The allocation algorithm for data centers in cloud computing architecture from security perspective

*Chuan-Gang Liu[1],Hsin-Yi Lin, Kun-Ta Hsien

Deparament of Information Technology, Chia Nan University of Pharmacy & Science[1]
**60 ,Erh-Jen RD .,Sec.1 ,Jen-Te ,Tainan, R.O.C.*
**Email: chgliu@mail.chna.edu.tw*
**Phone: +886-6-2664911 Ext.5705*
**Fax:+886-6-266-7834*

***Abstract*—The distributed cloud system provides the customers cloud services efficiently, which includes infrastructure (IaaS), software (SaaS) and Platform (PaaS) services. With such system, a lot of cost is saved and it becomes easy to deploy network services for Internet content providers, which just follows pay-by-use models. However, security is a main concern for cloud customers. However, in distributed cloud architecture, each data center should apply on-demand security mechanism and it is complex and costly. Hence, this paper proposes datacenters should be classified as two categories, high security datacenter and normal datacenter. However, the issue of allocation of high security datacenter arises and we propose allocation algorithms for high security datacenters considering security parameters in the distributed cloud architecture. We analyze the combination of those parameters and develop several algorithms. Among them, the proposed iterative algorithm preferring security parameters achieves our goal of this paper, high security. It facilitates the computation of the location of high security datacenters based on iterative searching in a solution pool of a basic algorithm. Hence, in this paper, we design several algorithms and provide an adequate algorithm to place high security datacenters, which is very helpful for cloud security and provides robust cloud architecture.**

Keywords—distributed cloud, security, allocation of the datacenter

1. INTRODUCTION

Recently, cloud computing attracts much attention in multiple fields. In fact, the similar concept behind this technique has been implemented in Distributed computing, Grid computing and Utility computing. However, the cloud computing employs business model (pay-by-use) to provide the cloud users service in different forms, including infrastructure (*IaaS*), software (*SaaS*) and Platform (*PaaS*). Fig. 1 shows the conceptual usage of distributed cloud architecture (Datacenters denotes DC). Although cloud users can benefit from low-cost cloud resource, security is a main concern for cloud customers. Cloud business users doubt whether business data is protected well from hackers' attack. People also concern about whether their privacy are accessed illegally. Security is a main key point to persuade people to use third-party cloud resource trustfully.

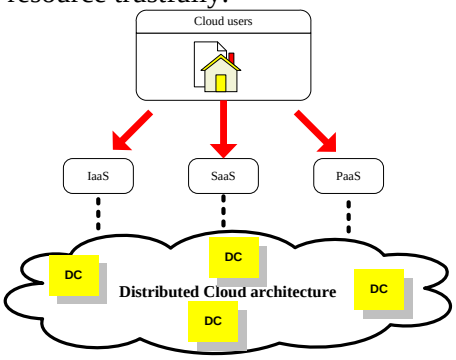

Fig. 1: The conceptual usage of distributed cloud architecture.

Security researches in cloud architecture propose many solutions. The authors in [1] survey many intrusion detection techniques in cloud. They introduce many possible intrusion situations and then survey various IDS and IPS techniques used in cloud computing. The details of this survey please refer to [1]. Beside, employing Secure Socket Layer/Transport Layer Security (SSL/TLS) protocols, IPSec, to protect network connection against the threats is traditional and popular network security mechanism. Other anti-virus techniques are like Firewall, virus detection, authentication, authorization, access control[6] etc., which are used to address various possible attacks. Based on the observation of the source of

security threats, we can find the security scale is wide. Basically, a well-designed security policy in cloud architecture should cover three domains, including network, service and storage security. However, deploying such large-scale security protection is complex and costly. Further, all cloud service employing the same security policy is not necessary. Research [2] proposes on-demand security architecture that each demand for cloud service can apply different security algorithm in three security domain. Cloud users just specify security level through web management interface without full knowledge about security. Such on-demand security architecture really meets each cloud service's security requirement ideally. However, in distributed cloud architecture, to implement this architecture, each data center should apply on-demand security mechanism and it is still complex and costly. Usually, the amount of critical and secret services is only small portion of all services in cloud. To protect such few services needs many network, service and storage security schemes, and this is not economy security solution. This paper proposes data centers should be divided into different categories according to different security levels. Critical cloud services should be assigned to data centers of high security level. However, the issue of allocation of high security datacenter in wide-scale distributed cloud architecture arises. And we propose allocation algorithms for high security datacenters considering security parameters in the distributed cloud architecture. To save the deployment cost of cloud security, this paper proposes to allocate the fixed number of high security level datacenters (we call these data centers as *HLDCs* and other data centers as normal datacenters *NDCs* thereafter) in distributed cloud architecture. However, there are some issues to locate *HLDCs*, including delay constraint, bandwidth requirement, security, etc. Furthermore, we also consider the impact of the number of *HLDCs* in cloud. Therefore our paper provides the following contribution:

1. To the best of our knowledge, this paper is the first to discuss the location of data centers with security consideration.
2. This paper proposes the allocation algorithms to locate fixed number of *HLDCs* with various security parameters and network constraints.
3. This paper discusses the various allocation algorithms in distributed cloud system and provides the analysis to design security cloud architecture.

Based on our proposed cloud architecture, there are two types of cloud data center, *HLDC* and *NDC*. Usually, *HLDC* needs more conscientious security policy and complex security settings. This paper provides a guide to allocate *HLDC* in distributed cloud architecture. Our proposed cloud architecture can save much cost to deploy security function in distributed cloud architecture and achieve the similar security level with fully-deployed security cloud architecture. The rest of this paper is organized as follows. Section 2 describes related work about security researches in cloud architecture. Then, in section 3, we introduce the allocation schemes of *HLDC*s and discuss the difference among algorithms. Section 4 gives a series of analysis for our allocation algorithms. We conclude this paper in Section 5.

2. RELATED WORKS

Previous work has paid much attention for the security in the cloud. Intrusion detection and prevention systems [1] are employed widely in cloud system. And honeypot technology is used to be a trap set to detect malicious actions[5]. Further, usually, we encourage cloud administrator to apply multiple security policies to authenticate cloud users, which can prevent normal users from various attacks. However, not all security methods are adequate to all cloud services. Previous research [1] divided cloud communication into three security domains. Each cloud service can require its security needs. Each datacenter should perform complex security functions to meet various security requirements of all cloud services, such as system resource management, admission control, various virus detection schemes, etc. Hence, in order to save the deployment cost of secure cloud architecture, allocating the fixed number of *HLDC*s is needed. However, the locations of those *HLDC*s should be planned well. The researches about location of data centers are also developed. [3] develops a framework and optimization problem to allocate datacenters based on the following parameters: cost, response time, consistency delay, availability and *CO2* emissions. However, research in [3] mainly places all datacenters efficiently with lower cost. In [4], it introduces the problem of the Area Process Center location. The authors in [4] make a decision-making approach which contains four steps to solve that problem and they focus on the third step -

recommending *APC* combination, homing arrangement and *APC* sizes. The issue in our paper is different from those schemes. Those researches about allocating datacenter do not concern about the location of different kinds of datacenters. In our paper, we focus on the allocation scheme of *HLDC*s in distributed cloud architecture. These *HDLC*s are just less percentage of all data centers. Making use of previous solutions is not adequate. Hence, we describe our proposed scheme in the following content.

3. THE ALLOCATION SCHEME OF HLDCS IN DISTRIBUTED CLOUD ARCHITECTURE

In this Section, we describe our allocation scheme with four sub-sections.

3.1. Our cloud architecture

In our cloud architecture, we assume there are *N* cloud datacenters which be composed of n_{HLDCs} and n_{NDCs}. Because there are just some *HLDCs* in the cloud, each cloud service user who have security requirement wants to access *HLDCs* closest to them. Hence, high availability and low response time are the main consideration for those cloud users. Furthermore, enough network bandwidth is also main concern. In this paper, we neglect the economic cost, including of land acquisition, datacenter construction, system administrator staff, etc. but only focus on the network factors and network security factors. However the location schemes of datacenters considering these parameters has been discussed in previous work. Reader can refer those works for the details.

3.2. The computation of the number of HLDCs

First, we analyze the number of *HLDC*s needed by cloud service users. As we know, Virtualization technology is key technology, which facilitates the cloud service provision for Internet service provider. Hence, we use virtual machine (*VM*) as the available resource. Based on the following definition, we make some analysis to predict the number of *HLDC*s. Here, we assume that all *VM*s in a datacenter are the same for simplicity.

TABLE I : THE PARAMETERS IN THE COMPUTATION OF THE NUMBER OF HLDC AND N_{VM}

Parameters	Definition
N_{vm}	The number of VMs in a *HLDC*
S_u	The number of users served by a *HLDC*, *u*
$P_n(t)$	The probability of *n VM*s requirement made by one user in a given time
$\overline{N_u}(t)$	The expected number of *VM*s required by *u* in a given time

We assume the distribution of $P_n(t)$ is *Poisson* distribution, which *Poisson* distribution is usually used to present the probability of network jobs. Hence, we can find Eq. 1 as follows.

$$\overline{N_u}(t) = \prod_{n=1}^{\infty} nP_n(t) \qquad (1)$$

The total number of expected number of *VM*s required by all users in a given time is divided by N_{vm} as follows.

$$N_{HLDC} = \left[\frac{\sum_{u=u_1}^{u=S_u(t)} \overline{N_u}(t)}{N_{vm}}\right] \qquad (2)$$

where N_{HLDC} denotes the expected number of *HLDC*s in a given time. We define the function [*a*] in Eq. 2 as the integer part of *a* plus 1. As the result of Eq. 2, we discover each *HLDC* has some superfluous *VM*s to deal with sudden much lower load. These parameters should be figured based on historical data and this is beyond the scope of this paper. So far, we have recomputed the expected number of *HLDC*s. Now, we also consider a more real case which $Var(N_u(t))$ exists. Under the premise that the number of *VM*s in a *HLDC* is fixed, N_{HLDC} should increase as follows.

$$N_{HLDC} = \left[\frac{\sum_{u=u_1}^{u=S_u(t)} \left(\overline{N_u}(t) + Var(N_u(t))\right)}{N_{vm}}\right] \qquad (3)$$

3.3 The discussion of security parameters

Based on the discussion of subsection 3.2, we know the expected number of *HLDC*s deployed in distributed cloud architecture. In this subsection, we discuss the consideration of deployment of *HLDC*s. Usually, in order to deploy datacenters should consider specified parameters. In this paper, we take the security parameters and network parameters into consideration.

Security policy guides the security domains which cover three domains, network, storage and service security. Among them, network security mainly relates with the location of *HLDC*s.

Hence, we design the allocation algorithms of *HLDC*s with consideration of network factors affecting security. Due to observation of the communication from source to datacenter, each router along the routing path may encounter the attacks from the hackers. We assume one router, *r*, has a probability attacked by malicious users, which is denoted as $P_a(r)$. Usually, routers along a hot path possibly encounter much attack. Hence, we should avoid placing the location of *HLDC*s on this hot path. To choose an adequate the location, hop count and hot routes should be taken into consideration and we call them as security parameters. To concretize the abstraction of attack, we give each hop an attack coefficient, *a*. Usually, log records in each router can give the hint to define this coefficient. Besides, we should avoid the neglect of the network performance parameters, bandwidth and delay. Then, we design our subject equation L_d and its goal is to discover the location of *HLDC*s with high security and high network performances.

W_h: the weight of the parameter of hop number;

W_d: the weight of the parameter of delay;

W_b: the weight of the parameter of bandwidth;

W_r: the weight of the parameter of the attack coefficient, *a;*

H(s,d): the hop number between source(s) and the chosen datacenter(d);

D(s,d): transmission time from source(s) to the chosen datacenter(d);

B(s,d): the bottleneck bandwidth along a route from source(s) to the chosen datacenter(d);

R(s,d): the sum of attack coefficients of all routers along route from source(s) to the chosen datacenter(d).

Subject equation: $maxi(L_d) = W_h / H(s,d) + W_r / R(s,d) + W_d / D(s,d) + B(s,d)\ W_b$ *(3)*

Constraint:

$W_h, W_d, W_b, W_r \geq 0$

D(s,d)<MaxDelay, which means the transmission time between*(s,d)* must be less than *MaxDelay*

B(s,d)>MinBandwidth, which means the bottleneck bandwidth along a route from *s* to *d* should be larger than *MinBandwidth*.

The latter two constraints are called as network constraint. Due to the applied parameters, our approach produces security-related cost for allocating the placement of *HLDC*, which is very different from other approaches. The relationship among the weights affects the allocating algorithms and we category these parameter weights into two groups, Security and Network-Related Parameter Weights(SRPW & NRPW). SRPW contains W_h and W_r; NRPW contains W_d and W_b. The following cases analyses discuss various combinations of these two categories.

Case I: *NRPW>> SRPW*

In this extreme case, *SRPW* is not important and even can be neglected. The problem of allocating datacenters becomes the previous problem like [4]. We do not discuss it here.

Case II: *NRPW << SRPW*

In this case, *NRPW* can be neglected and security parameters dominate the equations of allocating datacenters (Eq.3). There are two circumstances in such case.

- $W_h > W_r$: The algorithm developed based on *H(s,d)* becomes the shortest path algorithm while W_h is much larger than W_r. Under this algorithm, the locations of most HLDCs will be located in the central area of distributed cloud system. They are easy to become obvious targets to be attacked by malicious users. Hence, HLDCs should be apart *H* hops from other ones. In this algorithm, we call it as SP+H.
- $W_h < W_r$: in this circumstances, the locations of HLDCs may be arbitrary, which just keeps them out of hot router. This algorithm is called as the Least Attack Coefficient algorithm (LA). As the cause of developing SP+H, we also modify LA as LA+H.

We can see the algorithm developed based on single parameter should be not adequate. SP+H may still encounter much attack without considering W_r. LA+H may locate HLDC close to specified end users and it causes unfair for other end users. Hence a robust algorithm should be developed with both parameters and we call it as LA+SP+H. However, the discovery of the datacenter location based on multiple metrics is like to discover an optimal path from source to destination with multiple metrics, which is *NP*-hard problem. Hence, we discover our solution pool of *LA+SP+H* with iterative filtering. First, we find all possible solutions with *LA+H*, called as Loc_{LA+H}. Then, we can filter the solutions in Loc_{LA+H} with Eq. (3) adding hop count parameters.

In this case, we do not consider network performance parameters and it cannot be accepted for high quality cloud services. Next, we discuss the case considering network performance and the following algorithm is developed by extending *LA+SP+H*.

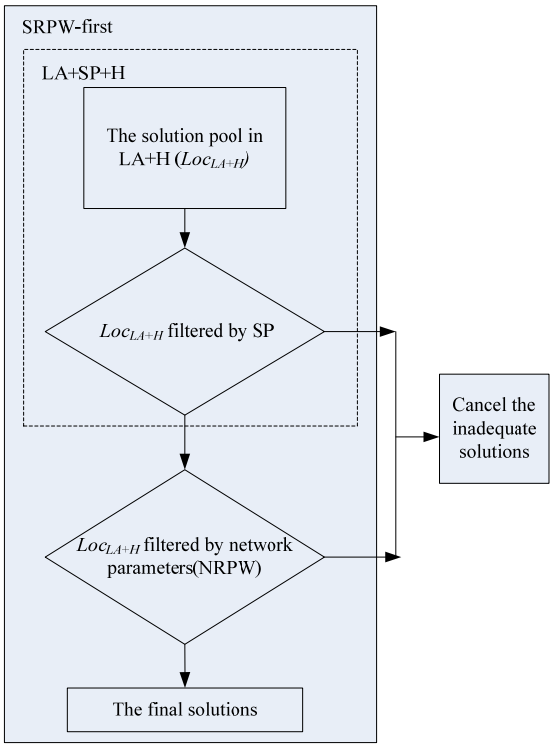

Fig.2: the process of *SRPW*-first algorithm

Case III: *SRPW* > *NRPW*

In this case, security parameters still dominate the locations of *HLDC*s. However, *NRPW* is slight smaller than *SRPW*. Usually, *HLDC*s rather focuses on security than network performance. Hence, we recommend the location algorithm is developed based on this case. An exhaustive approach in this case is to find costs of all possible location of *HLDC*. It usually takes much long time to find the best location solution. Furthermore, it may still choose a location which network performance performs better than security performance. Hence, we develop *SRPW-first* algorithm which it firstly finds all candidate location enhancing *SRPW* like *LA+SP+H* and then delete the locations violating network constraint. Among those candidate locations, we sieve best locations from them with the use of Eq. 3. This algorithm makes the location mission easy and saves much time. Based on this SRPW-first algorithm, the location of *HLDC*s in this algorithm emphasizes the security in distributed cloud system much obviously.

Case IV: *SRPW* < *NRPW*

In this paper, we usually expect the location of *HLDC*s is rather secured than network performance. In this case, network weight is strengthened. Unless the network condition is too bad somewhere, we do not consider this weight setting. As the reason of case III, we develop an algorithm called as *NRPW-first* algorithm. The process of the algorithm is also similar to *SRPW-first* algorithm.

4. ANALYSIS

So far, we have discussed all cases and develop several algorithms for these cases. We use the Table II to summary these algorithms in terms of security level, network performance and complexity. In Table II, we define five score levels such as Highest :5, Higher: 4, High:3, Medium:2 and Low:1. For security level, *LA+H* is the most secure because it only focuses on security coefficient. *LA+SP+H* should consider the hop number of the route and hence it ranks behind *LA+H*. *SRPW-firs*t is based on *LA+SP+H* and takes network parameters into consideration. So, the rank of those algorithms is as Table II. Among them, it is difficult to identify the security level of *SP+H* because hop number is related to security uncertainly. Hence, we let its security level being uncertainty. For network performance, we can find algorithms with network coefficients perform better than those only with security parameters.

TABLE II: THE SUMMARY OF ALL ALGORITHMS

Algorithms	Security level	Network performance	Complexity
SP+H	Uncertainty	Uncertainty	Low
LA+H	Highest	Uncertainty	Low
LA+SP+H	Higher	Uncertainty	Medium
SRPW-first	High	High	High
NRPW-first	Low	Highest	High

SRPW-first and *SRPW-first* are better choices. Other algorithms are designed without network parameters and network performance cannot be clearly defined for those algorithms. However, this paper develops *HLDC* placement mainly from a security perspective. Hence, *SRPW-first* is the best choice. Although *SRP*W-first seems to be more complex than other algorithms, it searches the solution based on *LA+H* iteratively. At each iterative, it filters inadequate solutions in the solution pool of *LA+H* with additional parameters. Hence, it becomes easy and fast.

5. CONCLUSIONS

Cloud computing is an emerging technology, which facilitates the provision of cloud service. However, security is key point for cloud users to use cloud function. Previous work suggests on-demand cloud security according to the security needs of each cloud user. But it is costly to

deploy full security mechanisms in every datacenters. We propose to classify datacenters into two types, *HLDC* and *NDC*. Hence, our goal is to allocate *HLDC*s in cloud architecture. Through the analyses of various combinations of parameters, we develop various allocation algorithms. Further, we suggest adequate allocation algorithms of HLDCs location. Hence, this paper is helpful to construct secure and robust cloud architecture.

REFERENCES

[1] C. Modi et al., "A survey of intrusion detection techniques in Cloud", Journal of Network and Computer Applications, 2012, in press.

[2] Jianyong Chen, Yang Wang, and Xiaomin Wang "On-demand security architecture for cloud computing," IEEE computer, pp. 73-78,July ,2012

[3] ´Ĩnigo Goiriyz et al., "Intelligent Placement of Datacenters for Internet Services", Distributed Computing Systems (ICDCS), 2011 31st International Conference on, 20-24 June 2011,pp.131-142

[4] Mansoor Alicherry, T.V. Lakshma, "network Aware Resource Allocation in Distributed Clouds," 2012 Proceedings IEEE INFOCOM

[5] V.H. Pham and M. Dacier, "Honeypot Trace Forensics: The Observation Viewpoint Matters," Future Generation Com-

[6] puter System—Int'l J. Grid Computing and E-science, vol. 27, no. 5, 2011, pp. 539-546.

[7] L.K. Hu, S. Yi, and X.Y. Jia, "A Semantics-Based Approach for Cross Domain Access Control," J. Internet Technology, vol. 11, no. 2, 2010, pp. 279-288.