Cloud services trust model based on the non-interference theory

Yang SU [1,a] Hong an XIE [1, b *], Dong LI [2,c]

[1] Electronics department engineering university of Chinese armed police forces

key laboratory of CAPF for information security Xi 'an china.

[2] Information engineering department Engineering University of Chinese Armed Police Forces

[a]suyang75@163.com,[b]15529332695@163.com, [c]563783912@qq.com

Keywords: Cloud services; trusted model; behavior trust; non-interference theory;

Abstract. In order to solve the security problem of resource sharing in cloud services environment. A new cloud services model NICTM (non-interference cloud services trust model) has proposed. Model formally defines the trusted domain and basic elements of cloud service environment and improves the traditional non-interference theory. Formally proof the domain is trusted when it satisfied non-interference conditions. The model was established by logic reasoning and independent of traditional actual security mechanism. So a trust cloud services system can be realized by any practice mechanism which satisfied the conditions of NICTM.

0 Introduction

Cloud service is facing the resource sharing security threat [1]. Cloud service improves the resource utilization ratio by sharing the resources. But a malicious user can bypass the logical boundaries to threat the security of the normal cloud users. One solution is to build trusted cloud [2].Similar scheme [3] has made some improvement. But due to the multi-domain virtualization in the cloud service environment, it is difficult to realize real time and dynamic trust measurements. Zhou[4] Put forward a kind of Tree trusted measurement model TSTM, judge the trusty of user domain by real-time integrity measuring of system. And Zhang [5] Are put forward, a trusted domain inheritance model based on the theory of the noninterference, it gives the formalization of trusted domain behavior and prove that the security isolation between the virtual machine and system to be trusted.

According to the above problem, this paper presents a cloud services behave trust model based on non-interference theory （non-interference cloud services trust model NICTM）

1 The definition of trust

TCG defined a state of computing platform is trusted: A state of computing platform is trusted when its behavior is in line with the trust strategy [6]， So the trust evaluation of the cloud service state affected by the behavior of user domains. Due to the state of domain is unlimited in practice, it is not feasible to measure each behavior state, for that reason we need to convert the trust evaluation of the state into a trust evaluation of domain's historical action sequence. So, the basic principle of a trust cloud service can conclude below:

Definition 1 state S is trusted when satisfy the following conditions (cloud service system trusted conditions)

（1） S_0 is the initial state and S_0 is trusted.

（2） S_0 can reach to the state S through a series of state transition

（3） The sequence of state transition is trusted.

The above definition is sufficient conditions; it can be taken as the basis for trust decision. This definition accord with the trust definition of the system which proposed by TCG .We uses trusted boot and integrity measurement to ensure the initial state S_0 is trusted and the purpose of this paper is proposed a kind of method to ensure the sequence of state transition is trusted.

1.1Non-interference theory

The Non-interference theory define the system security strategy by analyses the system behave and information flow between different entity. The non-interference theory can be described like this: Non-interference theory define a "delete" function. Then use the function to handle the domain's action sequence to clear away the action from the sequence which is non-interference the domains. After that if we observe the output of the action sequence before and after "delete", we can find out whether a latent interference between the domain and process existed in the action sequence. Non-interference theory defined a verification method which provides a way to verify the security of an information system.

2Basic symbol definition

To realize purpose model reference the literature [5] non-interference model. Model definition of symbol is given below.

Definition 2 cloud service environment $M=(S,D,A,O,P)$ is composed of:

S: set of states of M, $s_1,s_2,s_3...s_n$ denote element, s_0 is initial state.

D: set of domains , user process is running in the user domain, $d_1,d_2,d_3...d_n$ denote element.

A: Set of actions, domain can cause an action to change the state of cloud service environment, $a_1a_2a_3...a_n$ denote element. A^* is sequence of action, $\alpha_1\alpha_2\alpha_3...\alpha_n$,denote element.

O: Set of outputs, because M is composed of several D ,the outputs of M actually compose of the output set from running domains.

P: Set of process, process is running in user domain, $p_1,p_2,p_3...p_n$ denote element. P^* is sequence of process, $\rho_1,\rho_2,\rho_3...\rho_n$ denote element.

Definition 3 set of functions

1) Domain map function

$dcomp: D\times A\to P$, function decomposes the domain and the action to the process running in the domain

2) Action conversion function

$deact: S\times A\to D\times P$, function convert the state and the action to the domain and the process running in the domain , the action conversion function do not change the outputs of the action.

3) Action response functions

$sstep: S\times D\times A\to S$, Gets state when an action is applied. $soutp: S\times D\times A\to O$, Gets results returned by action.

4) Action sequence response functions

$dstep: S\times D\times A^*\to S$, Gets next state when action sequence is applied.

$doutp: S\times D\times A^*\to O$ get results returned by the sequence action "Λ" is used to denote the empty sequence, and "$\circ$" is used to denote the concatenation. For the definition above we can get following formula:

$dstep(s,d,\Lambda)=s$, $dstep(s,d,a)=sstep(s,deact(s,a))$, $dstep(s,d,a\circ\alpha)=dstep(sstep(s,d,a),d,\alpha)$

$doutp(s,d,a\circ\alpha)=soutput(s,d,a)\bigcup doutput(s,d,\alpha)$

Definition 4 Set of binary relations

1) "$\cong$" is used to denote the equivalence between members of domains, and $s_1\cong s_2$ denote when monitoring domain apply an action to observe the state of M the s_1 is equal to s_2。

2) Interference relation, "~>" Interference relation with reflexive , p_1 ~> p_2 denote p_1 interference p_2, and the state is changed from the perspective of monitoring domain, when the interference action is applied, at the same time if p_1 ~> p_2 we can get p_2 ~> p_1,and d_1 ~> d_2 denote d_1 interference d_2 ,while $\not\sim>$ denote noninterference.

3 Security analysis of NICTM

NICTM model give the trust conditions a trusted domain need to be followed, and formally proved the user domain which follow the restraint condition is trusted.

Definition 5(delete function) if $\forall d \in D$, $p \in P$, and $\alpha \in A^*$, define "delete" function $delete(d,\alpha): D \times A^* \to A^*$, $p \in d$ as

$$delete(d,\Lambda) = \Lambda \quad delete(d, a \circ \alpha) = \begin{cases} a \circ delete(d,\alpha) & \text{if } dcomp(d,a) \sim> p \,||\, dcomp(d,a) \sim> d \\ delete(d,\alpha) & otherwise \end{cases}$$

Interference relationship indicates that information flow is existed between domains. But noninterference theory focuses on the unexpected and illegality interference, so the purpose of introducing the "delete" function is to get rid of the legal interference between domain and process, by comparing before and after "delete" of action sequences to judge whether there is potential interference relationship between process and domains.

3.1Basic principle of behave trust

A user domain d is trusted when satisfying the following condition:

$$soutp(dstep(s,d,\alpha),a) = soutp(dstep(s,delete(d,\alpha)),a)$$

The system *M* start form state s_0 ,and after a sequence of action α is applied get to state $dstep(s,d,\alpha)$, at same time the monitoring domain apply an action a to observing the state of *M*. If there is no difference between the sequence of action and the sequence after "delete", it proof that there are no latent interference relation existed in the sequence, so the user domain d and the process running in this domain are trusted. Otherwise it's not trusted.

3.2Trusted properties of NICTM

There will be four properties as follows if the user domain is trusted.

Definition 6 Observational equivalence for a cloud service system, $s_1 \cong s_2$ indicate that s_1 equal to s_2 when the monitoring domain observe the system.

Definition 7 Result isolation, a user domain has result isolation properties when it satisfied the following condition:

d is a user domain, so $s_1 \cong s_2 \Rightarrow soutp(s_1,d,a) = soutp(s_2,d,a)$

If a domain satisfied result isolation when they start from the same state, applying the same action can get the same result.

Lemma 1 If cloud service system have property of observational equivalence result isolation, the domain d is trusted when satisfied the following condition:

$$dstep(s,d,\alpha) \cong dstep(s,delete(d,\alpha)) \tag{1}$$

Proof:

$\because dstep(s,d,\alpha) \cong dstep(s,delete(d,\alpha))$ $\quad\quad$ $\because s_1 \cong s_2 \Rightarrow soutp(s_1,d,a) = soutp(s_2,d,a)$

$\therefore soutp(dstep(s,d,\alpha),a) = soutp(dstep(s,delete(d,\alpha)),a)$

Satisfied domain trust conditions, proof are complete.

Definition 8 Non-interference isolation， $dcomp(d,a) \not\sim> d \Rightarrow s \cong sstep(s,d,a)$

Definition 9 Step isolation， $s_1 \cong s_2 \Rightarrow sstep(s_1,d,a) = sstep(s_2,d,a)$

By the above definition domain behavior credible theorem can be derived

Theorem 1（Domain behavior trust theorem）A user domain is trusted when satisfied four properties observational equivalence, result isolation, non-interference isolation and Step isolation.

Proof: if domain d satisfied the properties above, the equality below have to be proved.

$$s_1 \cong s_2 \Rightarrow dstep(s_1,d,\alpha) \cong dstep(s_2,delete(d,\alpha)) \tag{2}$$

Do a mathematical introduction on the length of sequence α .

When $\alpha = \Lambda$, eq. (2) holds.

If eq. (2) hold when the length of sequence α is n .

Then when the length of sequence α is $n+1$， there is $\alpha_2 = \alpha \circ a$， Substitute eq.(2).

Left: $dstep(s_1, d, \alpha_2) = dstep(s_1, d, \alpha \circ a) = dstep(sstep(s_1, d, a), d, \alpha)$ (3)

Right: $dstep(s_2, delete(d, \alpha_2)) = dstep(s_2, delete(d, \alpha \circ a))$ Classified discussion:

Case 1 $dcomp(d, a) \sim> p \,||\, dcomp(d, a) \sim> d$

By definition of the "delete" function

$dstep(s_2, delete(d, \alpha \circ a)) = dstep(s_2, a \circ delete(d, \alpha))$

Exist: $dstep(s_2, a \circ delete(d, \alpha)) = dstep(sstep(s_2, a), delete(d, \alpha))$

Because domain d satisfied step isolation

$sstep(s_2, a) \cong sstep(s_1, a)$ (4)

And by the assumption before

$dstep(s_1, d, \alpha) \cong dstep(s_2, delete(d, \alpha))$ (5)

So eq. $dstep(s_1, d, \alpha_2) \cong dstep(s_2, delete(d, \alpha_2))$ hold,

Case 2 Otherwise

By definition of the "delete" function, $dstep(s_2, delete(d, \alpha \circ a)) = dstep(s_2, delete(d, \alpha))$

Because domain *d* is satisfied the property of non-interference isolation. We can get $s \cong sstep(s, d, a)$

In summary: $\because s_1 \cong s_2 \therefore s_2 \cong sstep(s_1, d, a) \therefore dstep(sstep(s_1, d, a), d, \alpha) = dstep(s_2, delete(d, \alpha))$

From the above simplification to

$dstep(s_1, d, \alpha_2) \cong dstep(s_2, delete(d, \alpha_2))$, proof is complete.

For case 1, 2 it is to know when the sequence length is $n+1$, eq. (2) holds, by mathematical induction for the sequence of arbitrary length, eq. (2) holds. Proof completed.

Theorem 1 gives the conditions a trusted user domain needs to follow, and proof the domain which satisfied the conditions is trusted.

4 Summary

This paper proposed a NICTM model based on non-interference theory. Model introduces the traditional non-interference theory into cloud environment. The model is formally described and abstracts the elements of a cloud service environment. It gives the cloud service system trusted conditions and trust properties of a user domain, and formally proofs the security of the domain which satisfied the conditions. So the real system which satisfied the model can proofs it is trusted

References

[1]. DING Yan, WANG Huai-min, SHI Pei-chang, et al. Trusted cloud service [J]. Chinese Journal of Computers, 2015, 38(1): 133-149.

[2]. FENG Deng-guo, ZHANG Min, ZHANG Yan, et al. Study on cloud computing security[J]. Journal of Software, 2011, 22(1): 71-83.

[3]. BUTT S, LAGAR C, SRIVASTAVA A. Self-service cloud computing[C]//Proceedings of 2012 ACM Conference on Computer and Communications Security. New York USA, 2012: 253-264.

[4]. ZHOU Zhen-ji, WU Li-fa, HONG Zheng, et al. Trustworthiness measurement model of virtual machine for cloud computing[J]. Journal of Southeast University, 2014, 44(1): 45-50.

[5]. ZHANG Lei, CHEN Xing-shu, LIU Liang, et al. Trusted domain hierarchical model based on noninterference theory[J]. The Journal of China Universities of Posts and Telecommunications, 2015, 22(4): 7-16.

[6]. GRAEME P, CHEN Li-qun, DALTON C. Trusted computing platforms[M]. London: Springer, 2014: 1-25.