the permission associated with the roles assigned to the user. But this model fails to check the malicious

activity performed by the users. Some authors proposed trust based access control model for cloud environment. But the authors did not give so much attention to the users malicious activities in order to authorize the users.
In this thesis, we proposed a novel trust based access control model in which the users authorization is done based on their trust values.

1.7 Objective of Research

The main objectives of this thesis work is defined as follows:

- **Authorization Problem**: Design a trust based access control model which authorizes the user based on their trust values.

- **Quality of Service Problem**: To select the most trusted resources which can provide the quality of service according to the service level agreement, we have to evaluate the trust value of resources.

1.8 Thesis Organisation

The rest of the thesis is organized as follows:
In chapter 1, we have discussed about the basic concept of cloud computing, service and deployment models, security issues in cloud computing, motivation and objective of our research.

In chapter 2, we present the literature review where we have described some existing works on access control model.

In chapter 3, we present our proposed trust based access control model for

cloud environment.

In chapter 4, we focus on the implementation and experimental results. We implement the proposed model for different type of users in different cloud environment and finally compare our proposed model with the existing model.

Finally, chapter 5 present the conclusion and future work.

1.9 Summary

In this chapter, we discuss about service and deployment models of cloud computing. we also discuss about the security issues such as vulnerability, and threats to all security goals in cloud computing.

Chapter 2

Literature Review

In this chapter, we present a brief literature survey of existing access control model used in cloud environment.

2.1 Introduction

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 a 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 technlogy [14].

2.2 Access Control Model

Access control is a set of procedure which can be used to restricts the users access to a particular system. Access control system monitor and record all the attempts made to access a system. Access Control also identify the unauthorized access attempt by

the user. The access control system can be designed using the models, algorithms and different adminstartive capabilities. So each access control systems has their own attributs, methods and capabilities in order to restrict the user.

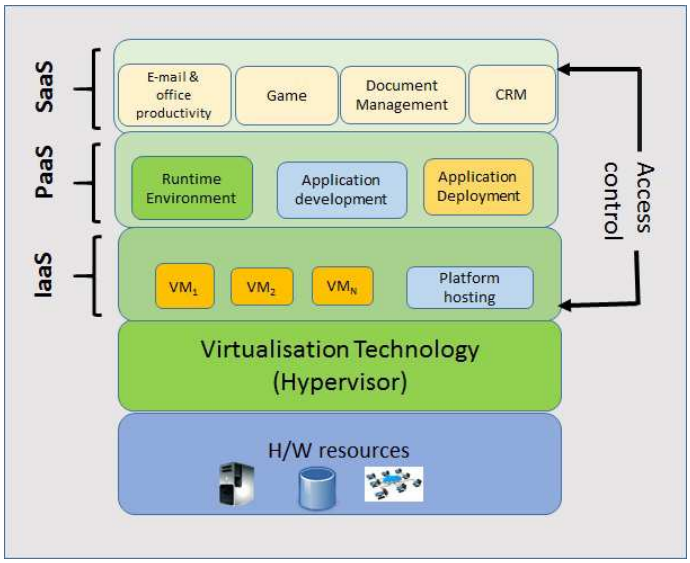

Figure 2.1: Positioning of access control in cloud architecture

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 action 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 IT evironment and cloud environment.

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

2.3 Identity based access control model

Identity-based access control (IBAC) is an access control mechanism which is based on the identity of the user, where access authorizations to specific objects or resources are assigned based on users identity.

2.3.1 Mandatory Access Control (MAC) Model

Mandatory access control model (MAC) [16] is an access control policy in which a subject or request initiator can perform some sort of operation on a particular object or resource. When a subject attempts to access an object or the information in an object an authorization rule is enforced to determine whether the access can take place by examining the security attributes. In order to establish secure access to objects or the information flow within objects, MAC assigns different security level to each subject and object. Although the MAC model protects the information flow or information leackage within object, it does not gurantee the complete secrecy of the infromation in an object.

2.3.2 Discretionary Access Control (DAC) Model

Discretionary access control (DAC) model [17] is an access control policy, grants the owner of an object or resources who is allowed to access the service. Most of the operating systems such as all Windows, Linux, and Macintosh and most flavors of Unix are based on DAC models. In these operating systems, when we can create a file, we decide what access privileges we want to give to other users. When the users wants to access our file, the operating system will make the decision based on the previleges assigned to the file. From security point of view MAC model is more secure than DAC model.
Since the above two models is traditional it would very difficult to protect the cloud enviornment due to the dynamic and openness nature of cloud computing.

2.3.3 Attribute Based Access Control (ABAC) Model

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 [18]. 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.

2.3.4 Role Based Access Control (RBAC) Model

Role based access control (RBAC) [19] model is an access control procedure or mechanism in which the access control decision is made based on the pre-defined roles assigned to the user. The main goal of this model is to authorize the user based on their roles and permission. Before accessing to any cloud resources, first the users role and permission is to be authorized. More than one role can be assigned to a particular user and a particular role can be assigned to more than one user. Roles can be granted new permissions as the application may be changes according to the users requirements. Figure 2.2 depicts the NIST RBAC model which shows the relationship between user, role, and permission. A role is a job function regarding the users authorization and responsibility within a particular organisation. The core of the RBAC model composed of four elements. i) Users ii) Role iii) Permission iv) Object or resource, where the permissions are the type of operations applied to a resource or object.

In comparison to DAC and MAC models, RBAC model has many advantages. But the main disadvantages of RBAC model is it can be only applied within a closed network. Since this model is identity based, it only checks the users identity information in order to authorize the user. If the user is doing any malicious activity

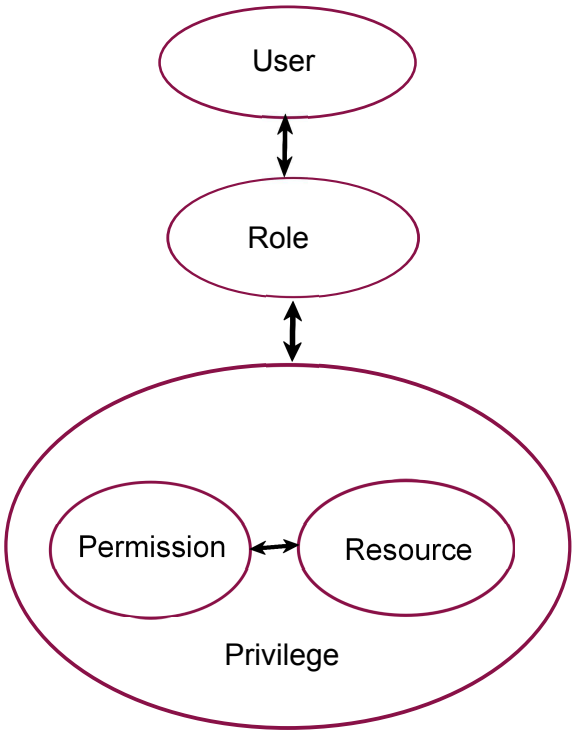

Figure 2.2: User, role and permission relationships in RBAC [2]

on cloud resources, then the RBAC model fails to identify this activities.

2.4 Trust Based Access Control Model

Since cloud computing is very popular form of Internet application, the number of users are very large and the user behaviour is always uncertain and dynamic. So, there is more risk of affecting cloud resources. The above model can not be applied to the cloud environment. Some researcher introduce the concept of trust mechanism [20] 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.

2.4.1 Mutual Trust Based Access Control (MTBAC) Model

Guoyuan et al. [21] proposed a mutual trust based access control model for cloud environment. MTBAC model take both user's behaviour trust and cloud services node's credibility into consideration. First, the trust value is evaluated of both cloud user and service node. If the users trust value is more than their trust threshold value then the user is allowed to access the service. If the cloud service nodes trust value is more than their trust threshold value, then the node is eligible to provide the service. Before the interaction between cloud user and service node they must be trusted to each other. However, this model does not mention the type of malicious operation or attacks the user can perform on cloud resources. This model also do not analyze and take any quality of service parameter to evaluate the resource trust value.

2.4.2 Trust Model Based on Quality of Service (QoS)

Paul Manuel [22] 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.

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.

2.5 Summary

In this chapter, we have discussed briefly about the access control model, different type of access control model such as identity based access control model and trust based access control model. We have discussed DAC model, MAC model, RBAC model, attribute based model, MTBAC model and QoS model, which are already applied for both traditional IT environment and cloud environment.

Chapter 3

A Novel Trust Based Access Control Model for Cloud Environment

3.1 Introduction

Cloud computing is a distributed computing paradigm which provides the services to the users on pay-per use basis. The main aim of designing the cloud computing system is to provide a scalable, on-demand services to the end users in a cost effective manner. Users do not need to be worry about the installation of high cost application on their system. In addition to this, the users do not need to maintain their own physical infrastructure and obtain their services on demand . The services provided by the cloud service provider (CSP) is called cloud services and these services are infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS) [3].

Since, users outsource their data and computation to the cloud server, they may lose the physical control over their data and computation. Loss of physical

control means the users are unable to resist the certain type of threats and attacks. In order to secure the users data and computation in cloud environment, the CSP should protect the cloud server from different tye of threats and attacks. Before the users outsourced their data and computation, the user and cloud provider must be trusted among themselves. Therefore, both the users and CSP must be trusted among themselves before their interaction. The user trust on the CSP based upon the security parameter and the quality of service the CSP provides. The CSP trust on the user based on the user behaviour parameter. If the user behaviour is malicious then the user is not considered as a trusted user.

Before accessing the cloud resources or services from the cloud server, users must be trusted by the CSP. If any legal user performs any malicious activity or introduce some attacks to the cloud server, then the resources of the CSP are affected. As a result, the CSP is unable to meet the security goals and service level agreement. In order to protect the resources, the CSP only allows the trusted user to access the service. To find the trusted user, we must first evaluate the trust value of the user. If the users trust value is more than the trust threshold value, then the user is considered to be a trusted user. The user trust value is evaluated based upon the user behaviour parameter.

3.2 Problem Description

In this thesis, we focus on the problem of user authorization, security, and quality of service provided by the cloud provider. The aim is to evaluate the user trust value and cloud resource trust value based upon user behaviour parameter and cloud resources respectively.

To formulate the problem mathematically, let us consider U_i where $i = 1, 2.....n$ as n number of cloud users and R_j where $j = 1, 2, ...m$ where m as cloud resource set. The main goal is to find the trusted user $TU_k \subseteq U_i$ and the trusted resource $TR_l \subseteq R_j$ based on the user behaviour parameter and the quality of service respectively.

3.3 Proposed Model

We proposed a novel trust based access control model in which the user request is passed through various sub modules to complete the authorization process. Figure 3.1 shows the proposed model is deployed and running inside cloud service provider (CSP). All the resources and services are protected in the cloud environment. There are several resources of same and different types, where each and every resources have different capability and trust values. The proposed model decides which user is allowed to access the service and select the most trusted resources for the users out of all available resources.

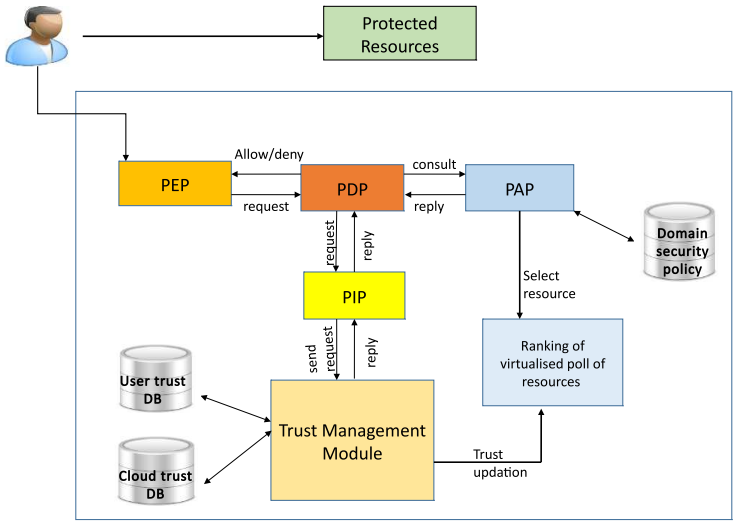

Figure 3.1: Proposed Authorization Model

We explain the function of each sub modules of the proposed model which are discussed as follows:

- **Policy Enforcement Point (PEP)**: PEP receives the user requests from the cloud clients and sends the request to the PDP for evaluation, and after receiving the grant or deny response from the PDP, ensures that the appropriate action is taken.

- **Policy Information Point (PIP)**: PIP is the module that aggregate the information to evaluate an authorization policy. PIP obtains the information about the requested user such as user trust value from the trust management module .

- **Policy Decision Point (PDP)**: PDP gets relevant information from the PIP and consults with the PAP to conclude with a decision whether to grant or deny an access request.

- **Policy Administration Point (PAP)**: PAP is a repository for the authorization policies that are expressed in terms of the actions. Subjects (cloud users) can take on various objects (cloud resources) in the system. The authorization policies are essentially an instantiation of the access control model tailored towards the organization. It is the main component for the authorization portion of access control. PAP makes decision by comparing the information receiving from PDP against the domain security policy of the cloud service provider. Domain security policy stores all the information regarding the user and cloud resources trust threshold value.

- **Trust Management Module(TMM)** : TMM is the main component of the proposed model. The authorization of the user is totally depend upon the trust management module. TMM evaluates the trust value of both user and and cloud resources. After the evaluation of trust value of cloud resources, TMM ranks all the resources having same type according to their average trust value. Finally TMM update the previous trust value of user and cloud resources in their corresponding database.

3.3.1 Authorization Process

Before accessing to any services from the cloud provider, first the user submit their quality of service such as security, computing power and netwoking speed to the cloud provider. The user and cloud provider may negotiate among themselves

about the quality of service for final agreement. This agreement is called as service level agreement. The following algorithm describes about the process of user authorization in order to access the service.

Algorithm

step-1: Policy enforcement point (PEP) accepts the user request and sends it to policy decision point(PDP) .

step-2: PDP first check all the user credentials and if it is correct then send it to policy information point (PIP).

step-3: PIP send the request to trust management module (TMM) for obtaining the user trust value.

step-4: After getting required information from TMM, PIP send it to the PDP.

step-5: PDP consults with the policy adminstrative point (PAP) by sending all infromation coming from PIP and PEP.

step-6: Finally, PAP checks and compares all the collected information of user with domain security policy and resource database. If the user trust value is more than the user trust threshold value then the user is allowed to access otherwise rejected.

step-7: If the user is allowed, then PAP identify the resources based on the user request type,and select the most trusted resource out of all available resources and send it to the PDP.

step-8: PDP sends resource ID to the PEP and if rejected then send deny message.

step-9: PEP forward it to the user with allow or deny message.

step-10: Finally, user can able to access the required serive.

3.3.2 Trust Management Module (TMM)

TMM is one of the most important module of the proposed authorization model. Figure 3.2 shows the TMM is composed of several sub-modules which is involved for the evaluation of trust value for the user and the cloud resources. This module is always running inside the CSP to monitor the user behaviour and the quality of service of the resources. Although the proposed model is deployed and managed by

the CSP, none of the module is biased towards the cloud provider. This module goes through sevaral phases or cycles inorder to evaluate the trust value of both user and resources. Now, we proceed to explain the function and activities of all the components involved in the total life cycle for the evaluation of trust value.

- **Cloud user**: Here the cloud users are all registered users of the cloud service provider. The user sends request to the cloud server and all the credentials are checked by the CSP and if it is satisfied, then the user is allowed to access.
- **Cloud resources**: The cloud resources may be any hardware or software resources that the user can access. All the resources must provide the quality of service according to the service level agreement mentioned during the negotiation process.
- **User behaviour monitoring module**: During the interaction between the user and resources, user can perform legal activities or any malicious activities during the execution of the process. The user behaviour monitoring module always enabled to monitor and record all the activities performed by the users.
- **SLA monitoring module**: This module checks whether the CSP is providing the proper quality of services or not. This module monitors the behaviour and performance of the resources to verify whether they are in compliance with SLA. SLA monitoring module captures data during the interaction process between the user and the CSP.
- **Trust evaluation module**: This module collects the information of the user and cloud resources from the feedback collection agent, SLA parameter database, and user behaviour parameter database. After collecting related information, it evaluates the trust value.
- **Feedback collection agent**: The user submits the feedback to the feedback collection agent after finishing the interaction with the cloud resources. The

user gives the feedback about the correctness of result of the process executed by a particular resource.

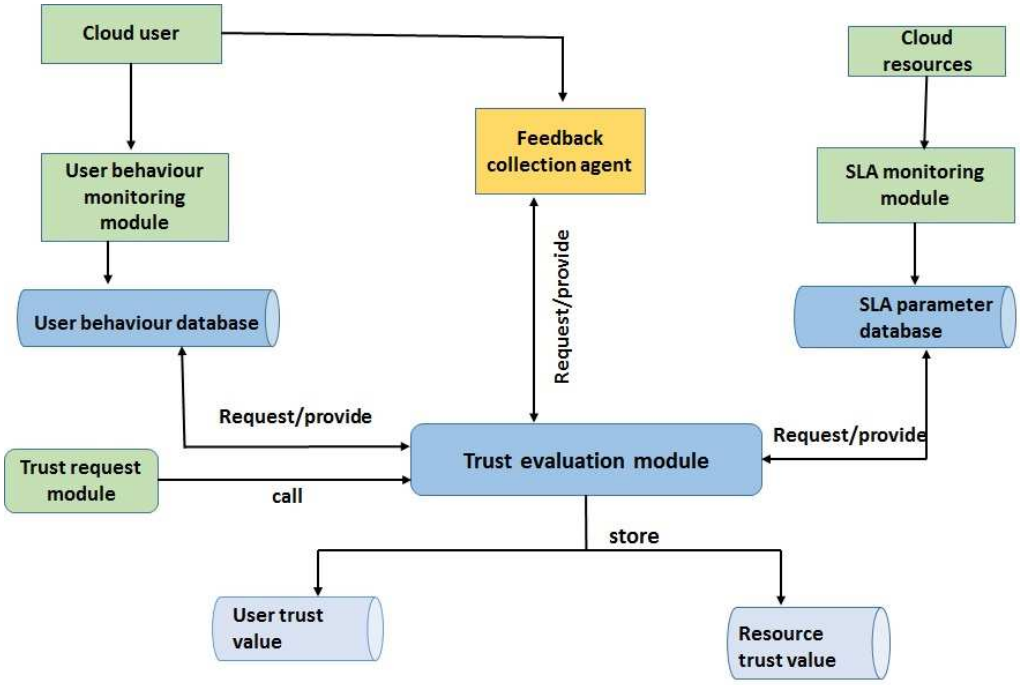

Figure 3.2: Architecture of Trust Management Module

3.3.3 Trust evaluation parameter

Trust evaluation parameter is considered for evaluation of trust values of the users and cloud resources. It consists of user behaviour parameter and SLA parameter.

User behaviour parameter

User behaviour parameter is used to evaluate the trust value of users. If the user is involving in any malicious activity or introducing any attack to the cloud server, then the resources will be affected in which the CSP is unable to meet the quality of service. The user behaviour monitoring module captures the interaction behaviour of user during the interaction of the user with resources and stores it in the user

behaviour database.

The different user behaviour parameters are discussed as follows:

- **Bogus Request Rate (BRR):** Bogus requests are dummy reqests or huge amount of nonsensical request send to the cloud server for consuming the cloud resources intentionally for denial of service attack. Dummy request is used for introducing DOS attack by performing bandwidth starvation. So, this parameter is mainly used for achieving the availability of the cloud computing.

  Let R_k is the number of nonsensical or dummy requests and R_t is the total number of requests made by an user in a unit time interval.

$$BRR = \frac{R_k}{R_t} \tag{3.1}$$

- **Resource Affected Rate (RAR):** The resources may be affected due to the execution of users malicious program execution by the cloud resources. This parameter is used to achieve the reliability of cloud computing. Resource affected rate is the percentage of resources affected out of the resources the user is accessing in a unit time interval.

  Let RA_k is the unit of resources affected and R_t is total unit of accessible resources in a unit time interval.

$$RAR = \frac{RA_k}{R_t} \tag{3.2}$$

- **Unauthorized Opearatin Rate (UAR):** Unauthorized operation is the illegal or malicious operation performed by the user for the purpose of stealing or modifying the data or computation by introducing some attacks. Illegal operation may be dishonest computation in remote servers, vulnerable code in programs. Let UA_k is the number of unauthorized operation performed

and R_t is total operation made in a unit time interval.

$$UAR = \frac{UA_k}{R_t} \tag{3.3}$$

SLA parameter

SLA parameter is used to evaluate the trust value for cloud resources. If the CSP is unable to meet the security level and SLA requirements of any user, then the CSP would be less trusted. The parameter which is involved for evaluation of trust value for cloud resources is discussed as follows:

- **Turnaround Efficiency (TE):** Turnaround time is the exact time between the submission of a job by a user and delivery of the completed job to the user. It is promised by the cloud service provider to the user during the service level agreement. This actual turnaround time is normally different from the estimated turnaround time. Turnaround efficiency of a resource R_k (TE) is the average of turnaround efficiency over all the jobs submitted during the period T [22]. Let TAT_{act} is the actual turnaround time and TAT_{est} is the estimated turnaround time promised by the cloud service provider.

$$TE\ for\ a\ job\ by\ resource\ (R_k) = \frac{TAT_{est}}{TAT_{act}} \tag{3.4}$$

Turnaround efficiency of a resource R_k (TE) is the average of the turnaround efficiency over all the jobs submitted during the time period T .

$$ATE(R_k) = \sum_{i=1}^{n} \frac{TE_i}{n} \tag{3.5}$$

The factors affecting the turn around efficiency of cloud resources which is allocated by CSP to the users are i) allocating the less configurable resources; ii) less effective scheduling algorithms.

- **Resource Availability (RAV):** Availability is the degree to which the system must be functional or operational when it is accessible [23]. If the resources are affected by the attackers or malicious users which consumes the resources intentionally, then the resources are unavailable and unable to process the user request.

  Let us assume that $R_1, R_2, ..., R_k$ are the cloud resources. For each $k = 1, 2, ..., m$, let N_k denotes the number of jobs submitted to cloud resource R_k over a time period T. Out of N_k jobs submitted to R_k, let A_k denotes the number of jobs accepted by the resource R_k over a time period T.

$$RAV(R_k) = \frac{A_k}{N_k} \tag{3.6}$$

  When the job is submitted to the cloud resources, the resources may be unavailable due to the several reasons. i) a part of the service of the resources is denied to the user; ii) resources may be shut down; iii) Resources are too busy to process the job [22].

- **Rate of Successful Transaction (RST):**

  RST is defined as the total number of job executed successfully by the resource R_k in a unit time interval. It is also called as success rate. RST of a cloud resource is a measure of successful completion of accepted jobs by the cloud resource [24]. Out of A_k jobs accepted by resource R_k, let C_k denotes the number of jobs completed successfully by the resource R_k over the period T.

$$RST(R_k) = \frac{C_k}{A_k} \tag{3.7}$$

  The reliability of resources is affected by several reasons. i) process or jobs fail due to the restriction on scalability; ii) jobs fail when the number of database connection pool is increased; iii) Due to time-out of jobs; iv) Overflow of

job queue; v) Data resource missing; vi) computational resource missing; vii) Database failure; viii) network failure [25].

- **Correctness of Result (COR):** Correctness of result is used to define the data integrity in cloud computing. Data integrity is a broad term which includes security, privacy and accuracy of data. Data may be modified or corrupted during the poor network latency or any hardware and software failure. Data precision loss might happen due to obsolete computing resources [22]. Let D_k is the number of jobs which preserved the data integrity or correctness of result out of the C_k jobs.

$$COR(R_k) = \frac{D_k}{C_k} \tag{3.8}$$

The data integrity of users data and computation is affected or modified by i) Due to poor network latency; ii) Due to obsolete computing infrastructure; iii) Dishonest computation.

3.3.4 Trust Evaluation Strategy

We evaluate the trust value of the users and cloud resources after finshing their interaction in a unit time interval. There may be several interaction in this time interval. First, we evaluate the trust value in current time window and evaluate the average trust value by using previous time window average trust value and current time window trust values. Fig. 4 depicts the time window diagram for the evaluation of trust value.

Let t_n and t_{n-1} be the time interval for the current time window and previous time window respectively.

The formulas for evaluating the user trust (UT) and average user trust (AUT) value are shown below:

$$UT = 1 - (W_1 * UAR + W_2 * BRR + W_3 * RAR) \tag{3.9}$$

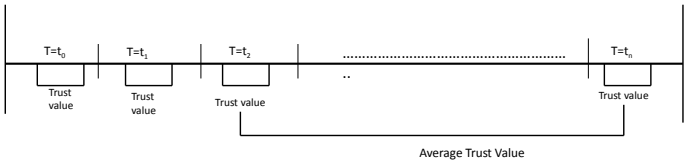

Figure 3.3: Time Window

$$AUT = \alpha * (UT)_{t_n} + (1 - \alpha) * (AUT)_{t_{n-1}} \tag{3.10}$$

where UT and AUT are the user trust value and average user trust value respectively. W_1, W_2, W_3 are the weight parameters of UAR, BRR and RAR respectively.

The formula for evaluating cloud resource trust (CT) value and average cloud resource trust value (ACT) are shown below:

$$CT = Q_1 * TE + Q_2 * RAV + Q_3 * RST + Q_4 * COR \tag{3.11}$$

$$ACT = \alpha * (CT)_{t_n} + (1 - \alpha) * (ACT)_{t_{n-1}} \tag{3.12}$$

where CT and ACT are the resource trust value and average resource trust value respectively. Where Q_1, Q_2, Q_3 and Q_4 are the weight parameters [22] of TE, RAV, RST and COR respectively. α and 1- α are the weight values for t_n and t_{n-1} time intervals.

3.4 Summary

In this chapter, we have discussed about our propsed authorization model and algorithm how to authorize the user. We have discussed the working principle of trust management module which is responsible for evaluation of users trust value and cloud resource trust value. We also discussed the user behaviour parameter and SLA parameter which is used for identify the trustworthiness. Finally, we evaluate the trust value of cloud users and resources using the above parameters.

Chapter 4

Implementation Work and Results

4.1 Introduction

We implement our proposed model, algorithm and evaluate strategy to evaluate the trust value of user and cloud resources. Based on the trust values, we discriminate the user and cloud resources as good or malicious.

4.2 Experimental Setup

We create a vitrual cloud environment in which the resources of different capabilities are defined. First the user submits their quality of service requirements such as security, computing power, and networking speed to the cloud provider.
We implement our proposed model using the following platform:

- jdk 1.7
- Net beans IDE
- oracle 11g

We assume the probability values of weight parameters for user behaviour parameter and SLA parameter according to the priority of the security requirement in our experiment. We consider the probability values for user behaviour parameter and SLA parameter [22], which are shown in Table 4.1 and Table 4.2 respectively. The machine configuration of the implemented system is corei5 processor having 3.2 ghz, 4GB RAM, 500 GB HDD and windows 8 oeratng system.

Table 4.1: For User Behaviour Parameter

Weight Parameter	**Probability**
W_1	0.5
W_2	0.2
W_3	0.3

4.3 Process of Implementation

The implementation steps involved for identifying the malicious users and resources is explained as follows:

- Negotiation of service level agreement (SLA) between user and cloud service provider.
- User authorization.
- Resource allocation to authorized users.
- Monitoring the user behaviour parameter and SLA parameter of user and cloud resources respectively.

- Users submit their feedback to the feedback collection agent.
- Collect the user behaviour parameter and SLA parameter information from their corresponding database.
- Evaluate the trust value and average trust value of cloud user and resources.
- Update the AUT and ACT.
- Ranking the resources according their trust values.
- Finally, identify the malicious or un-trusted user and malicious resources.

4.4 Simulation Results

We evaluate the trust values of cloud users and resources in each unit time interval. After evaluation of trust values, we categories the users and resources into two different type i.e good and malicious.

4.4.1 Trust value of different type of users

We evaluate the average trust values of all the users accessing the cloud service in a unit time interval. We evaluate the trust value in each time interval and average trust value using current time window and previous time window. According to the average trust value of users we classify in to good, and malicious users. In order to classify the users, we assume user trust threshold (UTT) value as 0.6 and the condition for good, and malicious users is shown in table 4.3. Figure 4.1 shows the trust value of good user, malicious user. The users whose trust value is more than the threshold vale is above the threshold line and the users whose trust value is less than the threshold value is below the threshold line. The threshold line is depend upon the user trust threshold value.

Table 4.2: For SLA parameter

Weight Parameter	**Probability**
Q_1	0.1
Q_2	0.2
Q_3	0.2
Q_4	0.5

4.4.2 Trust value of different CSP

Figure 4.2 shows the trust value of different CSP such as good, and malicious CSP . If the resources of cloud provider is affected by malicious attacks or due to some adminstartive problems, then the resources is unable to meet the service level agreement. As a result, the trust level of the resources is reduced and considered as a less trusted resource. Table 4.3 shows the condition for good, and malicious CSP. Figure 4.2 shows the trust value of good CSP, and malicious CSP.

Table 4.3: Type of user and CSP

	Good	**Malicious**
Type of User	$AUT \geq UTT$	$AUT < UTT$
Type of CSP	$ACT \geq CTT$	$ACT < CTT$

4.4.3 Rate of successful transaction (RST)

This experiment demonstrates the success rate of cloud resources. We evaluate rate of successful transaction of cloud resources based on the percentage of malicious

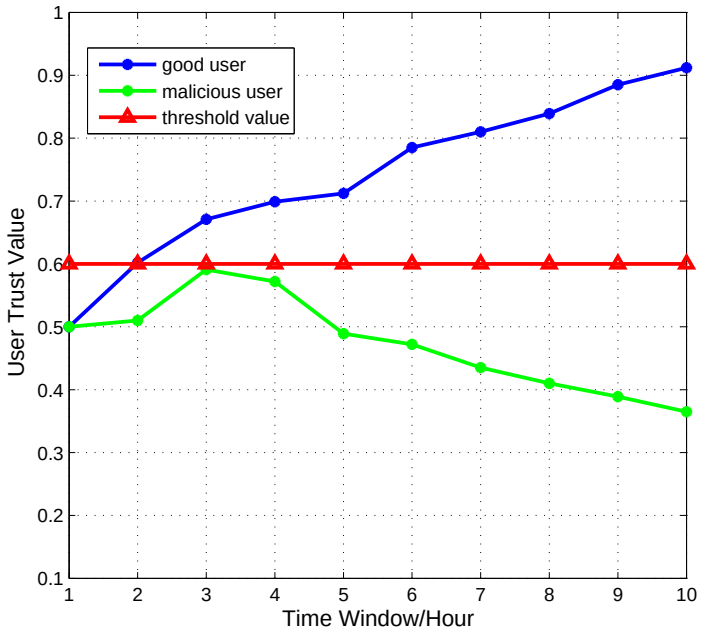

Figure 4.1: Trust value of cloud users

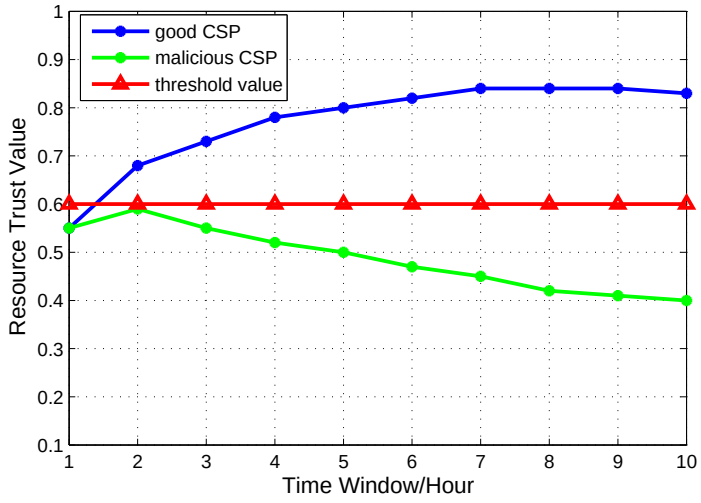

Figure 4.2: Trust value of different CSP

requests.

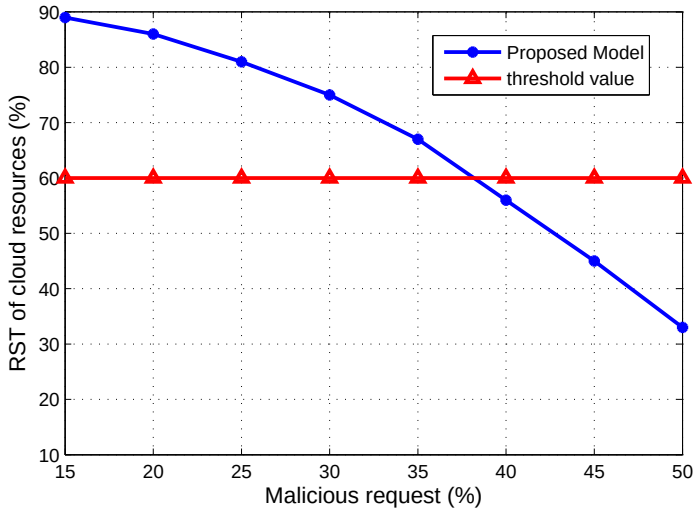

Figure 4.3: RST of cloud resources

4.4.4 Comparison with QoS Model

We compare our proposed model with the the existing QoS model for showing the quality of service provided by the CSP in terms of data integrity and success rate of cloud resources.

Rate of Successful Transaction

This experiment demonstrates the success rate of cloud resources in a unit time interval. We take same number of jobs in each time interval and send the request to both the models. As time goes on, user behaviour will dynamically changes. The proposed model identify the malicious user based on their trust value. But in QoS model, there is no point of checking the user malicious behaviour. Since the affected rate of cloud resources will be more in comparison to proposed model, the RST of cloud resources is less than the proposed model.

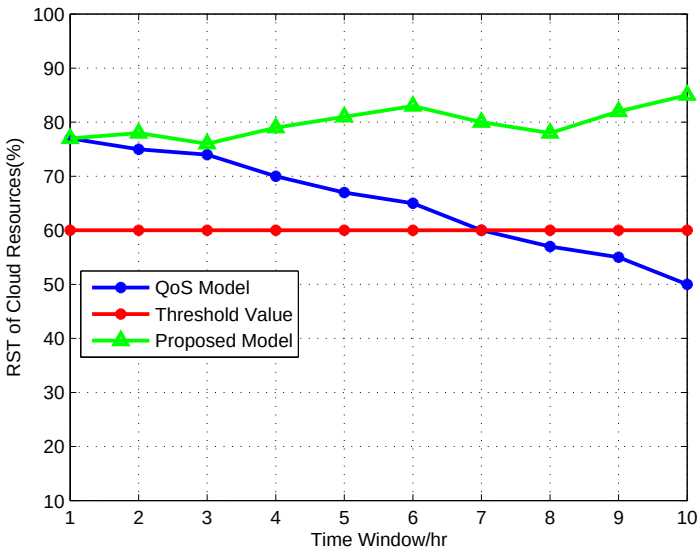

Figure 4.4: The Comparison of RST among Qos and Proposed Model

Correctness of Result

This experiment demonstrates the data integrity of the all submitted jobs by cloud resources in each time interval. We assume 200 jobs submitted by all the users in a unit time inetrval. We experiment the same number of users request to both the models. As time window increases the user behaviour parameter may change. The users trust level changes dynamically according to user behaviour parameter. The proposed model allows the user to access the cloud resource based on the trust value so there is very less chances of affecting cloud resources. But the QoS model has no point of user authorization which is more chances of affecting the cloud resources. So the percentage of correctness of the result would be less by QoS model.

4.5 Summary

In this chapter, we have implemented the proposed model and algorithms. We evaluate the trust value of different type of users in different cloud environment. Finally we compare our proposed model with the Quality of Service (QoS) model to

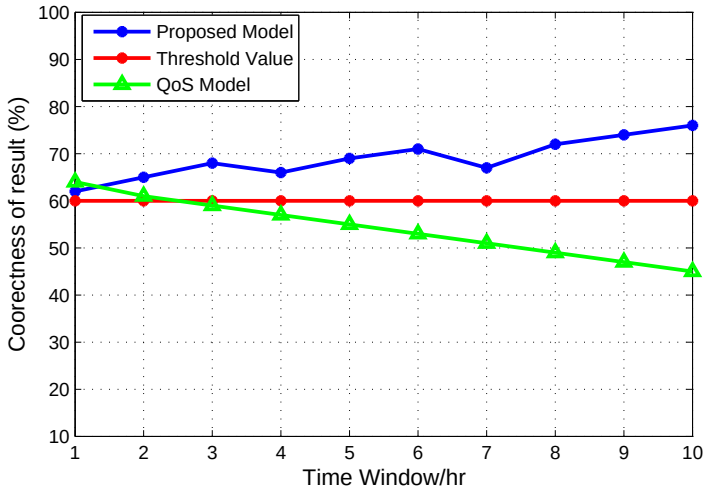

Figure 4.5: The Comparison of COR among Qos and Proposed Model

show the our model performs better than the Qos model.

Chapter 5

Conclusion and Future Work

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. We evaluate the trust value of all users and discriminate the user in to different categories such as good, and malicious users. We evaluate the trust value of cloud resources based on the quality of service provided to the users. We experiment how the reliability of resources is decreased as the cloud resources is affected by users malicious activity. Finally, we compare our proposed model with the existing Quality of Service model for showing the rate of successful transaction and correctnes of output. It shows our proposed model performs better than QoS model.

In future, we can extend our work to implement in multidomain cloud environment. We can make a decentralised access control model to work for different cloud service provider. We can add more security features to cloud environment by using different methods and techniques.

Bibliography

[1] Zhifeng Xiao and Yang Xiao. Security and privacy in cloud computing. *Communications Surveys & Tutorials, IEEE*, 15(2):843–859, 2013.

[2] 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.

[3] Peter Mell and Tim Grance. The nist definition of cloud computing. 2011.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Americas Headquarters. Cisco data center infrastructure 2.5 design guide. 2007.

[9] 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.

[10] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, and Dawn Song. Provable data possession at untrusted stores. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 598–609. Acm, 2007.

[11] Cong Wang, Kui Ren, and Jia Wang. Secure and practical outsourcing of linear programming in cloud computing. In *INFOCOM, 2011 Proceedings IEEE*, pages 820–828. IEEE, 2011.

[12] Meiko Jensen, Jörg Schwenk, Nils Gruschka, and Luigi Lo Iacono. On technical security issues in cloud computing. In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*, pages 109–116. IEEE, 2009.

[13] Vyas Sekar and Petros Maniatis. Verifiable resource accounting for cloud computing services. In *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, pages 21–26. ACM, 2011.

[14] Bai Qing-hai and Zheng Ying. Study on the access control model. In *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011*, volume 1, pages 830–834. IEEE, 2011.

[15] Ravi Sandhu, David Ferraiolo, and Richard Kuhn. The nist model for role-based access control: towards a unified standard. In *ACM workshop on Role-based access control*, volume 2000, 2000.

[16] Messaoud Benantar. Mandatory-access-control model. *Access Control Systems: Security, Identity Management and Trust Models*, pages 129–146, 2006.

[17] Younis A Younis, Kashif Kifayat, and Madjid Merabti. An access control model for cloud computing. *Journal of Information Security and Applications*, 19(1):45–60, 2014.

[18] Eric Yuan and Jin Tong. Attributed based access control (abac) for web services. In *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on*. IEEE, 2005.

[19] Mohammad A Al-Kahtani and Ravi Sandhu. A model for attribute-based user-role assignment. In *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*, pages 353–362. IEEE, 2002.

[20] Matt Blaze, Joan Feigenbaum, and Jack Lacy. Decentralized trust management. In *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, pages 164–173. IEEE, 1996.

[21] Guoyuan Lin, Danru Wang, Yuyu Bie, and Min Lei. Mtbac: A mutual trust based access control model in cloud computing. *Communications, China*, 11(4):154–162, 2014.

[22] Paul Manuel. A trust model of cloud computing based on quality of service. *Annals of Operations Research*, pages 1–12, 2013.

[23] Shuping Ran. A model for web services discovery with qos. *ACM Sigecom exchanges*, 4(1):1–10, 2003.

[24] Punit Gupta, Mayank Kumar Goyal, Prakash Kumar, and Alok Aggarwal. Trust and reliability based scheduling algorithm for cloud iaas. In *Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing*, pages 603–607. Springer, 2013.

[25] Yuan-Shun Dai, Bo Yang, Jack Dongarra, and Gewei Zhang. Cloud service reliability: Modeling and analysis. In *15th IEEE Pacific Rim International Symposium on Dependable Computing*, 2009.

Dissemination

1. P.K. Behera, P.M. Khilar, "A Novel Trust Based Access Control Model for Cloud Environment", *The Fourth IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2015 (Communicated)