One quantifiable security evaluation model for cloud computing platform *

Aobing Sun[1,2*] , Guohong Gao[1] , Tongkai Ji[1,2], Xuping Tu[1,2]

Cloud Computing Centre, Chinese Academy of Sciences, Dongguan, 523808, China[1]
G-Cloud Science and Technology Corp. Dongguan,523808, China[2],
absun@casc.ac.cn

***Abstract*—Whatever one public cloud, private cloud or a mixed cloud, the users lack of effective security quantifiable evaluation methods to grasp the security situation of its own information infrastructure on the whole. This paper provides a quantifiable security evaluation system for different clouds that can be accessed by consistent API. The evaluation system includes security scanning engine, security recovery engine, security quantifiable evaluation model, visual display module and etc. The security evaluation model composes of a set of evaluation elements corresponding different fields, such as computing, storage, network, maintenance, application security and etc. Each element is assigned a three tuple on vulnerabilities, score and repair method. The system adopts "One vote vetoed" mechanism for one field to count its score and adds up the summary as the total score, and to create one security view. We implement the quantifiable evaluation for different cloud users based on our G-Cloud platform. It shows the dynamic security scanning score for one or multiple clouds with visual graphs and guided users to modify configuration, improve operation and repair vulnerabilities, so as to improve the security of their cloud resources.**

Keywords—cloud computing, security, quantifiable evaluation, security visualization, security view

I. INTRODUCTION

With the continuous development of cloud computing technology, cloud has become one common method to create the different users' information infrastructure. AMAZON AWS, Microsoft AZURE, Ali Cloud and etc. develop very quickly and all have hyper scale datacenters to provide cloud service[1] The public clouds, private clouds, community clouds and hybrid clouds all have a large number of users. But as the cloud technology bring us very low-cost services and operation conveniences, it also caused that the information infrastructure of users is fragmented. The cloud users cannot know whether their cloud services are safe, and whether their data can be safely placed in different clouds; and cannot grasp overall security situation and repair security problems with efficient means[2, 3].

Currently, the host machines, virtual machines, storage devices, network devices and etc. within one cloud all have its isolated security scanning and repairing means. For one cloud, it is very difficult for cloud users, administrators and visitors to grasp the whole security situation of its accessible or administrable resources. If they adopt the services of different, the security status will be more complicated. So they have to put forward the wish to CSPs (Cloud Service Providers) to bring forward more secure cloud environment. But facing different CSPs and its own private clouds, the CSPs cannot also set up one universal security management mechanism to solve the security means across different clouds [4]. The cloud users need one GSV (Global Security View) or one USV(User Security View) for all of their information infrastructure perhaps composed by several clouds, so it is very important to create LSVs (Local Security View) , USV and GSV, then use them to improve security status.

We design a quantifiable security evaluation system for cloud computing infrastructure, including security scanning engine, security recovery engine, security quantifiable evaluation model, visual display module and etc. [5]. The security evaluation model composes of a set of evaluation elements corresponding different fields, such as computing, storage, network, maintenance, application security and etc. Each element is assigned a three tuple on vulnerabilities, score and repair method. The system adopts "One vote vetoed" mechanism for one field to count its score and adds up the summary as the total score. The cloud users can acquire the security situation of their whole information infrastructure added in the resource library through the security visual UI and judge the security level by the score. The system can also guide the users to repair the weaknesses of its clouds.

The rest of this paper is organized as follows: the next section introduces the related works. Section 3 presents the security quantifiable evaluation system. The security evaluation flows and algorithms are depicted in section 4. The prototype system and experiments are described in section 5. Finally, we draw the conclusions and give out the future works in section 6.

This paper is supported by Chinese National Key R& D Program of China (NO. 2016YFB1000500) and (NO. 2018YFB1004600).

978-1-5386-8034-6/18/$31.00 ©2018 IEEE
DOI 10.1109/CBD.2018.00043

II. Related Works

Cloud Computing has become the fundamental technology and service mode in the field of Information Technology. The business mode of cloud made the users is far away from the real computing devices. One user's information assets may include its own PCs, storages, network devices and other objects that located in different clouds. The users have no efficient means to evaluate the security of its own information infrastructure and have to believe in its cloud service provider. But in fact, the cloud security is one dynamic question, the users are short of technical tools to assess the cloud status of all its information assets in total.

Feng Dengguo, Zhang Min et al. describes the great requirements in Cloud Computing, security key technology, standard and regulation etc., and provides a Cloud Computing security framework [5]. Rong et al. pointed out that although many technological methods contributed to better security performances in the cloud, there are still no perfect solutions for many challenges, such as SLA(Service Level Agreements) of security and holistic security mechanisms to be resolved in the future[6]. Zunnurhain & Vrbsky focused on identifying and describing the prime security attacks on clouds with the goal of providing theoretical solutions for individual problems and integrating the solutions[7]. Jensen et al. focused on technical security issues caused by the usage of cloud services, especially cross-domain security. Venters & Whitley reviewed cloud computing research structured around technological and service dimensions, including security equivalence [8].

There are very few research on how to provide security views and improved means for different users as shown in Fig.1., and how to set up one quantifiable security evaluation model for cloud computing platform.

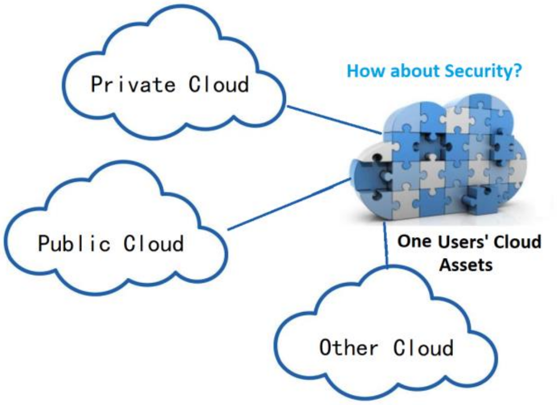


Fig. 1. The Dynamic Information Assets of Current Users

III. One Security Evaluation System

As shown in Fig.2, we create one quantifiable security evaluation system for single or cross cloud platform. One security quantifiable evaluation system includes security visualization display module, security vulnerability database, security scanning engine, recovery engine, security evaluation model, model establishment module and model maintenance module [9].

The security quantifiable evaluation model defines the collection of security items and quantifiable evaluation methods from the aspects of computing security set, storage security set, network security set, operation and maintenance security set, application security set and so on. The modules of evaluation systems can be deployed on single server or multiple servers (as one cluster) according to the scale of the monitored resources.

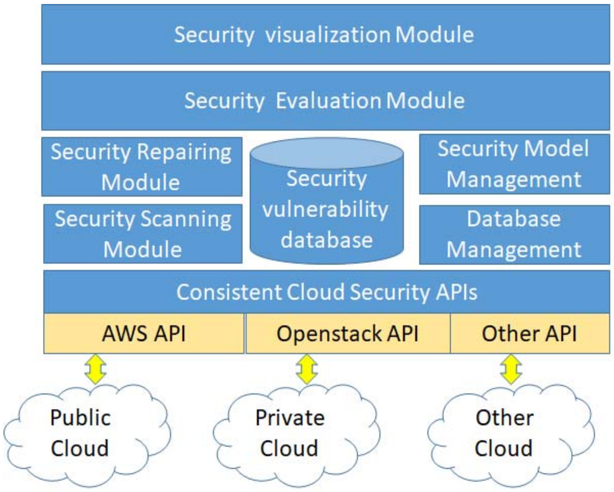

Security visualization Module
Security Evaluation Module
Security Repairing Module
Security vulnerability database
Security Model Management
Security Scanning Module
Database Management
Consistent Cloud Security APIs
AWS API
Openstack API
Other API
Public Cloud
Private Cloud
Other Cloud

Fig. 2. One Security evaluation system for Cloud Computing Platform

During real application, the security scanning engine of evaluation system scans the user's security collection, calculated the score of different security items, such as computing security, storage security, network security, maintenance security and application security. The scanning can be executed with serial or parallel means, and gives out one score for each resource according to the definition the evaluation model. The quantifiable evaluation result of the overall security for one cloud or only one user is a score as (0 to MAX), MAX is 1, 10, or 100. When users choose to repair security vulnerabilities, the repair engine is called for checked vulnerabilities and repair the vulnerabilities according to the defined rules [10].

IV. Quantifiable Security Evaluation Model

The core of the security evaluation system is its quantifiable security evaluation model. It defines the security evaluation means and repair rules. The model is created by the security expert group, and some items are adopted from some business or opensource scanning engine [11].

A. Security Collections and Items

One Security Evaluation Model is one collection composed by security fields as $P=\{P_1,P_2,P_3,P4,\ldots,P_N\}$.$P_i$ is one of the computing security collection, storage security collection, network security collection, maintain security collection, application security collection and etc [12].

One P_i of P includes different security checking item P_{ij}, as physical server OS, VM os, container systems, and other vulnerability items. And all items composed P_i.

$$P_i=\{P_{i1},P_{i2},P_{i3},P_{ij},\ldots,P_{iM}\}$$

TABLE I. SECURITY COLLECTIONS AND ITEMS FOR SECURITY QUANTITY EVALUATION MODEL.

Index	Collection Name	Main Items	Indicator
P_1	Computing Security Collection	Physical(Host) Machine OS	P_{11}
		Virtual Machine OS	P_{12}
		Container System	P_{13}
		Other Devices (GPU, FPGA, etc.)	P_{14}
P_2	Storage Security Collection	Storage of Physical Machines	P_{21}
		Storage of Virtual Machines	P_{22}
		Object Storage	P_{23}
		Block Storage	P_{24}
		File Storage	P_{25}
P_3	Network Security Collection	Network Configure	P_{31}
		Network Logs	P_{32}
		Network Device	P_{33}
P_4	Maintain Security Collection	Maintain Plan	P_{41}
		Management Architecture	P_{42}
		Running Safety Inspection	P_{43}
P_5	Application Security Collection	Application System Logs	P_{51}
		Behavior Audit	P_{52}
		Access Control Strategy	P_{53}

To every P_{ij}, the security scan engine will check the current security status of the objects within the cloud asset collection A of one user as equation (1).

$$A=\{A_1, A_2, A_3,A_4,\ldots,A_N\} \qquad (1)$$

$$A_i=\{A_{i1},A_{i2},A_{i3},A_{ij},\ldots,A_{iM}\} \qquad (2)$$

A_i is corresponding to users' physical machines, VMs and etc. As shown in equation (2), A_{ij} is one object needed to check its security status. If checking, the scanning engine will give out one triple S=[S_{ij}, L_{ij}, O_{ij}].

S_{ij} is the highest score, L_{ij} is security vulnerability level, and O_{ij} is one link to the fixed ways. L_{ij} can be leveled very complicated, with simplified means, it can be 0 for top weakness and 1 for no security risk.

One P_i corresponding to one S_i, the sum of total S_i is MAX(as 1 or 100) as equation (3) and equation (4).

$$\mathrm{Si} = \sum_{i=1}^{M} \mathrm{Sij} \qquad (3)$$

$$MAX = \sum_{i=1}^{N} \mathrm{Si} \qquad (4)$$

S_i can be one fixed score according to the weight of computing security, storage security or network security to give out one score. Then to every security checking items give one score S_{ij} according the importance and weight. S_i can also be one dynamic score, and changed with the weight of its including checking items.

B. Quantifiable Security Evaluation Process

Define the resource collection that the user can access as UP. UP_i is corresponding to P_i, P_i defines the checking items needed to scan of UP_i.

$$UP=\{UP_1,UP_2,UP_3,UP_4,\ldots,UP_N\}$$

As shown in Fig.3, the resource view of every user is one subset of Global Resource view. The resource view of the administrator with the highest privilege is the global resource view.

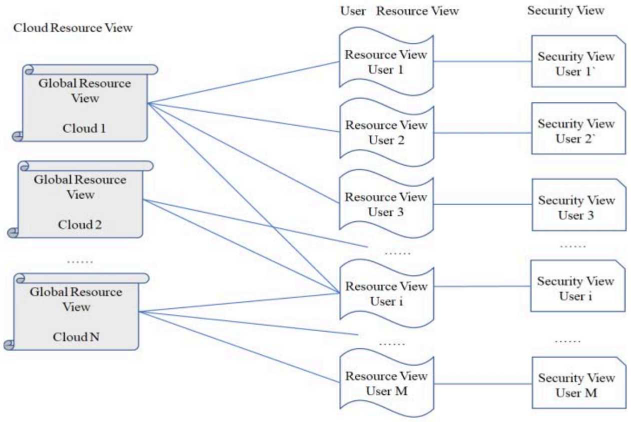


Fig. 3. Map Relations of Cloud Resource, User Resource and User Security View

The security scanning engine scans the user resource view according to the security evaluation model, it can scan the checking items P_{ij}, with serial or parallel means and give out one actual score US_{ij}.

$$US\mathrm{i} = \sum_{i=1}^{M} \mathrm{USij} \qquad (5)$$

Cloud security view is the actual security score of all kinds of checking items for user's cloud resource view. The administrator can acquire the global security view corresponding to the total cloud. To enhance the attention of one user to its cloud security, we adopt *One Veto Strategy* to depress the score if one cloud owning critical vulnerability.

One Veto Strategy: Corresponding to user's security view, the sum of total scores is the global quantifiable score. To summarize the scores, we can use the direct summary, average or one veto strategy. One veto strategy means if the score of one crucial checking item is below the threshold, i.e. L_{ij} is 0, then US_i is 0.

The security visualization module then displays the security view with graphically mode, i.e. the scores of the security scanning result for one user's cloud resources [13].

C. Repair Security vulnerability

When user select to repair the scanned holes, the security repair engine will call O_{ij} corresponding to P_{ij}. O_{ij} is one link corresponding to the repairing rules to different security hole. The repairing engine will repair the security holes serially or parallelly.

As shown in Fig.4., to one administrator or general users, the security system calls the repairing engine to fix the security holes, as downloading the patches, changes the configures, shut the services or ports and etc. The security repairing engine can fix the holes silently or interact with the user through user interface. After the repairing engine ends the work, the security evaluation model then gives out one new score, according to the fixed results [14].

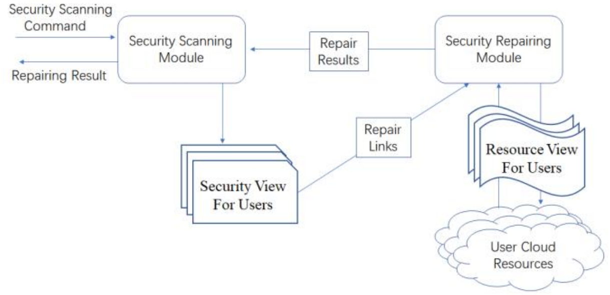


Fig. 4. . Repairing Process for Security Evaluation system

V. Simulation Experiments

The implementation of our quantifiable security evaluation system has been done based on our G-Cloud Platform[15]. Our experimental platform contains 2 independent Clouds. One cloud was set up based on G-CLOUD OS and one was based on OpenStack. The 2 clouds can be monitored and interact with same security API.

We used 2 group of experiments to test how about our evaluation system working for single or double cloud platform. The experiments were implemented with 3000 core computing resource pool, 200T storage resource Pool and 10GB/S network resource pool. The topo graph of the cloud is as shown in Fig.5.

Our experimental platform contains 2 independent Clouds. One cloud is set up based on G-CLOUD OS and one is based on OpenStack. As shown in Fig.5, Cloud 1 owns 16 physical machines (total 512 core) as computing resources and 200TB storage resources. Cloud 2 owns 10 physical machines (total 320 core) as computing resources and 150TB storage resources. The 2 clouds share the network bandwidth with 40Gb/s. The 2 clouds can be monitored with same security API.

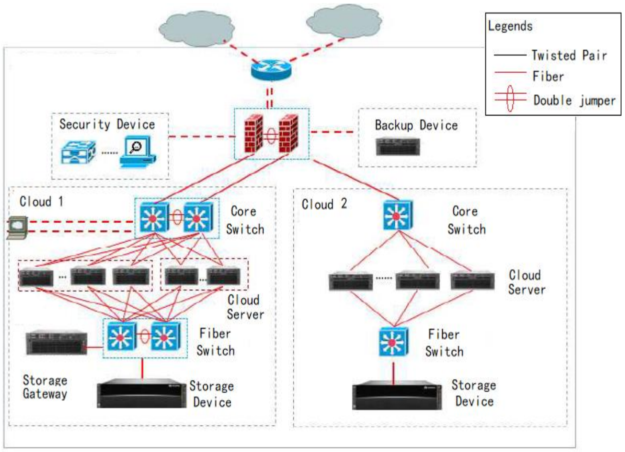
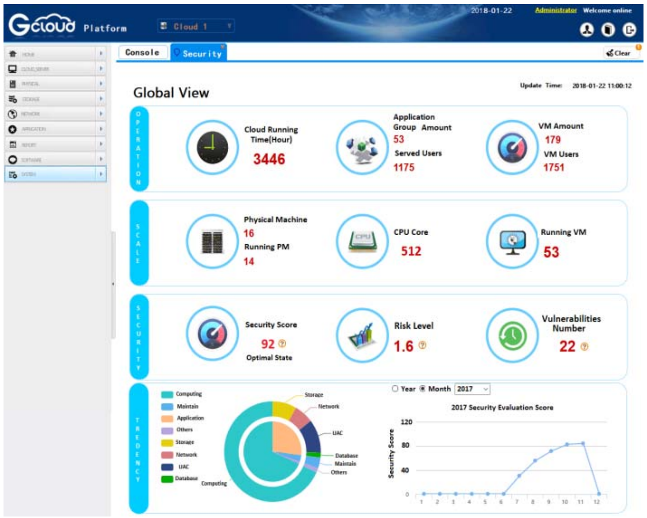


Fig. 5. The Experiment Environment for Cloud Security Quantifiable Evaluation

We used 2 group of experiments to test how about our evaluation system working. Firstly, the experiment was implemented in cloud 1 to simulate one private cloud. The running state, resource scale, security score and security trend were displayed on Fig.6. To one cloud platform, the global security scanning can be executed cyclicity. As same as this, the security situation of 2 cloud can be scanned and showed within one user interface, as the scanning module can access the 2 clouds with same API and owing privileges.

The quantifiable evaluation means can also be used to evaluate the security situation of one user. The scanning module will only check the securing status of the user's resources that were allowed to access. Then the security view can be given to show its status. The quantifiable means can give the administrators or users one intuitive user interface to know its security status and guide them to uncovering security vulnerabilities. That means will replace some non-automation security tools to improve the security maintain efficiency.


Global View

Update Time: 2018-01-22 11:00:12

Cloud Running Time(Hour) 3446

Application Group Amount 53

Served Users 1175

VM Amount 179

VM Users 1751

Physical Machine 16

Running PM 14

CPU Core 512

Running VM 53

Security Score 92 Optimal State

Risk Level 1.6

Vulnerabilities Number 22

○ Year ● Month 2017

Fig.6. The User Interface for Security Quantifiable Evaluation Result

TABLE II. Time Cost of Security Scanning with Serial or Parallel Mode .

ID	Scanning Mode	Serial Scanning Time(s)	Parallel Scanning Time(s)
1	Global Scanning for Single Cloud	3607	806
2	Global Scanning for 2 Cloud	5700	1211
3	User Scanning in Sing Cloud	121	30
4	User Scanning in 2 Cloud	260	50

As shown in Table 2, the security evaluation can be done with serial or parallel mode. If adopting serial scanning mode, the securing scanning module is deployed on one server, and every computing resource (as physical server or virtual server), storage resources and network resources was scanned one by one. Sometimes the resource scale was very big, the global scanning time is very long to several hours. Thus we can adopt the parallel mode to deploy the security scanning module on different servers (e.g. one cluster with 5 virtual machines) and divide one cloud into different resource groups and assigned the scanning tasks to different servers to accelerate the scanning speed and shorten the time to meet user acceptation. Equally, the security scanning for the cloud resources of one user in one cloud or 2 clouds can also adopt serial or parallel means. Generally one user's security view can be acquired within 30s, and the time can be accepted within one real cloud platform for its users.

VI. Conclusions and Future Works

In this paper, we provide a quantifiable security evaluation means for single cloud or multi-cloud environment. One quantifiable security evaluation system includes security scanning engine, security recovery engine, quantifiable evaluation model, visual display module and etc. The security evaluation model composes of a set of evaluation elements corresponding different fields, such as computing, storage, network, maintenance, application security and etc. Each element is assigned a three tuple on vulnerabilities, score and repair method. The system adopts "One vote vetoed" mechanism for one field to count its score and adds up the summary as the total score.

We implement the quantifiable evaluation system for different cloud users on our G-Cloud platform. It shows the dynamic security scanning score for one cloud with visual graphs, and then can guide users to modify configuration, improve operation and repair vulnerabilities, so as to improve the security of the whole cloud platform. Currently, the quantifiable security evaluation system can be implemented on single cloud or multi-cloud environment with consistent API and access privilege of cloud OS. We will wish to extend the evaluation system on other platform based on same security evaluation systems and make the resource monitoring and security monitoring within uniform security management mode and user interface.

References

[1] Mohanasundaram, R., A. Jayanthiladevi, and G. Keerthana. "Software-Defined Cloud Infrastructure." Handbook of Research on Cloud and Fog Computing Infrastructures for Data Science. IGI Global, 2018. 108-123.

[2] Rittinghouse, John W., and James F. Ransome. Cloud computing: implementation, management, and security. CRC press, 2016.

[3] Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." International Journal of Network Security & Its Applications 6.1 (2014): 25.

[4] Carlin, Sean, and Kevin Curran. "Cloud computing security." (2011)

[5] Mxoli, Avuya, Mariana Gerber, and Nicky Mostert-Phipps. "Information security risk measures for Cloud-based Personal Health Records." Information Society (i-Society), 2014 International Conference on. IEEE, 2014.

[6] Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." Information sciences 305 (2015): 357-383.

[7] Rebollo, Oscar, et al. "Empirical evaluation of a cloud computing information security governance framework." Information and Software Technology 58 (2015): 44-57.

[8] Chang, Victor, Yen-Hung Kuo, and Muthu Ramachandran. "Cloud computing adoption framework: A security framework for business clouds." Future Generation Computer Systems 57 (2016): 24-41.

[9] Al-Khanjari, Z., and A. Alani. "Developing Secured Interoperable Cloud Computing Services." European Scientific Journal, ESJ10.24 (2014).

[10] Kaur, Hasveen, and P. S. Mann. "An Improved Hybrid Re-Encryption Scheme for Mobile Cloud Computing Environment." International Journal of Computer Applications 162.4 (2017).

[11] Okonski, Aleksander. "Implementing Security Rules, Safeguards, and IPS tools for Private Cloud Infrastructures: GROOT: Infrastructure Security as a Service (ISaaS)." (2018).

[12] Chandni, M., et al. "Establishing trust despite attacks in cloud computing: A survey." Wireless Communications, Signal Processing and Networking (WiSPNET), 2017 International Conference on. IEEE, 2017.

[13] Boroojeni, Kianoosh G., M. Hadi Amini, and S. S. Iyengar. "Cloud Network Data Security." Smart Grids: Security and Privacy Issues. Springer, Cham, 2017. 71-82.

[14] Chang, Jeffrey, and Mark Johnston. "Approaches to Cloud Computing in the Public Sector: Case Studies in UK Local Government." Advanced Research on Cloud Computing Design and Applications. IGI Global, 2015. 51-72.

[15] G-Cloud OS, http://www.g-cloud.com.cn.