Credit Value and Attribute Based Access Control Mechanism for Cloud Data Centres

Ajay Kumar Dubey, Vimal Mishra

Abstract*: *Now-a-days the cloud is very useful for providing many IT services. These services are delivered over the internet and accessed globally with the help of internet. The cloud service provider ensures flexibility in provisioning and scaling of resources. The cloud services are completely managed by cloud service provider (CSP), which ensures the end to end availability, reliability and security of the cloud resources. The exponential growth of cloud services has provided many opportunities but has also perplexed severe security concerns. The popularity of cloud service based applications is rapidly increasing due to which many security and legal issues are arising. In this paper we describe the existing access control method and framework for securing cloud services. The concept of modified reputation and attribute based access control system has been discussed. In this approach the concept of crowd reviewing has been used to compute the credit value of users. The simulation experiment has been shown to protect the consistent users and to restrict the access of inconsistent users in cloud environment. It is an access control approach to mitigate the challenges in security concerns. This access control mechanism is helpful for cloud application services, which automatically restrict the malicious users from the access of resources. It is also helpful in authorization of users to access the cloud resources.

Keywords* : *Access Control, Crowdreviewing, Crowd Voting, Cloud Computing and Credit Value.

I. INTRODUCTION

The exponential growth of cloud services has provided enormous opportunities but has also created serious security concern. Though companies offer regular security updates as a patch work. Many security measures have been adopted regularly and new protocols have been developed to improve the security in the cloud environment. Even though to meet the security and performance of demanded cloud service is a tedious job due to the exponential increase in the demand. Many different types of users are accessing these open cloud services. It's very difficult to detect the behaviour of users and restrict the malicious behaviour. The cloud computing system should have provision for encourage the good behaviour and restrict the malicious behaviour to prevent the security risk in cloud environment [1] [2]. Crowdreviewing is the process of collecting opinion or feedback from large number of users. This process is also known as the crowd voting. The concept of crowdreviewing is based on the principles of crowdsourcing. crowdsourcing is an act of outsourcing a task to large number of people in the form of open call [3]. This crowdreviewing is useful in computation of the credit value of the users. The credit and reputation model [4] [5] is now very popular and useful for cloud based applications. This paper is structured into eight sections. The section II describes the significance of access control mechanism in cloud environment, the section III explains the access control framework for cloud environment and section IV describes the types of access control methods. In section V the literature survey has been performed. In section VI the credit value and attribute based access control model is defined. In section VII simulation algorithm and results has been shown. Finally, the conclusions and the future work are discussed in Section VIII.

II. SIGNIFICANCE OF ACCESS CONTROL MECHANISM IN CLOUD ENVIRONMENT

In cloud computing environment the access control mechanism is required, when any user want to access the resources from cloud server. Access to a system or a resource to be controlled by some process and we say this process as access control mechanism. Access control mechanism defines the capability of the user to perform an authorised operations viz. read, write, modify, delete, execute, update etc. The access control mechanism ensures confidentiality and security of the server resources. The important aspects of security are to protect the resources from unauthorized access, integrity of resources and ensuring availability of the resources for the authorized users. Access control mechanism shows the control flow of information between the different type of users and the resources. The components of access control mechanism communicate and interact with each other and work together to provide a secure environment. There are mainly following components responsible for secure access control mechanism [6] [7].

A. Identification

The effective access control mechanism must have some kind of strong identification system to identify the entities. If the identification system is poor then there is the chance of malicious entity gets identified. This malicious entity got access permissions may cause severe damage to the system.

Manuscript published on 30 September 2019
* Correspondence Author

Ajay Kumar Dubey*, Dr. A.P.J. Abdul Kalam Technical University, Lucknow, India. Email:ajaydubey78@gmail.com

Vimal Mishra, Institute of Engineering and Rural Technology, Allahabad, India. Email: vimal.mishra.upte@gmail.com

B. Authorization

The process of identification is based on authentication. On successful authentication of entity the authorization process is performed. In this the access levels granted for that particular entity. Every user has different level of access permission. A database is maintained on cloud server for different access role. Every entity may have its associated access role.

Authorization can be performed using any one of the following ways, the authenticated entity gets authorization and access control to perform the read, write, delete, update and execute operations.

C. Accountability

Accountability ensures that all actions of access control are attributed to an authenticated entity. Accountability is very important in access control mechanism in cloud environment; this is often achieved with the help of system logs and database maintenance. The system log stores the all information like the successful and failed attempts toward the access of the resources. The auditing of database maintenance also ensures the accountability; it is simply a tracking system for a particular application or services.

III. Access Control Framework for Cloud Environment

Access control mechanism explains the detail that which user can access what resources. The services or resources available in the cloud environment are elastic and loosely coupled which are highly prone to security attacks. So some defense mechanism is required for secure access of these services by users. The access control is the basic defense mechanism to restrict the access of the services or resources. The prerequisites for the access control framework are given below:

- There should be provision of access control in this mechanism, for sharing the services with a group of users.
- It should provide proper access to the user, i.e., the information is not shared without the permission of the data owner.
- The mechanism must be able to generate notifications about the usage of the services to the data owner.
- The mechanism must be able to define access control constraints according to the defined rules.
- The mechanism must be able to define access control based on predefined constant as well as dynamic properties of the services.
- The mechanism provides the options that users can perform any specific operations on services, such as read/write/execute.
- The mechanism process must be transparent to its users.

The access control framework is developed to implement the security policy and to define how the users can access the resources. The access control mechanism is needed for the protection of the services from the access attacks. The access control mechanism decides whether the access permission of the services or resources to be granted or not to the requested user. There exist several models [8] for the development of access control mechanism. The access control framework for cloud environment consists following components (i) Access Control Policies, (ii) Access Control Models and (iii) Access Control Mechanisms.

A. Access Control Policies

The access control policies define a set of protocols which are used while implementing access control mechanism. The request is processed by cloud server considering the services or resources available in the cloud environment. The cloud server determines whether to grant or deny the permission to user. The mechanism is implemented using some regulations established by the policy. Different mechanisms can be applied based on the permissions, by different means of security assurances.

B. Access Control Models

The access control model provides a formal presentation of the access control policy and its related functional working. It provides a formal proof of security properties being designed for access control system. They define low-level and high level functions that are defined by the policy.

C. Access Control Mechanisms

This defines the basic functions of model which implement the controls that are defined by the policy.

The mentioned concepts correspond to the conceptual separation between the different levels of the design and provide multilevel software development. The separation is between the policies and mechanisms applied on the services. It is possible to discuss the protection requirements based on the policies, compare different access policies and mechanisms and the enforcement of these policies on the entities involved in the communication. It should also provide tamperproof information, confined to a limited part of the system and apply rigorous verification methods. The various access control mechanisms are discussed in the following sections.

IV. Types of Access Control Methods

There exist many types of access control method. These access control method has been discussed and compared with reputation and attribute based access control method as follows:

A. Identity-Based Access Control (IBAC)

In identity based access control method the authentication and their access right policies are to be publicized by the certificate authorities [9]. The access rights of a user to access any resources can be stored with the help of access control list (ACL), i.e., the entry in the ACL specifies whether a user will be permitted or denied to access any resources within the cloud network. The agents in the cloud network can store the list of the authenticated users and their permissions in the databases. The requests of the entities can be fulfilled by other databases, if it comes via an authenticated entity. The identity based access control method is very straight forward but it may contain Information leakage problems.

B. Authorization-Based Access Control (ABAC)

The identity-based access control depends on the identification process of the entity and in this approach the entities access control permissions are stored with the certificate authorities. While in authorization based access control, if a service is requested by the entity then it is forwarded to the policy engine for determining the authorizations. The service is allocated to the entity on the basis of its authorization but not on the identity. The identity of the entity is forwarded to the policy engine and it returns the access permissions, which the entity is allowed to do. Entity requests the service by including the rights it wants to access. In this case authorization gets priority over identity, which improves the security of the system [10]. The IBAC has a list of entities associated with the service while ABAC has a list of access permissions for each entity. A policy language can be used to store which entity gets which rights. This has an advantage over IBAC as each database has the details about its own entities, no problem of distributed identity management. If one entity changes the duties to another, the access permissions are simply changed in that database and can revoke that are not appropriate. No need to inform other databases about the changes, as no other database is involved and no information leakage about the organization as the structure of the database is not revealed to another.

C. Rule-Based Access Control (R-BAC)

In this system, the access to the services is based on the list of predefined rules for the access to be granted. The rules are created by the owners and access controls are granted on the basis of the specified condition. In the ACL, the matrix can specify which entity is allowed to access what, whereas in rule-based system conditions are applied for the access of a particular application. Rule-based access control [11] is similar to the discretionary access control. In this control system owner makes the rules according to its organization's need. Rules are enforced using a mediation mechanism which ensures the access by intercepting each and every request comparing with the access permissions of the entity.

D. Policy-Based Access Control (PBAC)

In this case all defined policies are stored in policy repository and system verifies whether an entity is authorized to access a service according to the repository and agreed by the entity. The activities are controlled by the rules with diverse granularities on cloud server. The security policies are dependent on the role the entity plays within an organization. These policies are implemented by different levels of the owners of that particular department [12]. Since the different policies are described for different users, so it's very difficult to reach on common consensus for global view of the policies. Sometimes few policies may conflict and it is almost impossible to reach on common consensus. The solution of this problem is to enforce the predefined rules in a consistent way and keep track of the access rules, always keep them up to date. It should allow a wide variety of mechanisms to implement; the access status should be made clear and no direct access to the services. All these rule are to be considered and some meta information to combine them for taking a final decision. A policy will specify how these rules are to be combined, composite aggregate rules using a composite pattern are considered. All the applicable rules are to be stored in repository of the cloud server [13].

E. Discretionary Access Control (DAC)

Discretionary access control is a very early form of authorization which are widely deployed in many architectures like UNIX, Linux etc., as it is flexible in nature [14]. These are implemented on the option of the user. Now-aday's these are used to manage the owners data in their own systems and the security of that files, OS as well as it is supported by Linux. The owner determines the privileges they can allocate for others. It is user based and the owner has the right to allocate the access and to whom based on the requirements. The owner can allow, in general, unrestricted access or they can allow specific entity or set of entities to access the service. The owner of the service has full control regarding the access of the owned service by other entities and such controls are called discretionary. The matrix gets updated when the service and the entities are added or deleted. These are inadequate for enforcing the information policies. The policies control the access of the entities to the services on the basis of the entity's identity and specific access permissions, for individual entity or a class of entities which are allowed. If the access permission is related to the service, the access is allowed or denied. The problem with this approach is that there is no constraint on copying the information from owner service to other [15]. As well there is no actual assurance of information flow and does not impose any restriction once the entity receives the service. In mandatory systems the diffusion of the service is controlled by restricting the information flow from high level to low level entities.

F. Role-Based Access Control (RBAC)

The Role-based access control mechanism is most popular and widely used access control technique due to its low cost and optimum security. It was pioneered in the 1970s for the online systems which has begun with multiuser environment. The advantage of this technique is that it is not directly related with the policy but has been well known as a safety model and enforces the access control mechanism in an organizational way [17]. This has greatly simplified the management of permissions. The access control is allocated based on the roles the entities are assigned by the organization of a network. The owner governs what the roles can access and how they can access the services as in DAC or Policy-based or as with MACs. It regulates entity access on the basis of the entity activity execution in the system and its own access capabilities. Role-based policies depend on identification of the roles in the system. A role is a set of activity, can be performed by the entity. Services are linked with a role that contains the privileges assigned to that role. Entities can be reassigned from one role to another. Entity supports the following three security concepts:

i. Least privilege ensures that only those permissions are assigned to the users, which are necessary for the completion of the tasks.

ii. Separation of duties is ensured by invoking the mutually exclusive roles to complete a particular service.

iii. Data abstraction issues an abstracted permissions to the entities rather than the read, write, execute which are allocated by the operating system.

Table 1: Role Access Matrix

Sr. No.	Role of the User	Permission Granted
1	Technical User	Read, Write
2	Normal User	Read only
3	Data Owner	Read, Write, Append
4	Service Provider	Read, Write, Execute

The adoption of this model has several advantages like authorization management, roles hierarchy and separation of duties [18]. This allows better management by separating the entity assignment to the roles and the access control to the roles. It allows better static/dynamic constraint enforcement that restricts the number of roles allowed for a given privilege. This is true even for a group of entities and the roles the entities play in various groups [19]. When we look at the meaning of a group, it is a list of entities which have the same access permissions for a period of time using some defined procedures. It includes the capability to establish the relationships between the roles and the permissions as well as entities and roles.

V. LITERATURE SURVEY

M. Mulimani and R Rachh [24] reviewed existing access control mechanisms and analyses these schemes. According to them access control plays a major role in providing data security and privacy. It is the simplest way to protect the cloud storage from unauthorized and malicious users. One of the major areas where access control is used is in medical health care, wherein sensitive information can be accessed only by authorized users such as doctors, researchers, and medical staff. It is concluded that Attribute-based Encryption (ABE) is the most suitable access control mechanism for the cloud computing environment. Attribute-based access control provides best access control by granting different access rights to a set of users and allows flexibility in specifying the access rights of individual users.

R. Aluvalu and L. Muddana [25] surveyed many access control models related to cloud computing. In this literature they discussed merit and demerit of these models and possible solutions to overcome their limitations. In this paper they mainly analysed the effective access model required for cloud system. Since cloud computing is a distributed and dynamic model, static policies are unsuitable for access control in cloud system. Hence, access control models that support dynamic policies and attribute-based access control models using encryption techniques are discussed and analysed. In this paper access models using Extensible Access Control Markup Language (XACML) are implemented for a comparative study. XACML is mainly an attribute based access control system (ABAC). Their Future work includes the implementation of a risk-aware role-based access control model integrated with a hierarchical attribute-based set.

Demchenko et al [26] defined the basic model and architectural pattern for federated access control in heterogeneous multi-cloud and inter-cloud federation. There exist mainly two types of federations i.e. client side federation and service provider side federation. The client side federation includes cloud based services and client architecture while the service provider side federation includes the set of service providers and client. The main task of service provider side federation is to outsource their resources to the customer. The proposed access control method, in this paper uses the federated identity management (FIDM) model which rely on the trusted third party such as cloud service broker (CSB). This paper define the Inter-Cloud Architecture Framework (ICAF) which resolves the problem of multi-domain heterogeneous cloud based application integration and inter-platform interoperability. This research analyses different federated identity management scenarios and proposes solution for number of practical problems in multi-provider service integration and enterprise users.

Zhou et al. [27] proposed a trust model with cryptographic role-based access control (RBAC) for secure cloud data storage. The proposed system considers role inheritance and hierarchy to evaluate the trustworthiness of users and roles. The proposed system uses role-based encryption (RBE) to encrypt and decrypt user requests. In this paper the concept of account role inheritance has been used to propose a trust model for role based access control. This paper shows that how the trust model can be integrated into a system that uses cryptographic RBAC scheme. The trust model is analysed and evaluated with a real-time application. The results show that trust models can be used to reduce risks and enhance the decision making skills of data owners and role managers in cloud storage. However, the performance of this system is poor due to the large size of the encryption and decryption key.

Varadharajan et al. [28] proposed a novel cryptographic administrator model for managing and evaluating a cryptographic role-based access control model (AdC-RBAC). Cryptographic techniques are used to verify that administrative tasks are performed only by authorized administrators. The proposed RBE implements access policies on encrypted data for improved data privacy in cloud storage. In the proposed technique the data owner can encrypt the data into specific role. So only authorize users of this role can decrypt it. The advantage of this technique is that if administrator wants to add or delete any existing user from this role, it only need to update their role parameter without affecting any user or other roles. The AdC-RBAC model can be used in an untrusted environment since its security is guaranteed by using cryptographic RBAC technique.

Ayed and Zaghdoudi [29] proposed a Kerberos-based access control system for the cloud environment. This is a generic access control system which is applicable on many different cloud service models. This proposed system is based on the Kerberos, access control lists and authorization tickets.

This system is designed and developed using the CloudSim cloud simulator, which is a Java-based open source simulation environment. The proposed solution is implemented over an Openstack cloud platform with Kerberos. In this paper a new single sign on (SSO) access control system is proposed. The test result shows that token interception and replay have been prevented. The main advantage of this system is its generality. This system can be extended to examine the performance of mobile and fog computing.

Khamitkar et al. [30] proposed a Kerberos based single sign-on (SSO) authentication method, which is helpful in preventing the distributed denial of service attacks in cloud environment. This method is developed using the Visual Basic 2010 framework and implemented with Amazon S3 cloud. This method can work as a trusted third party between the cloud service provider and the consumer. It ensures the secure access of cloud services. The performance analysis of this method shows that it is very dynamic and robust. It is justified for various size users and suitable for many different roles of users. The most advantage of this method is the reduction of burden and memory usage in cloud based access authentication of client.

Yaser et al. [31] proposed a very secure authentication scheme known as the Kerberos authentication with role-based access control for cloud services. This system provides efficient authentication as well as high robustness. This system is design and developed using C# and implemented using Amazon S3 cloud storage. The simulation performance of this model is analysed in terms of multi-user creation and many-role creation. This system provides efficient role assignment even though rapid increments in user and role counts. This paper gives the concept of flexible and an effective distributed system with dynamic data support including Kerberos authentication service. The only drawback of the proposed system is that the performance is little bit slower due to extra overhead.

David et al. [32] have proposed privacy-preserving, identity management system with proxy re-encryption using OpenID for cloud environment. The OpenID attribute exchange is used for identity management, and the proxy re-encryption method is used for cryptographic encryption. In this paper true privacy preservation has been achieved by the concept of the proxy re-encryption i.e. identity provider delivers attributes to other users without reading their values. This prototype implementation is performed using Java language. The identity management service is performed with the help of OpenID4 java library and proxy re-encryption scheme is implemented using the jPBC library. This whole simulation is performed on Apple Macbook Pro laptop with 2.66 GHz intel core 2 duo processor and 4GB RAM, operating on MAC OS X 10.6.8. The proposed method is able to transform encrypted information from the user to the service provider and also it reduces the memory consumption, but addressing user identity information and their authentication is the limitation of this method.

Nitin Naik and Paul Jenkins. [33] discussed the Federated Identity Management (FIdM), which is the most popular way to digitally identify the resources in cloud environment. The FIdM has three important standards: Security Assertion Markup Language (SAML), Open Authentication (OAuth) and OpenID Connect (OIDC). This paper presents the analysis of these standards on the basis of its architectural design, working principles, security strength, and security challenges. The conditions for analysis are suggested, and the functionalities of these standards compared with respect to the proposed conditions. Finally, a detailed comparative analysis of possible security vulnerabilities in the selection of an appropriate FIdM standard is presented.

VI. CREDIT VALUE AND ATTRIBUTE BASED ACCESS CONTROL (CAAC)

The credit value and attribute based access control is used to secure the resources in cloud environment. The ultimate aim of this technique is to encourage the reputed users and discourage the malicious users. In this technique the unintended behaviours of malicious users is detected and prevented their further action for privacy protection [20] in cloud environment. There exist various credit and reputation model [21], [22].

In recent years many researches are going on in this direction to develop an online application system based on credit and reputation model. Nowadays credit and reputation based applications are very popular in cloud environment. This application is also helpful in online financial transaction and online e-commerce marketing. Here, we discuss the conventional credit and reputation model and suggest few modification based on crowd reviewing.

A. Basic Design of Reputation and Attribute based Access Control Model

Here, we explain the basic principles of reputation and attribute based access control model [23].

1. Encourages Reputed Users:

The reputation and attribute based access control model is designed to encourage the good users. In this model a credit value is assign to user on successfully completion of every task. The users, who properly utilise the resources of cloud computing environment and does not perform any malicious activity gets the higher credit value. If the user continuously performs as good user then value of credit score will increase.

2. Discourages Malicious Users:

The reputation and attribute based access control model is designed to restrict the malicious behaviours of wicked users. This model safeguards the honest users and cloud resources. To discourage malicious user this model immediately reduces the credit value, if any user performs the unintended activity and if the users credit value is below the threshold value then user won’t be able to access any resources from cloud environment.

3. Credit Computation:

The credit computation is most important feature of reputation and attribute based access control model to ensure the security in cloud environment. This system assigns a positive or negative credit value to users on each and every activity of the users.

When user performs any upright activity then system appends positive credit value to its initial credit value and on every malicious action it appends negative credit value. The reputation and attribute based access control model utilises this credit value to restrict the malicious user from accessing the cloud resources.

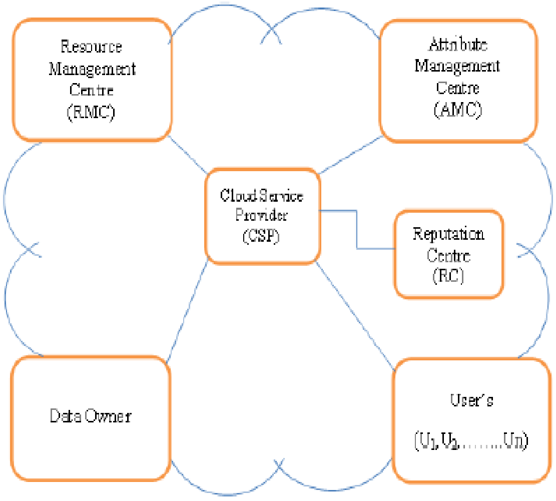
Resource Management Centre (RMC)
Attribute Management Centre (AMC)
Cloud Service Provider (CSP)
Reputation Centre (RC)
Data Owner
User's
$(U_1, U_2, \ldots\ldots U_n)$

Fig. 1.Reputation and Attribute based Access Control System

B. Credit Value and Attribute based Access Control System (CAACS)

This credit value and attribute based access control system (CAACS) is based on crowd feedback mechanism of credit value for securing the cloud resources by authenticated users. In this technique after any transaction every user gives the feedback to reputation centre in term of credit value. As shown in Figure 1 the modified reputation and attribute based access control system contains mainly three sub systems: Attribute Management Centre (AMC), Resource Management Centre (RMC) and Reputation Centre (RC).

1. Attribute Management Centre (AMC)

The attribute management centre is very important sub system of the credit value and attribute based access control system. This is responsible for maintaining the all attributes of users. When any user wants to access any resources in the cloud environment, the attribute management centre grant the permission on the basis of its attributes. So any users have to must register with the attribute management centre as a legitimate user. The attribute management centre works on the basis of users attribute. It provides the identification and authentication services to users.

2. Resource Management Centre (RMC)

The first step is every user has to register with the attribute management centre. After successful registration the reputation centre will assign the initial credit value to user. Now user can login to the system to access the resources with the resource management centre. When the user login to the system, it is the responsibility of the resource management centre to check the users credit value and verified it from reputation centre, if the credit value is lower than the threshold value then user will not get the access permission. If the users credit value is above the threshold value and successfully authenticated then user can now access the resources. The resource management centre continuously checks the users credit value and keeps control the users rights for accessing the resource in the system.

3. Reputation Centre (RC)

The reputation centre is the most important part of the modified reputation and attribute based access control system. The reputation centre is responsible for monitoring all the resources access by the user and calculation of latest credit value of the user. The reputation centre receives the feedback credit value from all connected users and calculates the latest credit value for that user. The reputation centre also updates the credit value to the attribute management centre.

VII. SIMULATION EXPERIMENT

We construct a simulation environment in cloudsim to demonstrate the credit value and attribute based access control model for cloud environment. In this simulation, firstly we analyse the users behaviour and then evaluate the users credit value on the basis of his behaviour genuineness. The execution of transaction process in our simulation experiment, between users and cloud service provider (CSP) is shown in figure 2 with the help of sequence diagram. We have taken three components: Users, Cloud Service Provider (CSP) and Reputation Centre (RC).

i. Users: The User requests the cloud resources or services from cloud service provider (CSP) or other Users.

ii. CSP: The cloud service provider entertains the Users with their requests. All users have to register themselves with the CSP. On successful registration by users with all attributes the CSP initialises its credit value.

iii. RC: The reputation centre is responsible for monitoring all the resources access by the user, and calculation of the credit value of each user. It provides the current credit value to CSP and Users for access protection in transaction between Users and CSP. The sequence diagram of transaction is shown in Figure 2. This can be explain in following steps:

Step 1: A User broadcasts a message Ask4Resource to the CSP and its all users available in simulated cloud system. In this message user requests its required resources.

Step 2: The Users who have the requested resource will reply IhaveResource message to the User through CSP.

Step 3: If there is not a single reply message received in the fixed time interval then repeat step 1.

Step 4: If there is only single reply message received then CSP will enquire RC for the latest credit value of the user by sending the Ask4CreditValue message and the RC will reply the latest credit value with message CreditValue. If the credit value is less than the threshold, then CSP will deny the service from the user, and go to step 1; otherwise, CSP will connect to user for further trade.

Step 5: If there is many reply messages received then CSP will enquire RC for the latest credit values of the Users, and the RC will respond the credit value with message ReturnCreditValue. After receiving all the credit values, CSP will select the User with the highest credit value. If the credit value is less than the threshold value, then CSP will deny the service, and go to step 1; otherwise, CSP will connect to the User for further trade.

Step 6: When CSP connects to the User for resource request, the User will send a RequestResource message to CSP, and wait for response.

Step 7: When CSP received a RequestResource message from User, CSP will again enquire RC for the latest credit value of the User, and the RC will respond the latest credit value with message ReturnCreditValue.

If the value is less than the threshold, then CSP will deny the request from the User; otherwise, CSP will reply a ResourceReady message to the User.

Step 8: The transaction process started between the User and CSP.

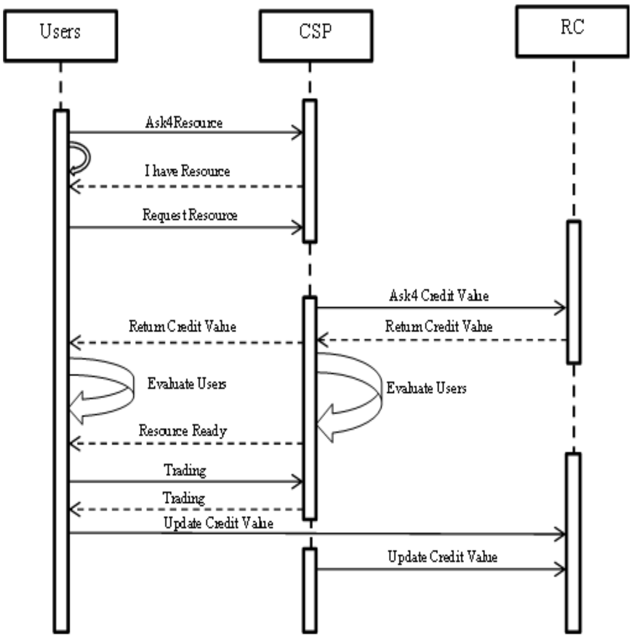

Fig. 2.Sequence Diagram for Transaction between Users and CSP

Step 9: After the transaction process, all other Users and CSP will feedback the credit value to RC for further usage.

Step 10: When RC receives the feedback credit value of the User and CSP, it will calculate and store the latest credit value of the User for future use.

A. Type of Users in Cloud Environment

There exist different types of users in the cloud environment, for simplicity we consider mainly two categories i.e. consistent user and inconsistent user.

i. Consistent User (CU): The consistent users are the honest users. They strictly follow the rules regulation of the cloud computing environment.

ii. Inconsistent User (IU): The inconsistent users are irresponsible user; they don’t strictly abide the cloud environment rules. The inconsistent user sometime behaves properly to gain high credit value and may perform malicious activities in the cloud environment

B. Credit Value Computation

In the simulation experiment of the proposed credit value and attribute based access control (CAAC) model two types of users considered. Among all the transactions between Users and CSP, we mainly consider the two main parameters which are the Success-Ratio and the Average-Credit-Value of users.

(i) Success-Ratio: The Success-Ratio is defined as the ratio of successfully completed transactions and total transactions in the cloud environment:

$$\text{Success Ratio} = T_{\text{success}} / T_{\text{total}} \qquad (1)$$

(ii) Average-Credit-Value: The Average-Credit-Value is the average value of individual credit values of all users.

$$\text{Average Credit Value}=\sum i=1:N \sum j=1:N(C_{i,j})/N_t \qquad (2)$$

where N and N_t is Total No. of users and specific type users respectively.

C. Result Evaluation

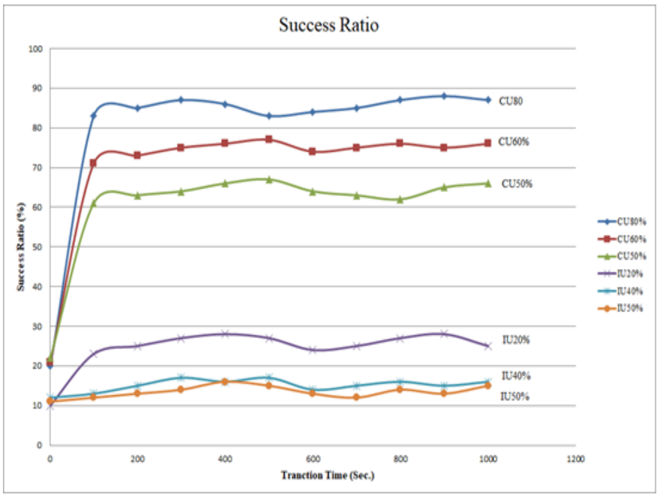

Fig. 3. Succes-Ratio Graph of Consistent and Inconsistent Users

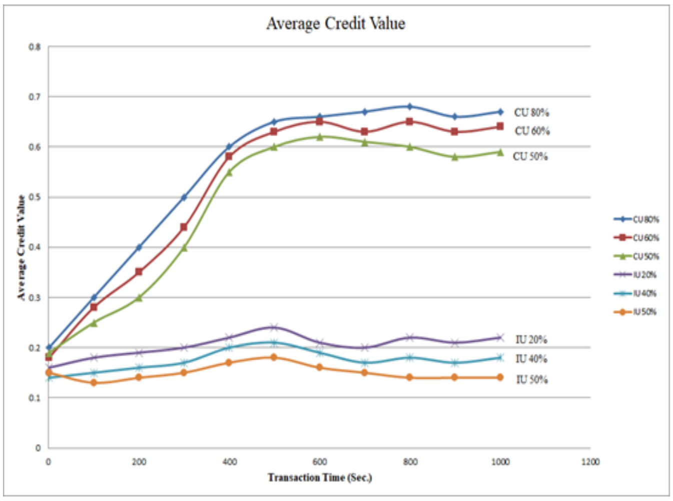

Fig. 4.Average Credit Value Graph of Consistent and Inconsistent Users

This cloud environment simulation is performed with the help of cloudsim, In simulation experiment we have taken N=2000, which means there are total 2000 users. In which there are two types of users: the Consistent User (CU) and the Inconsistent User (IU). In this simulation, each user performs 1000 transactions with another user. The main aim of our simulation system is to evaluate the ability of the CAAC system against Inconsistent User (IU). So in our simulation system we just consider the implementation of Consistent (CU) and Inconsistent User (IU) for following three different cases. This is also shown in figure 3 and figure 4:

(i) Case1: CU=80 % and IU=20 %

(ii) Case2: CU=60 % and IU=40 %

(iii) Case3: CU=50 % and IU=50 %

In this simulation result of the reputation and access control method we find the Success-Ratio and Average Credit Value for consistent user is very high than inconsistent user. As the number of inconsistent users increases in the system the Success-Ratio and Average Credit Value for inconsistent user is far below the threshold value.

VIII. Conclusion

The credit value and attribute based access control system provide the security to consistent users in cloud environment. It protects the illegal access of cloud server from malicious users. The simulation experiment graph shows that the success ratio and average credit value of consistent users is much higher than the inconsistent users. So this system restricts the malicious user’s access of resources, since its success ratio and average credit value is much lower than threshold value. This system encourages the consistent or honest user by increasing their credit value and discourages the inconsistent or dishonest user by decreasing their credit value. In future the credit value computation mechanism can be improved by using the crowdsourcing concepts.

REFERENCES

1. Ronggong Song, Larry Korba, and George Yee,” Pseudonym technology for e-services,” In Privacy Protection for E-Services., *IGI Global,* 2006 , pages 141–171.
2. Andrea Miconi, Lee rainie & barry wellman, “networked: The new social operating system,” *International Journal of Communication,* 7:6, 2013.
3. Abhishek Tripathi, Nargess Tahmasbi, Deepak Khazanchi, and Lotfollah Najjar. Crowdsourcing typology: a review of is research and organizations. Proceedings of the Midwest Association for Information Systems (MWAIS), 2014.
4. BoyangWang, Baochun Li, and Hui Li. Oruta: Privacy-preserving public auditing for shared data in the cloud. IEEE transactions on cloud computing, 2(1):43–56, 2014.
5. Sini Ruohomaa, Lea Kutvonen, and Eleni Koutrouli. Reputation management survey. In The Second International Conference on Availability, Reliability and Security (ARES’07), p ages 103–111. IEEE, 2007.
6. Pierangela Samarati and Sabrina Capitani de Vimercati. Access control: Policies, models, and mechanisms. In International School on Foundations of Security Analysis and Design, pages 137–196. Springer, 2000.
7. Ravi Sandhu and Pierangela Samarati. Authentication, access control, and audit. ACM Computing Surveys (CSUR), 28(1):241–243, 1996.
8. Cornelis Jan Leune et al. Access control and service-oriented architectures. Technical report, Tilburg University, School of Economics and Management, 2007.
9. Xu Chen, Damon Berry, and William Grimson. Identity management to support access control in e-health systems. In 4th European Conference of the International Federation for Medical and Biological Engineering, pages 880–886. Springer, 2009.
10. Alan H Karp. Authorization-based access control for the services oriented architecture. In Fourth International Conference on Creating, Connecting and Collaborating through Computing (C5’06), pages 160–167. IEEE, 2006.
11. Barbara Carminati, Elena Ferrari, and Andrea Perego. Rule-based access control for social networks. In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", pages 1734–1744. Springer, 2006.
12. Yuri Demchenko, Leon Gommans, Andrew Tokmakoff, and Rene van Buuren. Policy based access control in dynamic grid-based collaborative environment. In International Symposium on Collaborative Technologies and Systems (CTS’06), pages 64–73. IEEE, 2006.
13. Pavan Reddivari, Tim Finin, Anupam Joshi, et al. Policy-based access control for an rdf store. In Proceedings of the IJCAI-07Workshop on SemanticWeb for Collaborative Knowledge Acquisition, 2007.
14. Ravi Sandhu and Qamar Munawer. How to do discretionary access control using roles. In Proceedings of the third ACMworkshop on Role-based access control, pages 47–54. ACM, 1998.
15. Deborah D Downs, Jerzy R Rub, Kenneth C Kung, and Carole S Jordan. Issues in discretionary access control. In 1985 IEEE Symposium on Security and Privacy, pages 208–208. IEEE, 1985.
16. Jonathan M McCune, Trent Jaeger, Stefan Berger, Ramon Caceres, and Reiner Sailer, “Shamon: A system for distributed mandatory access control,” In 2006 22nd Annual Computer Security Applications Conference (ACSAC’06), pages 23–32. IEEE, 2006.
17. Joon S Park, Ravi Sandhu, and Gail-Joon Ahn. Role-based access control on the web. ACM Transactions on Information and System Security (TISSEC), 4(1):37–71, 2001.
18. Anelia Mitseva, Mohamad Imine, and Neeli R Prasad. Context-aware privacy protection with profile management. In Proceedings of the 4th international workshop on Wireless mobile applications and services on WLAN hotspots, pages 53–62. ACM, 2006.
19. Raouf Boutaba and Issam Aib. Policy-based management: A historical perspective. Journal of Network and Systems Management, 15(4): 447–480, 2007.
20. Yagiz Sutcu, Qiming Li, and Nasir Memon. Protecting biometric templates with sketch: Theory and practice. IEEE Transactions on InformationForensics and Security, 2(3):503–512, 2007.
21. Thanasis G Papaioannou and George D Stamoulis. Effective use of reputation in peer to-peer environments. In IEEE International Symposium on Cluster Computing and the Grid, 2004. CCGrid 2004., pages 259–268. IEEE, 2004.
22. Paul Resnick, Richard Zeckhauser, John Swanson, and Kate Lockwood. The value of reputation on ebay: A controlled experiment. Experimental economics, 9(2):79–101,2006.
23. Sun Donghong, LiuWu, Ren Ping, and LiuKe. Reputation and attribute based dynamic access control framework in cloud computing environment for privacy protection. In 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pages 1239–1245. IEEE, 2016.
24. Madhura Mulimani and Rashmi Rachh. Analysis of access control methods in cloud computing. 2016.
25. RajaniKanth Aluvalu and Lakshmi Muddana. A survey on access control models in cloud computing. In Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1, pages 653–664. Springer, 2015.
26. Yuri Demchenko, Canh Ngo, Cees de Laat, and Craig Lee. Federated access control in heterogeneous intercloud environment: Basic models and architecture patterns. In 2014 IEEE International Conference on Cloud Engineering, pages 439–445. IEEE, 2014.
27. Lan Zhou, Vijay Varadharajan, and Michael Hitchens. Trust enhanced cryptographic role-based access control for secure cloud data storage. IEEE transactions on information forensics and security, 10(11): 2381–2395, 2015.
28. Lan Zhou, Vijay Varadharajan, and Michael Hitchens. Secure administration of cryptographic role-based access control for large-scale cloud storage systems. Journal of Computer and System Sciences, 80(8):1518–1533, 2014.
29. Hella Kaffel-Ben Ayed and Bilel Zaghdoudi. A generic kerberos-based access controlsystem for the cloud.Annals of Telecommunications, 71(9-10):555–567, 2016
30. Santosh Khamitkar, Yaser Fuad Al-Dubai, Parag Bhalchandra, and Pawan Wasnik.Kerberos authentication with cloud computing access control.International Journalof Advanced Computational Engineering and Networking, ISSN, pages 2320–2106,2015.
31. Yaser Fuad Al-Dubai, SD Khamitkar, and Parag Bhalchandra. Kerberos authenticationwith role based access control model for cloud environment.International Journal ofEmerging Trends in Science & Technology, 2(1):1758–1767, 2015.

32. David Nunez, Isaac Agudo, and Javier Lopez.Integrating openid with proxyre-encryption to enhance privacy in cloud-based identity services. In4th IEEEInternational Conference on Cloud Computing Technology and Science Proceedings,pages 241–248. IEEE, 2012.
33. Nitin Naik and Paul Jenkins. Securing digital identities in the cloud by selecting anapposite federated identity management from saml, oauth and openid connect. In201711th International Conference on Research Challenges in Information Science (RCIS),pages 163–174. IEEE, 2017

AUTHORS PROFILE

Ajay Kumar Dubey is research scholar in computer science department of Dr. APJ Abdul Kalam Technical University, Lucknow, India. He received his B.E. (CSE) from Dr. B.R.Ambedkar University Agra, India in 2002 and M.E.(CSE) from Panjab University Chandigarh, India in 2009. His research interests include Image processing, Performance optimization of cloud application, trust and cloud security. He has published more than ten papers in national and international journals and conferences.

Dr. Vimal Mishra is director of Institute of Engineering and Rural Technology (I.E.R.T.), Allahabad, India. I.E.R.T. is a renowned engineering institute of northern region. He received his B.Tech. and M.Tech. degree from Kamla Nehru Institute of Technology, Sultanpur, India in 1991 and 2002 respectively. He received PhD from Indian Institute of Technology, BHU, Varanasi, India in 2010. He has guided many Ph.D. and M.Tech. theses in Computer Engineering. His research interest includes Machine Translation, Artificial Intelligence, Cloud Computing, Machine Learning etc. He has published more than fifty (50) peer reviewed research articles in national and international journals. He has published a book and 2 book chapters. He is also an editorial board member of International Journal of Computational Systems Engineering, Inderscience publications.

Retrieval Number: C5734098319/2019©BEIESP
DOI:10.35940/ijrte.C5734.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication