# Design and Implementation of Trust - based Access Control System for Cloud Computing

Hui Xia[1]
1. Software College,Shenyang Normal university
Shenyang, China
freund_xia@126.com

***Abstract*—Reasonable authorization and access control is one of the urgent problems that cloud computing applications need to solve, especially in the context of dynamic establishment of trust relationship between entities to study the open access security environment. This paper proposes a generation method of cross-domain access control strategy from trust evaluation to trust management. Based on the trust generation method of cross-domain access control policy, a trust-based access control system of cloud computing is designed and implemented. The system is mainly divided into four functional modules: credit evaluation module, trust relationship data mining module, trust management strategy generation module and access strategy implementation module. The main process, design and implementation method of the corresponding method are expounded. The access control file is verified, and the expected access control results are obtained.**

***Keywords—access control ； reputation assessment ； trust management；XACML***

## I. INTRODUCTION

At present, the advantages of cloud computing has been widely recognized, cloud computing become the main development direction of the global information industry, but cloud computing is still in its early development stage, is faced with many challenges and problems [1]. Because the user's trust boundary extends to the cloud service provider of security domain and the dynamic changing, the separation of data and infrastructure, and different from traditional IT outsourcing many tenants new features, such as information security become the biggest obstacle to the worldwide deployment of cloud computing, this also is in the field of cloud computing is one of the most pressing issues on its [2].

## II. RELEVANT TECHNICAL INTRODUCTION

### *A. User authentication and authorization*

User authentication and authorization for legitimate users to access to the system and access the data for the corresponding authorization [3]. Mainstream of cloud computing user authentication and authorization measures should have identity management and access authorization of user management, distributed environment and many factors authentication function, can provide personal information change password self-service Web interface and implementation, and unified identity authentication based on LDAP protocol will be dispersed to complete the unification, the user and the system access resources of through the centralized management, realize the user only use single sign-on can access to multiple system [4].

### *B. Access control model*

(1) Role-based access control model Role-based access control model is a non-autonomous access

The model is a non-autonomous access control model. In the role-based access control model, the user's role as the main access. Role-based access control model After the establishment of the system, the main task is to authorize or cancel a user's corresponding role. The model also has the advantage that the administrator of the system is at a similar level of abstraction than the management of the enterprise-related business [5].

(2) Trust management

The current mainstream trust management has two main aspects:The first is trust management based on access control policies and trust certificates, which correspond to rational trust or can be said that the objective of the trust relationship management;The second study is based on the credibility of the trust management, which corresponds to a trust management is a subjective or emotional trust management relationship.

(3) Attribute - Based Access Control Model

In the process of system operation, the attribute as a variable, but the strategy is relatively stable, attribute-based policy description can be a good way to attribute management and access to determine the phase separation[6].By introducing the middle element of the role, the role-based access control model can make the privilege be aggregated through the role first, then the authority can be assigned to the corresponding subject, which can simplify the authorization and regard the role information as an attribute , This will be based on the role of the access control model into a property-based access control model [7].

## III. TRUST - BASED CROSS - DOMAIN ACCESS CONTROL POLICY

*A. Reputation assessment and trust management*

It provides a method of generating cross-domain access control policy from trust evaluation to trust management. It can dynamically generate authorization policies according to the behavior and environment attributes of entities. It has good adaptability and can be applied to the cloud with large numbers of unknown entities Computing and other cross-domain environment[6].The method is realized by the following technical scheme, which comprises the following four processes:

(1) The credibility evaluation model is established, and the corresponding credit evaluation subsystem is implemented. Based on the evaluation information given by the interactive entity, the credibility of the evaluated entity is evaluated.

(2) According to the result of reputation evaluation, the association rules of attribute, attribute, behavior, environment and entity are extracted by using classification association rules mining method.

(3) According to the process(2)based access control policy, and uses Extensible Access Control Markup Language (XACML)described.

(4) The general access control policy generated in the process (3) is translated into the policy of the specific trust management system.

*B. The Design of Credit Evaluation Model*

The model is a non-autonomous access control model. In the role-based access control model, the user's role as the main access. Role-based access control model After the establishment of the system, the main task is to authorize or cancel a user's corresponding role. The model also has the advantage that the administrator of the system is at a similar level of abstraction than the management of the enterprise-related business [5].

The reputation T is a quantitative concept on the universe $U=[0,n]$ (n is an arbitrary positive integer), denoted by the reputation cloud $T(Ex,En,He)$. The credibility of the *Ex* cloud computing using Bayesian network, cloud drops corresponding to the root node Trust, each context information corresponds to a leaf node, the cloud droplet of the expected value is $Ex$. The value of cloud droplet r is n discrete values, and is expressed by $level_1, level_2, level_3 ... level_n$. There are m kinds of context information, each kind of context has the value of km. $C_{ij_i}(i \in \{1,2,3...,m\})$ is used to represent the j value of the i following, and the context information for each interaction is represented by element $C^{(C_{1j1},C_{2j2},...,C_{mjm})}$ .The integrity of the evaluation algorithm is as follows:

**Input**:An Evaluation Set R Containing Context Information

**Output**:The three parameters of the reputation cloud： $Ex, En, He$ ,Specific steps are as follows:

(1) All CPT are initialized to uniform distribution;

(2) The Bayesian network is updated with all the evaluations in R, The procedure is as follows:

**Step 1**. i=1

**Step 2**. The evaluation $r_i$ and the relevant context information C are read from $R$

**Step 3**. If required, the time decay process is initiated periodically and the CPT of the node "Trust" is updated using equation (1)

$$P(Trust = level_k) = \frac{1}{n}$$

$$P_{m+1}(Trust = level_k) = \frac{kP(m)(Trust = levelk) \bullet (1+\lambda) + \lambda}{m + (2 \quad m)\lambda} \qquad (1)$$

$\lambda = e^{En} \in [0,1]$ ,Where : $P_{(m)}(m \geq 0)$ is the probability of using the math round of attenuation; $\lambda$ is bad reduction factor; $E_n$ is the current entropy.

**Step 4**. The CPT is updated with the evaluation $r_i$;

**Step 5**. $i = i + 1;$

**Step 6**. Repeat step 2~5 until all the readings in $R$ are read.

(3) The probability of entity quality of service in $level_k$ in different contexts C is:

$$P(Trust = level_k \mid C), k \in \{1,2,...,n\} \qquad (2)$$

Calculate the expected value:

$$Ex = \sum_{k=1}^{n} P(Trust = level_k \mid C) \times k \qquad (3)$$

(5) Compute entropy in different contexts $C$:

$$En = \frac{1}{i}\sum_{j=1}^{i} |r_j - Ex_i| \quad , \qquad i \geq 2 \qquad (4)$$

(6) Compute super entropy in different contexts $C$:

$$He = \frac{1}{i}\sum_{j=1}^{i} \left| En_i - \frac{1}{i}\sum_{k=1}^{i} En_k \right| \quad , \qquad i \geq 3 \qquad (5)$$

Once the reputation cloud of each evaluated entity is obtained, the accuracy of the evaluated entity can be calculated. For each entity being evaluated, each entity that has evaluated it can use the reputation evaluation algorithm described above to calculate the reputation cloud of the entity [8]. The similarity of the two reputation clouds can be measured by the cosine distance of the three-parameter cloud of the evaluated entity and the reputation cloud given by the specific entity. The higher the similarity is, the higher the accuracy of entity evaluation is.

### C. The Mining of Trust Association

The association mining method mainly includes the following two steps:

**Step 1**. According to the credibility of the behavior of the entity, the relationship between the attributes, resource attributes, behavior attributes, environmental attributes and entity credibility of the evaluated entity is extracted.

**Step 2**. Then, the relationship between the attributes of trusted entities and attributes, resource attributes, behavioral attributes and environmental attributes of the evaluated entities are extracted. Then, the relationship between the trustworthiness evaluation entity and the evaluated entity is analyzed.

The classification item of the classified association rule mining method is the rank of the reputation degree of the behavior and the association rule of the reputation degree, and the non-classification item is the attribute and / or environment attribute of the related entity; the value of the reputation degree The interval is divided into a plurality of sub intervals, one for each sub interval.

The relationship between the two mining relationships are as follows:

(1) Entity Credibility Association Rule ID:(Evaluated entity attribute 1, evaluated entity attribute value 1),(Resource attribute 1, resource attribute value 1),(Behavior Attribute 1, Behavior Attribute Value 1),(Environment attribute 1, environment attribute value 1) → Credit rating.

(2) Evaluation Accuracy Association Rule ID:(Evaluate entity attribute 1, value 1) → Entity Credibility Association Rule ID.

The accuracy of association rules mining based on Apriori classification association rules mining algorithm, using (attribute, value) format.A non-categorical item is an attribute that evaluates an entity, and a categorical item is a corresponding reputation association rule identifier(Contains the evaluated entity attributes, environmental attributes, and reputation levels).

### D. An XACML description of the access policy

Attribute-based access control policies include two types of access control policies, one for each type of association, one for an entity that has a specific attribute, which allows or disallows access to resources with specific attributes under specific environment attributes. Another describes whether an entity with a particular attribute is allowed to recommend other entities with specific attributes.When the access control policy is described in the XACML language, each reputation association rule and the associated accuracy association rule are converted into a policy set, which comprises two policies with the entrusting relation, the <Target> field of the policy The attribute matching in the description of the association rules of the project.

The first policy describes the authorization of the entity recommendation (delegation) behavior, and is a credible management policy describing the attributes of the recommendation entity (policy publisher);The second policy describes the authorization of the entity access behavior, is a delegate access strategy.

### E. Transformation of Trust Management Strategy Based on XACML

Although the strategy of concrete trust management system expresses the authorization relationship in different custom formats, the three aspects of authorization, authorization and access are respectively related to the recommended entities, the recommended entities and the access entities in the general access control strategy Permissions corresponding to.And the generated XACML access control policy is transformed into the strategy of the typical trust management system dRBAC (distributed Role Based Access Control).

The dRBAC policy syntax defines the Subject, Object, and Issuer roles as Subject, Object, and Signer dRBAC does not give the specific meaning of the role of the format and syntax, by the application of custom.This system is represented by XACML syntax. It includes: the access entity attribute of the subject role, the resource attribute, the behavior attribute and the environment attribute of the Object role. The Signer role contains the recommended entity attribute.

Compared with the prior art, the method has the following beneficial effects:

(1) Mainstream access control technology is essentially identity-based authorization, can not meet the open cross-border environment, a large number of unfamiliar entities access needs.

(2) The existing trust management strategy is preset and can not achieve a finer granularity that dynamically reflects the behavior characteristics of specific application entities. With the help of the reputation evaluation results, only fine tuning can be done within preset limits.

(3) Using the standard Access Control Policy Language (XACML) to describe the generated policies, it can be easily transformed into other format policies to facilitate seamless integration with access control mechanisms in existing legacy systems.

## IV. SYSTEM DESIGN AND IMPLEMENTATION

### A. System Overview

Based on the cloud model and Bayesian network, the reputation system is represented and evaluated, and then the attributes of the evaluated entities are compared with the attributes, resource attributes and behavior attributes of the evaluated entities. Based on the evaluation results, , The relationship between environmental attributes of the relationship between the trust digging.And then generates the XACML access control policy based on the accuracy association rules and the associated reputation association rules.Finally, the XACML access control policy is transformed into the strategy of dRBAC and the access control is implemented. The prototype system is JavaWeb project based on JSP frame, the development platform EclipseJEEIDEv1.4,Web server Tomcat v7.0.

### B. System design and implementation

Trust-based cloud computing access control system is divided into four functional modules: reputation evaluation, trust mining, trust management policy generation, access control implementation.System architecture shown in Figure 1.

(1) Reputation Assessment Module,the main function is to combine the cloud model proposed by Academician LiYide and the Bayesian network to represent and evaluate the reputation, according to the original evaluation information, randomness, uncertainty and ambiguity. The uncertainty evaluation model of credit is established and implemented.The main work flow of the credibility evaluation module is shown in Figure 2.

(2) The main function of the trust relationship mining module is to extract the attribute of the evaluation entity, the attribute, the resource attribute, the behavior attribute, the environment attribute and the attribute attribute of the evaluated entity by using the classification association rule mining method according to the credibility evaluation result obtained by the previous module credibility evaluation module. Entity credibility of the relationship between the relationship. The process of trust relationship mining module is shown in Figure3.

(3) A trust management policy generation module is used to generate the attribute-based access control policy according to the association relationship obtained by the trust relationship mining module and describe it with the extensible access control markup language XACML.

(4) Access control implementation module, the main function is to trust management strategy to generate a common access control strategy into dRBAC(role-based distributed access control) trust management system strategy.The main data flow of the module shown in Figure 4.

## V. TEST RESULTS

The system is based on JSP Web applications, basically achieve a trust-based access control architecture. Below will be the system to verify the function of each module.

Click Credibility Assessment to enter the reputation assessment module system for reputation assessment. You need to fill in the parameters, and then read the stored CSA format of the original evaluation information file. After completing the relevant parameters, read the original evaluation information file and click on the "Start a reputation assessment" link to conduct a reputation assessment.

Click Re-conduct Reputation Assessment or the Next: Trust Relationship Mining link to perform a reputation assessment or start trust relationship mining. Here the evaluation ID input Value1, credibility threshold set to 2.0, trust relationship mining set to 0.8, click the "mining trust relationship" link to start mining the trust relationship, generate trust mining relationship results.

After clicking the Generate Trust Management Policy button, you can include the direct authorization policy and the indirect authorization policy (set). In the results page, click the "Rebuild Trust Management Policy" link or the "Next Step: Access Control Enforcement" link to re-drill the trust relationship or to implement the access control enforcement function.

The parameter behavior required for the access control implementation reputation threshold is set to 2 here. Access request file Select the file with the name set in advance to implement access control. At the same time, the file for saving the access control policy is directAuthPolicy.xml and indirectAuthPolicyFile.xml.After clicking the "Access Control Decision" button, the access is successful. And select the request_deny.xml file implementation of access control, then show access failure. According to the generated policy, different access control decision results are obtained by using different request files.

## VI. CONCLUSION

By studying the current status of access control in cloud computing security and summarizing the shortcomings of existing research technologies, mainstream access control technology is essentially an identity-based authorization that can not meet the access requirements of a large number of unfamiliar entities in an open cross-domain environment.In this paper, a trust-based cross-domain access control policy approach is proposed, and the generation of the method is described in detail. Finally, a trust-based cross-domain access control strategy generation method is presented, and a trust-based cloud computing access control system is designed and implemented.


## ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grant No.60970112, Natural Science Foundation of LiaoNing Province under Grant No.2014020118, and Liaoning Provincial Department of Education Science and Technology Project Fund under Grant No.L2014441.


## REFERENCES


[1] WINSBOROUGH W H, SEAMONS K E, JONES V E. Automated trust negotiation [C]// Proceedings of 2000 DARPA Information Survivability Conference and Exposition. Hilton Head:IEEE,2000:88-102.

[2] Zheng R, Chakraborty N, Dai T, et al. Automated Multilateral Negotiation on Multiple Issues with Private Information[J]. Social Science Electronic Publishing, 2016, 28(4):612-628.

[3] Baumann A, Peinado M, Hunt G. Shielding applications from an untrusted cloud with Haven[C]// Usenix Conference on Operating Systems Design and Implementation. USENIX Association, 2014:194.

[4] Cadenhead T, Kantarcioglu M, Khadilkar V, et al. Design and Implementation of a Cloud-Based Assured Information Sharing System[M]// Computer Network Security. Springer Berlin Heidelberg, 2012:36-50.

[5] Zou C, Deng H, Qiu Q. Design and Implementation of Hybrid Cloud Computing Architecture Based on Cloud Bus[C]// IEEE, International Conference on Mobile Ad-Hoc and Sensor Networks. 2013:289-293.

[6] Wu Y, Yang Y, Ouyang J. Implementation of Cloud-based Access Control and Resource Management System[J]. ICCSEE-13, 2013, 463-464:1630-1633.

[7] Chen M X. Design and Implementation of Information Management System Based on Cloud Computing Mode[J]. Applied Mechanics & Materials, 2014, 556-562:6685-6688.

[8] Qiang W U, Zuo Y L, Zhao X L. Design and Implementation of Agricultural Information System Based on Cloud Computing[J]. Journal of Anhui Agricultural Sciences, 2014.

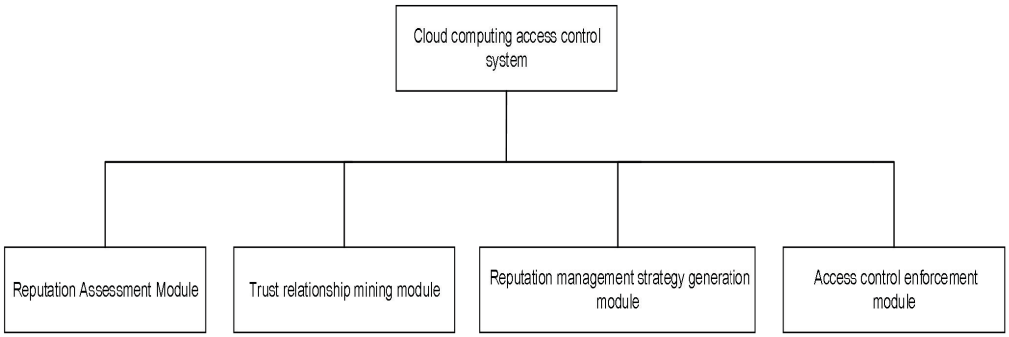


Fig. 1. System frame diagram

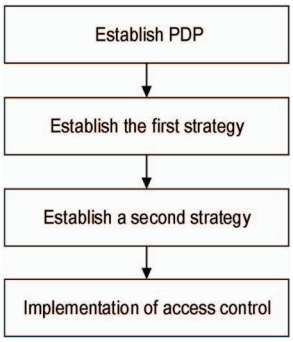


Fig.4 System frame diagram

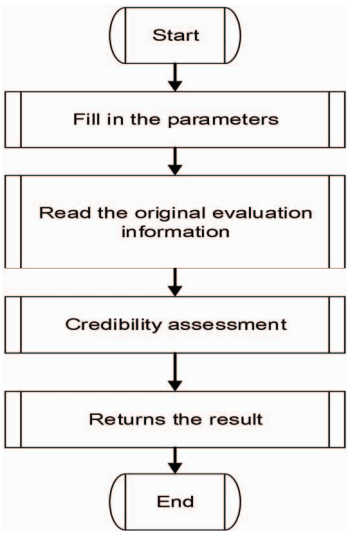


Fig.2 Credit Evaluation Module Flow Chart

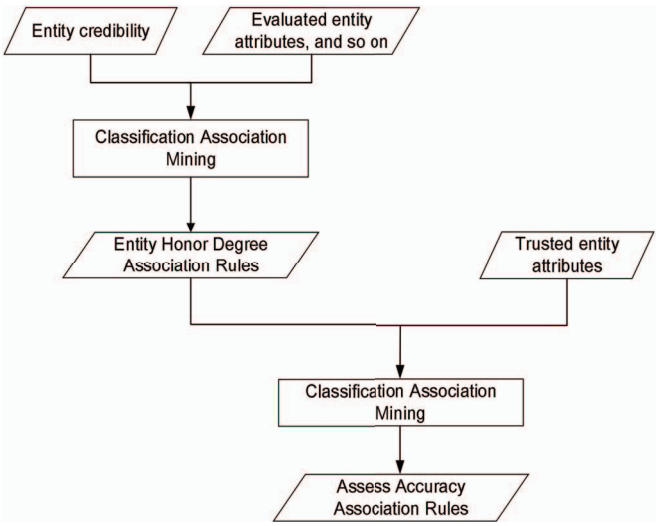


Fig. 3 Trust relationship mining module processing flow