International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.375-388
http://dx.doi.org/10.14257/ijsia.2014.8.6.32

A Security Assessment Framework and Selection Method for Outsourcing Cloud Service

Xiaochen Liu[1], Chunhe Xia[1], Jiajin Cao[1], Jinghua Gao[1] and Zhao Wei[2]

[1]*Beijing Key Laboratory of Network Technology, School of Computer Science and Engineering, Beihang University, China,*
[2]*Lenovo Corporate Research & Development, Subsystem Research Lab,China*
ann4498@sina.com, xch@buaa.edu.cn, cdoublej@126.com, jhgao09@gmail.com, wz@cse.buaa.edu.cn

Abstract

Cloud services have become state of the art of resource sharing and interoperability among different service providers. The federated cloud seek to reduce costs and maximize efficiency, provide flexible and reliable services composed of various external cloud service and internal services, but this would introduce a risk of security due to outsourcing. For organization which provide an integrity cloud service must rely on SLA to illustrate the capacity of risk and performance, the various providers involved in the federations or services compositions should effectively distribute the organizational responsibilities and SLA. To solve the fears and deal with the threats associated with outsourcing, new method for selection of outsourcing cloud service providers(CSP) based on assessment of security and performance is urgently needed. This paper presents an approach on how to select the proper CSP to guarantee organizational SLA, which quantify the SLA terms and calculate a security weight, the organization can choose the appropriate CSP based on security weight, meanwhile minimize the business cost. This paper make contribution on modeling the capacity of the CSP, considering the business cost and historical performance. The proposed approach is validated through case study that shows selected CSP through our approach can best meet the organizational security and cost needs.

Keywords: *Cloud computing, SLA, QoS , Security, Risk, Trust*

1. Introduction

Cloud computing provides a way to increase the service efficiency, dynamic allocate resources and decrease the business IT cost. In order to achieve offering on-demand and scalable service manner, the cloud organization need some cloud service provider to apply some specific minimal services. To put it simply, cloud service is outsourcing, many cloud service providers would participate in the federated cloud to maximize the efficiency and flexibility. For example, communication services outsource message service which is supplied by various CSP [2]. However, outsourcing introduces the threat of security, the responsibility for implementing and maintaining efficient organizational security mechanisms will be in the hands of the outsourcing providers.

To mitigate the security risk associated with the cloud, organizations must rely on service level agreements (SLAs) to assess cloud provider security offerings, and make objective comparisons between different service offerings. The performance constraints can be expressed as service description terms (SDTs) and service level objectives (SLOs). SDTs

ISSN: 1738-9976 IJSIA

describe the functional service which cannot be expressed by numerical value, SLOs are some exact values which define the allowable ranges that the service can operate within it, stand for the quality of service and quality of security assurance. To overcome the fear of the outsourcing, the organization need to convince their customers that their external providers would guarantee the data security and applications will be properly operated. This can be resolved by SDTs and SLOs which assure the cloud can be served as SLA defined. Our work focus on quantifying the SDTs and combine with SLOs to calculate a risk weight for assessing the performance of the candidate provider.

Outsourcing implies the bidirectional trust relationship. With emerging federated cloud services, this situation describes a chain of transitive trust. From the organization perspective, the notion of trust can be increased via getting better performance when choosing the outsourcing CSP, for example, the outsourcing provider can greatly mitigate the risk via privacy protection and security measure which increase the trust and confidence between organization and outsourcing CSP. So we not only consider the risk perspective when choosing the proper CSP, but also take trust weight into account, which represents the historical performance of a service node that are evaluated from neighbor nodes. The trust weight and risk weight are connected with each other, and then aggregated a security weight, which describes the capacity of the specific service provider about how to accomplish service.

But we also have to be aware that how to reasonable control the business cost of the specific service is another important issue to be considered. Organization is willing to choose low cost and high reliability outsourcing services, abandon services which are pursuing high performance and security but the cost is extremely large. So our approach struggle to balance the proper business cost and the security, and then to select the adequate outsourcing CSP.

Our previous work did some research on service level agreement, current SLA specifications focus on quality of service and lack security service terms [1]. [2] developed the traditional SLA specifications, WS-Agreement, which allow security constrains to be expressed over the SDTs and SLOs, but it is still a difficult problem about making standard examination of security across various CSPs. [3] enabled CSPs to express their security offerings, increased the likelihood an organization would use their service, but it focus on the extension WS-Agreement schema and make comparison based on historical log record, which has limits on objective [5]. Gave a pair wise matchmaking algorithm could provide a least risk service selection that best met organizational needs, but which did not consider the trust of neighbor node. The current work about selection of service provider did not focus on the relationship between the cost and security or performance [4].

In this paper, we develop a selection method that, given a set of security SLA terms, calculates and ranks by quantitative evaluation algorithm, and obtain a set of trust weight from other connected service providers, aggregate them into a security weight. The result allows organizations to identify where service term match their requests and where compliance gaps might exist under the business cost constraints, and ultimately select the outsourcing cloud services that best meet their security or performance needs. Our quantitative evaluation algorithm examines the candidate services at runtime and is applicable to any service quantitative evaluation scenario involving security and cost, most importantly, this algorithm can updates the security evaluations as SLA changes propagate back to the organization, and this allows for organization-to-CSP matchmaking for choosing adequate outsourcing CSP in federated cloud scenarios.

The rest of the paper is organized as follows. In Section 2, we give a motivation scenario about our approach. Section 3 specifies the framework of selection method. Section 4

describes the research about quantifying security assessment. Section 5 validates our method through a case study. Section 6 concludes the paper.

2. Motivation Scenario

Organization would supply a part of service and others would be applied by outsourcing CSPs. We take Unified Communication (UC) as an example; we illustrate it in Figure 1. UC enterprise as organization often contained four types of communication service, communication service, voice service, message service and conference service. UC enterprise can offer only communication service, and use agreements with external service providers for delivery of additional services, such as email or video conference. So how to select the proper CSP provide other specific service?

A solution would offer the possibility to have different services available for different requirements, as well as support for guarantee the organization's request. Organization want to select outsourcing CSP which is both excellent in security and performance, but also under a reasonable cost. For example, D is the most consistent with organizational video requirement, but the cost of A would be as much of 10,000$. An offering service have not better performance than A, but cost would be about 8,000$, organization would consider a as their first choice if the difference of the performance can be accepted. UC provider can select the best proper message and conference service CSP with well performance and cost from all candidate CSPs.

So a method to solve the gap between organization and CSP is essential important. Organization can find the suitable CSP to satisfy their SLA, minimize the business cost through this method.

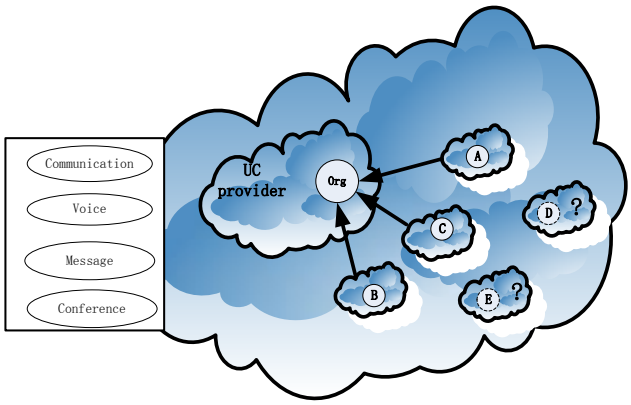

Figure 1. An Example Scenario of UC Provider

In above case, organization's video service be supplied by external CSP A, but A also outsource this service to P1, and which distributes parts of video service such as mobile or fixed telephony service to other CSP, as P2 and P3. P4 would apply some operation to P3 as to complete P3's service. So this scenario becomes a chain of federated CSP, and each CSP must face to select the best candidate for cooperation as Figure 2 described.

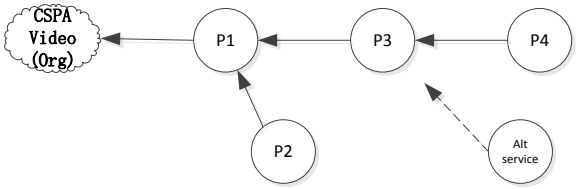

Figure 2. An Example Scenario of Federated Cloud Chain

Each CSP should analyze to determine suitable candidate service along the chain, and decide proper replacement services once SLA violated. For example, if P4 service is against the SLA required by P3, P3 immediately search most security alternative CSP instead of P4. Comparisons of security SLA between CSP determine accuracy of selection results, but in order to avoid CSP frequently violating security SLA, we must consider CSP historical performance reliability as well. So selection method should consider previous security performance and can support a chain of federated cloud service scenario.

3. Selection Method

To select the most proper outsourcing CSP which can guarantee the compliance with the organizational security controls , organizations must be able to justify whether the security control constraints in SDTs and STOs can be satisfied by the candidate CSP, and then find out the best one.

Our approach focuses on the interactions between the organization and CSPs. Here we describe the necessary steps in the method. As can be seen in Figure 2, it consists of different phases: select, establish weakness assessment-determine, trust assessment-determine, aggregation, matchmaking, non-compliance. Steps 1-7 show how an organization can derive a service request with a set of security- weighted terms. Step 8 examines the appropriate offered service, and in step 9, changes in the accepted service offering affect the organization.

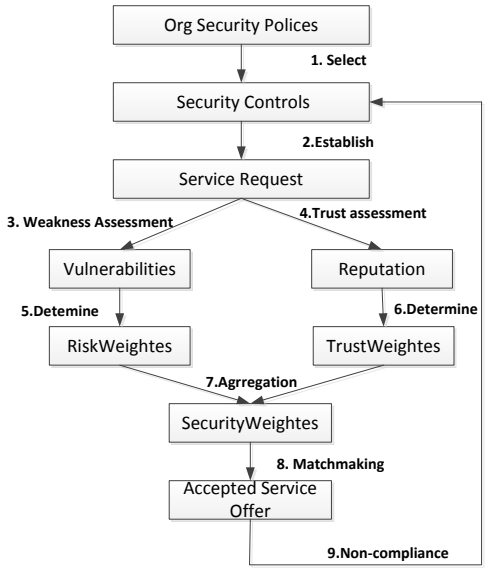

Figure 2. SLA-based Selection Method Framework

Beginning at step 1 and 2, the selected security polices described in SLA should be translated into the terms of a service request. We use a high level process that collects security control requirements and sorts them into functional constraints (SDT) and performance constraints (SLO). This high level process can be realized by formal semantics of languages. For example, the service must offer an prevention of DDoS attacks capacity, once the system was crashed by attacks, the recovery time is within 6s, which can be seen as a security control requirement, and can be divided into SDT term as the service must offer an prevention of DDoS attacks capacity, and SLO term as the recovery time is within 6s.

At step 3-8, the established service terms are quantified using weakness assessment and trust assessment. In weakness assessment phase, the riskweight is heavily rely on the importance of a particular SDT or SLO for ensuring service's security constraints are satisfying with the organizational requirements. On the other hand, the riskweight of a specific CSP is also determined by how closely they match the organization's service requests, the riskweight would be higher if the term matched more satisfactorily. In trust assessment, the historical performance of CSP is needed to be considered. All CSPs evaluate each other, whenever a transaction takes place between a pair of service nodes, in this case, a CSP can be considered as a service node, and therefore, all nodes send local trust score among themselves. And then we aggregate the local scores to calculate a CSP's global trust scores. Eventually we get a global trust matrix; each element in the matrix presents the trustweight of specific CSP. Furthermore, when consider the real environmental factors that may combine riskweight with trustweight, we calculate a securityweight, which stands for the assessment about CSP's overall performance to organizational requirements. This part is the key part of our approach; we would discuss it in the following section with detailed.

Step 9 focuses on how to cope with changes in the accepted service offering affect the organization. Once the organizational security constraints need to change, the original CSP cannot adapt to these new service constraints properly. So this step can ensure that reselect the best suitable outsourcing CSP if organization change the service policies.

4. Security Assessment Framework

Given our approach for selecting the proper outsourcing CSP, we focus on a core problem of organizational security evaluations in a dynamic distributed cloud environment and how to identify the security weight based on SDTs and SLOs with business cost constraints.

If we do not consider the business cost and only focus on service security, the service selection that most minimizes risk but would simply choose the exorbitant price service. Security capabilities provided by the CSP is proportional to the price, but organization would not choose some CSPs which have far more capacity than they request. So how to select the proper CSP which not only can guarantee the organizational security requests but also control the economical cost becomes a difficult issue.

So CSPs which provide services mostly close to the organization are our best choice. Firstly, the organization seeks outsourcing CSPs which offered services can most closely match organizational requests, based on the security weighted. Secondly, the federated cloud changes and the service no longer meet original SLAs, our approach would automatically help the organization to seek the new best one. We formalize the description about SDTs specified in SLA and introduce a prototype assessment method to calculate a CSP's security weight that minimized risk and cost.

4.1. Risk Assessment

In the previous discussion, we divide the SLA terms into SDTs and SLOs , SDTs describe the functional request and SLOs are used to evaluated the exact performance constraints. We encode risk weighted SDTs and SLOs separately.

Let SLA be a dualistic group containing two sets defining the SLA terms, $SLA = \{SLO, SDT\}$. oSLA is a pair involving two sets defining the outsourcing CSP offered SLA terms , $oSLA = \{oSLO, oSDT\}$.

4.1.1. SLO Matchmaking

Let $comparatorSLO$ be a triple that contains the organizational requested $rSLO$, the outsourcing CSP offered $oSLO$ and the impact factor of this metrics W_{SLOi} , which denoted as $\overrightarrow{comparatorSLO} = \{\overrightarrow{rSLO}, \overrightarrow{oSLO}, \overrightarrow{W_{SLOi}}\}$.

Let $rSLO$ be a feature vector that contains N requested service level features, $oSLO$ be an $M \times N$ matrix where the ith row corresponding to the ith outsourcing CSP and $oSLO_{ij}$ is the jth service level feature offered by that CSP, W_{SLOi} be also a feature vector that contains N features which reflect the level of risk incurred if the requested service feature is not present in the service level of offering $oSLO_j$. These vectors can be showed as follows:

$$\overrightarrow{rSLO} = \begin{pmatrix} rSLO_1 \\ rSLO_2 \\ rSLO_3 \\ \cdots\cdots\cdots \\ rSLO_N \end{pmatrix} \tag{1}$$

$$\overrightarrow{oSLO} = \begin{pmatrix} oSLO_1 \\ oSLO_2 \\ oSLO_3 \\ \cdots\cdots\cdots \\ oSLO_M \end{pmatrix} = \begin{pmatrix} oSLO_{11}oSLO_{12}\cdots\cdots oSLO_{1N} \\ oSLO_{21}oSLO_{22}\cdots\cdots oSLO_{2N} \\ oSLO_{31}oSLO_{32}\cdots\cdots oSLO_{3N} \\ \cdots\cdots\cdots \\ oSLO_{M1}oSLO_{M2}\cdots\cdots oSLO_{MN} \end{pmatrix} \tag{2}$$

$$\overrightarrow{W_{SLOi}} = \begin{pmatrix} W_{SLO1} \\ W_{SLO2} \\ W_{SLO3} \\ \cdots\cdots\cdots \\ W_{SLOk} \end{pmatrix} \tag{3}$$

In order to assess the outsourcing CSP service level offerings meet the organizational requested service level features, we not only to calculate the difference between $rSLO$ and $oSLO$, also give the specific feature presents the importance to organization, which can be stated as W_{SLOi} . For example, through CWE, the insufficient Logging events ($W = 0.5$)would be more important than a confidentiality breach on classified data($W = 0.45$). When the organization assesses the level of risk based on each requested service, the all weights are consisted of a vector W_{SLOi} .

TO evaluate how closely CSP service level offerings meet the requested organizational service level features, we calculate the Euclidean distances between pair $(rSLO_i, oSLO_{ij})$ and

which consider the weight W_{SLOi}, and sum them to produce a total distance $SLOd_i$ for the ith CSP. The results illustrate the consistency of ith CSP offering service features with organization. Through following equation, we can iteratively calculate each CSP and place them in the column vector $\overrightarrow{SLOd_i}$.

$$SLOd_i = \sum_{j=1}^{N} W_{SLOj} \sqrt{(oSLO_{ij} - rSLO_i)^2}, 1 \le i \le M \qquad (4)$$

4.1.2. SDT Matchmaking

Similar to SLO, we also care about the functional terms in SLA. Let $comparatorSDT$ be a triple that contains the organizational request $rSDT$, the outsourcing CSP offer $oSDT$ and the impact factor of this metrics W_{SDTi}, which denoted as $comparatorSDT = \{\overrightarrow{rSDT}, \overrightarrow{oSDT}, \overrightarrow{W_{SDTi}}\}$. $rSDT$ is a set which contains N functional service feature of organization request. Each element of $rSDT$ is a security or performance requirement demanded by organization. $oSDT$ be a set of N vectors and each vector presents the specific CSP can provide the capability in accordance with organizational service feature.

$\overrightarrow{W_{SDTi}}$ also be a feature vector that reflects the potential impacts of this service term if violated. These concepts can be showed as follows:

$$rSDT = (rSDT_1, rSDT_2, rSDT_3 ... rSDT_N) \qquad (5)$$

$$oSDT = (\overrightarrow{oSDT_1}, \overrightarrow{oSDT_2}, \overrightarrow{oSDT_3} ... \overrightarrow{oSDT_M}) \qquad (6)$$

$$\overrightarrow{oSDT_i} = (oSDT_{i1}, oSDT_{i2} ... oSDT_{iN}) \qquad (7)$$

$$\overrightarrow{W_{SDTi}} = \begin{pmatrix} W_{SDT1} \\ W_{SDT2} \\ W_{SDT3} \\ ..... \\ W_{SDTk} \end{pmatrix} \qquad (8)$$

For our algorithm, we give a match making method to measure the consistency between organizational requested and CSP offering. This mapping method is based on formal semantics.

First, we give the description of the SDTs based on formal semantics.

The description language of SDT

< Properties > ::= ´ Properties :´ ,´ Functional´ < FuncProp >
´ Non-Functional´ < NonFuncProp >;

< FuncProp > ::= < StateP rop > | < StateP rop >< FuncProp >;

< StateP rop > ::= < AtomProp > | ´ not´ < StateP rop > |< StateP rop >´ (and|or|imply)´ < StateP rop > |´ A´ < PathP rop > | ´ E´ < PathP rop >;

< AtomProp > ::= < ASID >´ .´ < State > | < EID >´ .´ < State > |< ASID >´ .´ < SAttrName >< Compare >< Real >< EID >´ .´ < EAttrName >< Compare >< Real >;

< Compare > ::= ´ <´ |´ >´ |´ ≤´ |´ ≥´ ;

< PathP rop > ::= < StateP rop >´ U´ < StateP rop > |´ F´ < StateP rop > | ´ G´ < StateP

rop >;

< NonFuncProp > ::= ´ Time :´ < TimeProp >´ Reliability :´ < ReliabP rop >´ Cost :´ < CostP rop >;

< TimeProp > ::= < FuncProp >´ →´ < CC > |< FuncProp >´ →´ < CC >,< TimeProp >;

< ReliabP rop > ::=< FuncProp >< Compare >< Real[0;1] >< FuncProp >< Compare >< Real[0;1] >,< ReliabP rop >;

< CostP rop > ::=< FuncProp >< Compare >< Real≥ 0 >< FuncProp >< Compare >< Real≥ 0 >,< CostP rop >;

< Time > ::= < Clocks >< Invar >< TGuard >< CReset >;
< Clocks > ::= ´ Clocks :´ < Clock >* ;
< Clock > ::= < String >;
< CC > ::= < Clock >< Compare >< Real≥ 0 > | < CC >´ ∧´ < CC >;
< Invar > ::= ´ Invariants :´ (< State >´ →´ < CC >)* ;
< TGuard > ::= ´ Time Guard :´ (< Trans >´ →´ < CC >)* ;
< CReset > ::=´ Clock Reset:´ (< Trans >´ →´ (< Clock >´ := 0´)*)* ;

< Reliability > ::= ´ Reliability :´ < Succ >* ;
< Succ > ::= < Trans >´ →´ < Real[0;1] >;

< Cost > ::= ´ Cost :´ < StateCost >,< TransCost >;
< StateCost > ::= (< State >´ →´ < Real≥ 0 >)* ;
< TransCost > ::= (< Trans >´ →´ < Real≥ 0 >)* ;

This language can clearly describe the state transition of specific function in SDT. Rime, Reliability and Cost metrics are constraints of the SDT terms.

An outsourcing provider offering SDT term once be depicted by this language, we can verify whether it satisfies the organizational request SDT through model checking method [9]. In model checking process, the organizational request SDT term must be translated into logic description language and in order to validate the reachability of expected state. The detailed of this process we do not discuss in this paper.

We define a function called $matchdegree(\overline{oSDT}, rSDT)$, which represent the match degree of one provider capacity and organization requirement. Through model checking, if the results shows that provider can exact reach the state of the organization needed, we assign the value 0, else, assign the value 1.

In order to describe how closely the ith CSP matches the requested operations, we calculate $SDTd_i$, which iteratively sums the results of the match degree function, and the importance evaluation W_{SDT_i}.

$$SDTd_i = \sum_{j=1}^{N} W_{SDTj} \cdot matchdegree(\overline{oSDT}, rSDT), 1 \le i \le M \qquad (9)$$

We make risk assessment combined two parts: the risk incurred by a CSP's failure of organizational SLOs, and the risk incurred by a CSP not providing required operation. So we quantify the risk assessment through these two parts and arrive at a single risk value for each CSP. a_1 and a_2 are respectively stand for organizational value about SDTs and SLOs.

$$\overline{riskweight} = a_1 \cdot \overline{SLOd} + a_2 \cdot \overline{SDTd} \qquad (10)$$

4.2. Trust Assessment

In previous part, we describe method to evaluate the riskweight incurred by match-degree of SLA, and can choose the best appropriate CSP which mostly satisfy organizational requirement. However, if performance of some CSP is not staying at stable state, which would lead to extensive change in offering SLA and organization have to reselect the proper CSP. The reselect process would extremely influence normal performance of federated service, so we introduce the concept of trust as to solve this problem.

We need building a chain of trust between CSPs. Each CSP has a trust score, which is derived from neighbour CSPs and aggregate these scores to calculate the final trust score of specific CSP. The value of trust score expresses the trustworthy from other CSP's perspectives.

Consider the trust matrix $R = (r_{ij})$,where $r_{ij} = s_{ij} / \sum_{j=1}^{N} s_{ij}$ and s_{ij} is the feedback trust score that ith CSP rates jth CSP. r_{ij} is the proportion of ith CSP in the trust score as a whole to jth CSP, which presents the trustworthiness that i to j. For convenience, let s_{ij} be ranged from 0 to 10, the lower value of s_{ij} represents the smaller risk observed by their previous experience. If the ith CSP have no relationship with jth CSP, let s_{ij} be the biggest value 10. r_{ij} should satisfy condition that $1 \le i, j \le n, 0 \le r_{ij} \le 1, \forall i \sum_{j=1}^{N} r_{ij} = 1$. Each CSP normalizes all issued feedback trust scores and aggregate it into the trust matrix.

Let $V = (v_i)$ be a global reputation matrix, and is formed by all global reputation scores v_i for n CSP where $\sum_{i=1}^{n} v_i = 1$. The global reputation matrix can be calculated recursively by:

$$V_{(t+1)} = R^T \times V_{(t)} \qquad (11)$$

If given an arbitrary initial $V_{(0)}$, we can get the global reputation matrix by this recursively process. We can assume that the initial $V_{(0)}$ as $v_i = 1/n$, after a sufficient number of k iterations, we can get the global reputation matrix, and v_i means the ith CSP's trust weight at that time, describes the ith CSP's reliability of performance in the previous service.

4.3. Security Assessment

Under estimation of riskweight and trustweight, there is a process for aggregating two weight for obtaining final securityweight.

Considering both risk and trust aspects, we can calculate securityweight as follows:

$$\overline{\mathrm{sec}\,urityweight} = c_1 \cdot \overline{riskweight} + c_2 \cdot \overline{V(t)} \qquad (12)$$

This equation defines the final security calculation as weighted vector, where c_1 and c_2 are defined by organization, mean the relative importance of awareness with SLA and experience performance respectively. Organization can select the best outsourcing CSP through $\overline{\mathrm{sec}\,urityweight}$.

However, an one-pass choosing process is not realistic. The CSP satisfy the organization's requirement through federated service. If one of CSPs fails to meet the requirement, the

organization would reselect the proper one. Thus, the clouds and service chains require that security assessment be more dynamic and adaptive as services may be substituted in and out of the service composition. So we must make sure that at every step of our method, which can modify the CSP offering violates and trust, to analyze other CSPs and determine the most suitable replacement CSP for satisfying the organizational security constraints. We can summarize this process as follow algorithm:

SLA Renegotiation and Security Propagation:

```
CSPselect(SLA, Trust, Org, CSP, newrisk)
        Org.totalrisk ← updateRisk (SLA, Trust, newrisk)
 If newrisk > SLA.aggreedRisk
         (altCSP, altRisk) ← matchmaking(rSLA, Trust, CSP)
     If altRisk<newRisk
          CSP ← altCSP
           newSLA ← formNewSLA(Org, CSP)
            Org.totalrisk ← updateRisk (SLA, Trust, newrisk)
  If prevSLA ≠ null
         CSPselect(prevSLA,  prevTrust,  prevOrg,  CSP,
org.totalRisk)
  Else
          Notify Org of changes for approval
```

5. Evaluation

We now describe the evaluation of our method in this section. First, we illustrate the process of our security assessment using a case study, and then we examine the accuracy of the selected CSP compared with other method. Finally, we show how to reselect a proper CSP when someone is failure.

5.1. Case Study about Security Assessment

The following table presents our security calculation process applied to an example scenario. The organization requests five service function, three guarantee terms and cost constraint. In requested service functional operation, it contains authentication, read/write, backup, alert, and logging. In requested service objectives, it involves 95% logging of alert events, backup once every 10 minutes, the presence of non-authentication mechanism, and alert when emergency situation. Cost constraints would be about 100 units.

The outsourcing service provider responds with a service offer that contains three service operations, which are read/write function, alert function and service administration function. Service administration function consists of authentication and audit, which can satisfy the organizational authentication requirement. It also involves four SLOs, which are 90% logging of alert events, backup once every 8minutes, the presence of non-authentication mechanism and alert when emergency situation, estimated cost would be about 105 unites.

We assume the initial trust matrix would be $v_i = 1/4$, and calculate new trust scores when neighbor node give feedback scores. After five iterations, we get the trust weight of CSP1. Let a_1, a_2, c_1, c_2 be 1 for convenient, and calculate the securityweight of CSP1.

In order to illustrate that our assessment method can well quantify the security assessment, we also make assessment about CSP2, which can partly satisfy the organization's requirement. From the table we can note that although CSP2 better meet some of SLO, it failed in whole aspects of the security requirements. So organization would select CSP1 due to the value of securityweight.

5.2. Comparing with Others

In this part, we compare our method with other studies about choosing outsourcing CSP.

In [10], which provided a conventional method only focus on SLOs, lacks the semantic description of SDTs. So through this method, organization would only compare service objectives but ignore service operation. In the above example scenario, organization would choose the CSP2 because CSP2 can supply service more matchable with organizational SLO than CSP1.

In [11], which illustrated an approach based on minimizing business cost, the author cared more about economic aspects. They want to find an adequate CSP which can satisfy most of the organizational requirements with minimal business cost. So in this approach, organization would select CSP2 due to lower cost, ignoring the performance effects.

In [12], which proposed a novel method combined both functional operation and service objectives. It used WS-Agreement to compare functional operation and make match through a hybrid algorithm. According to the match degree, it assigned 1, 0.6 0.2, 0 respectively. Through this work, organization would select CSP1 or CSP2, they are all applicable. However, it ignored the completely exact matchmaking and historical performance. Our work would both consider the former historical experience and assign exact value to service functional operation. So organization can choose CSP1 for better reliable and security service.

We can observe that CSP1 is the most suitable candidate for organizational requirement whatever in SLA or in historical performance from Table 1, but we find other method cannot successfully select CSP1 as first choice. Our method formalizes SDT description, translate it as understanding meaning, and verify the correctness between organization and CSP under economics aspects. This method avoid the suddenly change in service process and consider historical performance stability. So it obviously demonstrates that our method is the best one.

Table 1. Example of CSP Assessment

Organization		SLO_d / SDT_d	*CSP1*	*CSP2*
S D T	*Authentication operation* $W_{SDT1}=1$	*1*0* *1*1*	*Service administration (Authentication)*	*No*
	Read/write operation $W_{SDT2}=0.7$	*0.7*0* *0.7*0*	*Read/write function*	*Read/write function*
	Alert operation $W_{SDT3}=0.6$	*0.6*0* *0.6*0*	*Alert function*	*Alert function*
	Logging operation $W_{SDT4}=0.5$	*0.5*0* *0.5*1*	*Logging function*	*NO*
		added	*Service administration (Audit)*	*NO*
S L O	*95% logging of alert events* $W_{SLO1}=0.5$	*0.5*5%* *0.5*0*	*90%*	*95%*
	backup once every 10 minutes $W_{SLO2}=0.8$	*0.8*2* *0.8*0*	*8*	*10*
	the presence of non-authentication mechanism $W_{SLO3}=1$	*1*0* *1*1*	*Y*	*NO*

	Alert when emergency situation W_{SLO4} *=0.7*	*0.7*0* *0.7*0*	*Y*	*Y*
Cost	*100*		*105*	*90*
Trust			*0.24*	*0.56*
Security			*1*0.185+1*0.24=0.425*	*1*2.5+1*0.56=3.06*

6. Conclusion

Assessing security aspects in the cloud requirements need to consider both SDTs and SLOs. The complexity of cloud services make the process of choosing proper CSP is extremely vague. In this paper, we have shown how quantify security in cloud combined with riskweight of security policies and trustweight of historical experiences, along with business cost perspectives. Using this method, organization can select the adequate CSP both in security and business, which is also capable of traversing cloud federations and service chains in order to reduce security effects and minimize business cost with the organizational requests. Future work will be focused on how to manage security mechanisms, better understanding of SLA and how to evaluate the new risk when provider introduces new CSP.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant No. 61170295, the Co-Funding Project of Beijing Municipal Education Commission under Grant No.JD100060630 and the Project of National Ministry under Grant No.A2120110006.

References

[1] S. A. de Chaves, C. B. Westphall and F. R. Lamin, "SLA perspective in security management for cloud computing", In Networking and Services (ICNS), 2010 Sixth International Conference on, IEEE, **(2010)** March, pp. 212-217.

[2] R. R. Henning, "Security service level agreements: quantifiable security for the enterprise", In Proceedings of the 1999 workshop on New security paradigms, ACM, **(1999)** September, pp. 54-60.

[3] H. Takabi, J. B. D. Joshi and G. J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, vol. 8, no. 6, **(2010)**, pp. 24-31.

[4] M. L. Hale and R. Gamble, "Risk propagation of security SLAs in the cloud", In Globecom Workshops (GC Wkshps), 2012 IEEE, **(2012)** December, pp. 730-735.

[5] A. Morali and R. Wieringa, "Risk-based confidentiality requirements specification for outsourced it systems", In Requirements Engineering Conference (RE), 2010 18th IEEE International, **(2010)** September, pp. 199-208.

[6] R. Zhou and K. Hwang, "Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing", Parallel and Distributed Systems, IEEE Transactions on, vol. 18, no. 4, **(2007),** pp. 460-473.

[7] P. A. Bonatti, A. Hogan, A. Polleres and L. Sauro, "Robust and scalable linked data reasoning incorporating provenance and trust annotations", Web Semantics: Science, Services and Agents on the World Wide Web, vol. 9, no. 2, **(2011),** pp. 165-201.

[8] X. Li, F. Zhou and X. Yang, "A multi-dimensional trust evaluation model for large-scale P2P computing", Journal of Parallel and Distributed Computing, vol. 71, no. 6, **(2011),** pp. 837-847.

[9] T. Ball, V. Levin and S. K. Rajamani, "A decade of software model checking with SLAM", Communications of the ACM, vol. 54, no. 7, **(2011),** pp. 68-76.

[10] L. O'Brien, P. Merson and L. Bass, "Quality attributes for service-oriented architectures", In Proceedings of the international Workshop on Systems Development in SOA Environments, IEEE Computer Society, **(2007)** May, p. 3.

[11] K. Djemame, D. Armstrong, M. Kiran and M. Jiang, "A risk assessment framework and software toolkit for cloud service ecosystems", In CLOUD COMPUTING 2011, The Second International Conference on Cloud Computing, GRIDs, and Virtualization, **(2011)** September, pp. 119-126.

[12] K. Bernsmed, M. G. Jaatun, P. H. Meland and A. Undheim, "Security SLAs for federated cloud services", In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on IEEE, **(2011)** August, pp. 202-209.

Authors

Liu Xiaochen, she is currently a Ph.D. candidate at School of Computer Science and Engineering in Beihang University, Beijing, China. She received the B.S. degree and the M.S. degree in school of Computer Science and Technology in Beijing Posts and Telecommunications University, China. Her research interests include network management, cloud service management, and cloud security analysis. Email: ann4498@sina.com

Xia Chunhe, he is now heading the Beijing Key Laboratory of Network Technology, Beihang University, Beijing, China. He received his Ph.D. degree in Computer Science and Engineering from Beihang University, Beijing, China, in 2003. His research interests include network security, network management, and network measurement.

Cao Jiajin, He is currently a master candidate at School of Computer Science and Engineering in Beihang Univerity, Beijing, China. His main research interests include computer network and cloud computing.

Gao Jinghua, she is currently a master candidate at School of Computer Science in Beihang University, Beijing, China. Her main research aspect include cloud computing and software defined network

Wei Zhao, he born in 1984, Ph.D., Lenovo Corporate Research & Development, Subsystem Research Lab, His main research include mobile computing and cloud security.