

- works, Technical Report No. DSC/2001/046, Swiss Federal Institute of Technology, Lausanne, August 2001.
8. Niyato D, Hossain E, HAN Z. Dynamics of multiple-seller and multiple-buyer spectrum trading in cognitive radio networks: A game-theoretic modeling approach. *IEEE Transactions Mobile Computing*, 2009, 8(8).
 9. <http://dx.doi.org/10.1109/TMC.2008.157>



Service Oriented CSOMA Model for Risk Evaluation of Cloud Computing System

Fan Lin, Lvqing Yang, Wenhua Zeng, Yue Wang

School of Software, Xiamen University, Xiamen, China
Corresponding Author: lqyang@xmu.edu.cn*

Corresponding author is Lvqing Yang

Abstract

Virtualization asks for safer and better quality to service-oriented cloud computing system suppliers. Most of the traditional researching is focus on the risk assessment of the information system and DDoS, but lacking of researching on cloud computing in deep. So that the service-oriented cloud computing system risk evaluation researching is very essential. In this paper, we build a service-oriented cloud computing system risk assessment framework that using distributed dynamic status monitoring of virtual machine system and making risk prediction value to summarizing the final risk assessment level of the system as a whole. The model can be used in monitoring, identifying, predicting and evaluating for cloud computing security risk that is having effect on the risk evaluation of virtual machine node and whole cloud system.

Keywords: SLA, QOS, RISK EVALUATION, CLOUD COMPUTING, DDOS.

1. Introduction

Cloud computing platform, which mainly provides a multi-tenant-oriented environment with web services, is an integration of extensible application service access which can be obtained through frequently-used communication protocols on the Internet. Cloud computing service relies on a large-scale

data center and mostly uses virtualization server to run web application programs and web services [1]. The service-oriented cloud computing system presents the following characteristics in three aspects:

(1) Large-scale and extensible design of service layer. It refers to a complex distributed-load balancing technology, and uses a dynamic and elastic on-

demand distributed computing strategy for computational task, data access, and database OLTP and OLAP processing. General cloud computing manufacturers structure the service on the infrastructure after unified virtualization - virtual machine (VM), and the operating system in the bottom layer provides network communication, IO access, memory management and CPU dispatch for VM. Therefore, the large-scale service problem of cloud computing is substantially the problem of service components of virtual machine with unified specifications..

(2) Tight coupling design of service layer. The application program is in cooperative development with service in the bottom layer to make the best of resource. In order to give full play to the virtualized and distributed overall cooperation competence, many cloud computing systems adopt tight coupling and flattening design; service layer is no longer a traditional single application layer, but closely integrated with IO dispatch, network optimization and CPU optimization of virtual machine. In this case, the operating status of server directly reflects and influences the status of virtual machine, thus directly representing the resource status of overall cloud computing system.

(3) High-reliability and availability design of service layer. Cloud computing system implements the real-time supervision of overall resource through Virtual Machine Management (VMM) and carries out dynamic coordination and dispatch of the operating status monitoring data of virtual service components via VMM, thereby guaranteeing the reliability, availability and safety of the whole system's operation.

According to the operating characteristics of the service-oriented cloud computing system, we bring in a model for risk evaluation of cloud computing system. The model uses the recording, tracing and filtering methods to implement the collection of both real-time operation monitoring data and system safety event logs for each virtual node through monitoring components internally installed between VMM and virtual service component layer, and builds a distributed model framework for system risk evaluation on the basis of single-point monitoring data to implement risk identification, risk prediction and risk assessment from the perspective of cloud computing system service.

The introduction of risk evaluation system in a cloud computing system implements dynamic risk analysis, risk assessment and intervention, effectively solving the insufficiency of conventional information system risk evaluation method.

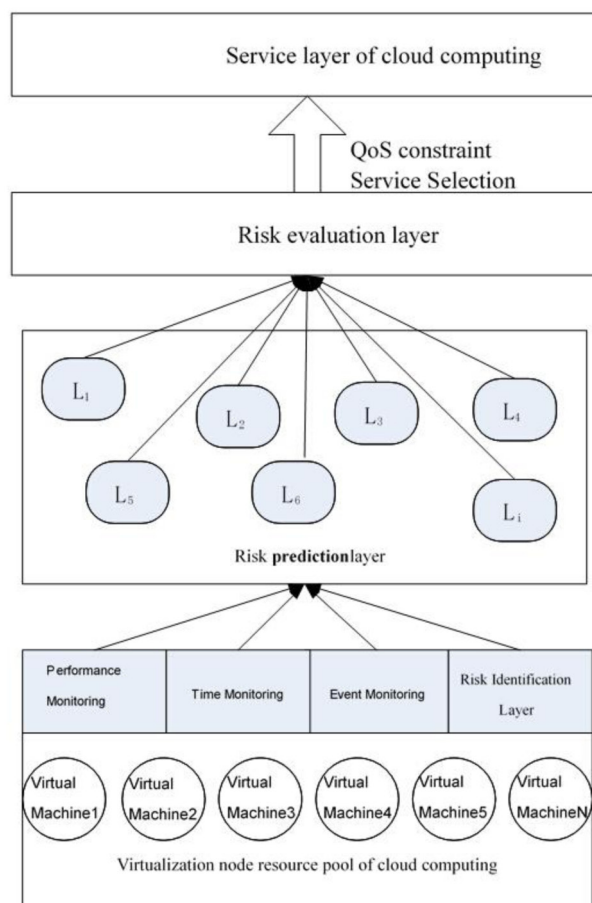


Figure 1. Framework of Cloud Risk Evaluation

2. OPEN Service Security Architecture of Cloud Computing Based on Safety Monitoring

2.1. Problem of DDOS Attack of Cloud Computing

In recent years, cloud computing system provides various on-demand services and interfaces for the suppliers to tenant in their space. The services provided by these suppliers change dynamically along with the change of virtual machine; these suppliers also provide flexible and diverse host services. The cloud computing system implements on-demand distribution and redistribution of computing resources shared and distributed by each device and software, and provides matched performance.

In 2009, KPMG passed the E-Crime Bill ^[1]. The study of E-Crime Bill shows that the security risk of online customers is steadily on the increase. For example, the research report of E-Crime Bill reveals that the customers of 63% of enterprises are mainly confronted with virus website attacks; according to an investigation report, the attack and threat technologies faced by customers of 40% of enterprises are increasingly complex.

If the use of DDoS (Distributed Denial of Service) by intruders threatens their cloud computing systems,

many nodes in a cloud computing data center are attacked, resulting in system breakdown; if a node is attacked by flooding messages, all other nodes are possible to be under attack, making the system offline or stopped. For example, the competitors of Amazon or Ebay may rent a commercial cloud computing system and use its known bugs in the system to invade the system, causing other normal users unable to use cloud computing services^[2].

There are many types of DDoS attack tools, such as Agobo, Mstream and Trinoo^[3], which are still widely used by attackers today. However, most attackers tend to use less complicated web-based attack tools, such as XML-DoS (XML-based Denial of Service) and HTTP-DoS (HTTP-based Denial of Service). Padmanabhuni and Jensen have introduced and described XML-DoS and its distributed version DX-ML-DoS (Distributed XML-based DoS)^[4,5]. When a XML message is sent to a WebService interface, the XML request containing incorrect contents consumes all resources of virtual machine where WebService is placed.

It can be observed that most network threats in the web service environment are from specific DDoS attack. Since attackers use normal WebService interface to initiate a request in the disguise of conventional XML message to conduct data exchange, server resources (including CPU, memory, and network bandwidth) are consumed via a large number of attack links to make the system unable to provide valid users with normal service access capability.

In this case, we present a cloud computing service-oriented monitoring architecture - CSOMA (Cloud Service Oriented Monitoring Architecture) to change the existing safety infrastructure of cloud computing by active defense. The architecture provides a distributed monitoring-based security risk evaluation model, which is composed of multiple methods in different layers and can implement real-time monitoring and recording of nodes in virtual machine of cloud computing system. Through the single-point risk identification, risk prediction and overall macro risks assessment of cloud computing system operating risks, the model can provide effective and safe prevention strategies for dynamic service selection and resource scheduling of cloud computing system.

2.2. WS-Security Standard Model

WebService is a typical loose coupling framework, which is characterized by self-description, platform-independence and discoverability of service interface^[6]. Since WebService is widely used for the interaction among enterprises, safety issues extend from Internet to cloud computing platform, greatly

increasing the risk of cloud computing system; Web-Service applications in a cloud computing environment become more dynamic due to the introduction of virtualization technology, so it is very complex to provide safe, reliable cloud computing WebService services.

WS-Security is a WebService-oriented standard, which stipulates message header of WebService protocol and extension of SOAP, combining with multiple technologies, frameworks and safe modes, as well as realizes the confidentiality and completeness of data. The realization of WS-Security, irrelevant to platform, is a general, cross-platform security mechanism, mainly including confidentiality of message, completeness of message and authentication of single message^[7].

WS-Security uses XML labels and XML encryption to put XML fragment into SOAP header to implement security encryption of data. However, traditional DDoS tools are less linked with network security defense measures^[8]. For example, spoofing message enables the attacker to obtain a legal ID, and then the attacker can paralyze the server by sending a large number of message or virus files. A better method is to combine WS-Security and WebService in a normative way and conduct security transformation of information message within a certain range, and to improve security capability of the system through the modification of security description of the packet, with extremely limited effect^[9].

3. Risk Evaluation of Cloud Evaluation

3.1. Virtualization Calculation

Virtualization is one of critical technologies of cloud computing. Virtualization implements the partitioning of cheap hardware of cloud computing center through virtualization tools, and each partition constitutes an independent virtual machine to make computation. Virtual machine includes devices such as CPU, hard disk, memory and network, and conducts the paralleled data processing. Virtualization means central abstraction layer, which packages module resources on the bottom layer based on the principle of time division multiple access, providing flexible resource management capability for modules on an upper layer. Major cloud computing platforms use virtual machine as their basic components.

Virtual machine is the smallest resource unit provided by resource of cloud computing center. Each host machine is divided into several VM, each of which provides different WebService, and different VM can dynamically migrate in local area network, as is showed in the Figure:

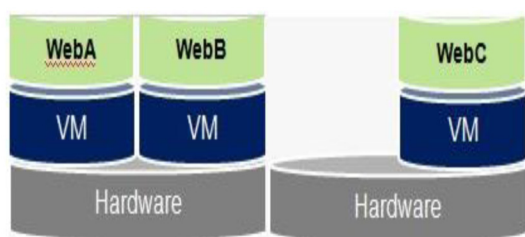


Figure 2. Schematic Figure for Resource Scheduling of Virtual Machine

3.2. Risk Monitoring of Virtualization Resource

In the cloud computing environment, resource pool of virtual machine includes several virtual machines, each of which consists of devices such as CPU, hard disk, memory and network, etc. Every web application transfers resource from host platform of virtual machine and implement dynamic migration.

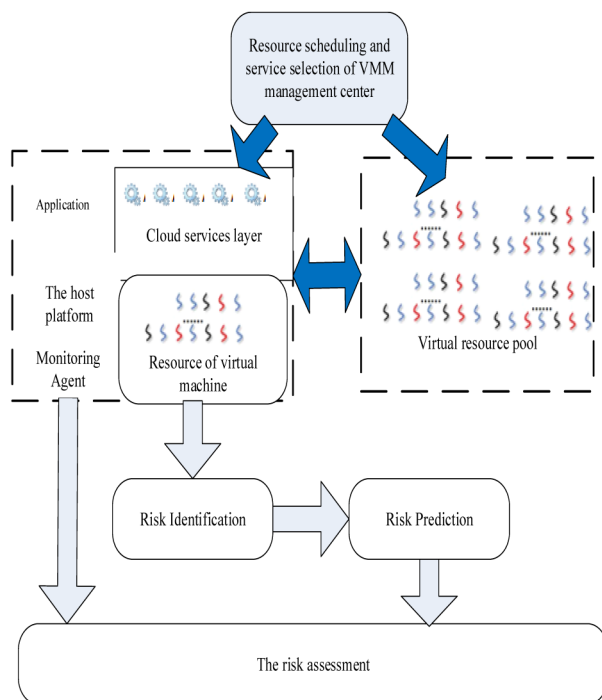


Figure 3. Structure Figure for Risk Evaluation of Virtualization Resource

For the cloud computing system and distributed environment, the key to strengthening controllability of system risk is to extensively adopt risk monitoring measures. In the cloud computing environment, any node can be added into the resource pool when using open network application protocol as long as it is in accordance with VMM hardware standard. Since virtualization technology unifies hardware of different specifications into standard virtual computing resource, including virtualized CPU, virtualized memory, virtualized storage and virtualized network.

The design of these applications must comply with existing virtualization strategies.

Therefore, it is necessary to take several factors into consideration when designing risk monitoring mechanisms, such as dynamic resource scheduling mode in each management level, cross-domain strategy and various kinds of standard protocols. Normally, monitoring mechanisms reside in a virtual machine system in the form of agent, the key of which is that monitoring behaviors of the agent cannot affect the operation of virtual machine and must conform to several typical characteristics as follows [10]:

(1) Transparency: the monitoring mechanism must be transparent for target system. It shall be able to blend into the target system in the mode of loose coupling without interfering normal operation of the system.

(2) Extendibility: the problem of extendibility contains two aspects: on one hand, when the number of monitored objects increases, the system performance cannot degrade sharply and the system still operates efficiently and steadily; on the other hand, a specific distributed monitoring can be efficiently conducted for a large number of objects.

(3) Independence: cloud computing system faces with different requirements from application and service in various layers, which requires risk monitoring mechanism to be able to adapt to the dynamic changes of cooperative work of nodes in application layer, as well as to the features with multiple application types. Monitoring agent and Web service shall be mutually independent in the aspects of coding and business process.

(4) Controllability: monitoring system can be flexibly configured during operation according to users' demand, and users can select distributive deployment and operating strategy. Frequentness, granularity and dimensionality of monitoring can be freely defined.

(5) Adaptively: it is able to make dynamic and adaptive adjustment according to environmental change and adjust monitoring demand autonomously.

Risk monitoring is also confronted with other problems: One is about stable, fault-tolerant and reliable monitoring system (namely availability). A high available system should ensure its robustness and have fault-tolerant capability, without providing wrong data as much as possible while maintaining stable operation. The second is about the manageability and transportability of monitoring system for the convenience of system management and updating. The third is about availability and comprehensiveness of monitoring information, which should be guaranteed to be valid data and meet different requirements

as much as possible. The fourth is about the safety of monitoring data and system. To guarantee resource safety is the precondition for network system resource providers to be willing to provide resource services [11].

This paper designs a service-oriented model for risk monitoring of cloud computing system, which adopts COSMA framework as evaluating principle and standard of the risk, adopts KVM as virtualization tools, adopts SOAP/HTTP protocol as standard detecting objects, and adopts SLA as integration of constraint conditions of QoS access for cloud computing service.

3.3. Risk Monitoring Methods based on Virtualization Components

Risk monitoring is the behavior of collecting operating status of cloud computing system and the information of features of virtualization resource, displaying and measuring real-time status of virtualization components in cloud computing system, measuring the status of virtualization components in each layer at special time and conducting risk calculation on such basis. Just to ensure the effectiveness of monitoring, the range of monitoring shall generally cover: (1) performance index of virtual machine (such as network throughput, occupancy rate of RAM, I/O quantity and occupancy rate of CPU); (2) relevant indexes in Web service layer of virtualization (such as average response time, memory and CPU condition of Web service, concurrent connections); (3) information of log events in close relation to safety, etc. Risk monitoring shall cover virtualization nodes in relation to Web service in the system as much as possible.

Therefore, the risk monitoring framework is the guarantee mechanism for risk control of cloud computing system, and can select specific cloud computing service for users and provide constraint basis for SLA, making it an important component of cloud computing security environment.

Currently there are several different methods in the classification of monitoring [12]:

(1) Division by monitoring objectives: since cloud computing system is a collection of a large number of virtual computing resources, there are physical host monitoring and virtual machine monitoring. This paper mainly researches the virtual machine monitoring.

(2) Division by monitoring contents: there are the monitoring of Web service layer of a virtual machine and the monitoring of operating system and virtual hardware resource state of a virtual machine;

(3) Division by monitoring method: there are two kinds: passive monitoring and active monitoring. The

main difference between passive monitoring and active one is that the former does not actively increase load but collect information in a way of Agent process residing memory; the latter can actively increase load through other devices, and observe and record operating conditions and results of the target.

By comparing the above-mentioned monitoring methods, the following measures are generally taken in a cloud computing system to implement distributed monitoring of virtualized resources:

(1) Division by monitoring objectives: including the monitoring of Web service layer of virtualization and the monitoring of virtual machine's nodes. The monitoring of virtual machine mainly includes: capacity of hard disk, utilization rate of CPU, occupancy rate of memory, memory capacity and CPU clock speed, and monitoring of operating status of virtualization hardware. The monitoring contents of Web service layer contain operating system, Web service log, operating status of user task, Web server log, etc, and the monitoring of related information of Web service program in a virtual machine. For the SLA agreement of cloud computing, we should conduct monitoring with attribute of time on Web service layer, which can reflect the basic capacity and quality of service access provided for users by Web service layer, mainly including the monitoring of virtualized network device and the monitoring of network performance among resources, such as access path of service, access delay of service, average waiting time and effective bandwidth.

(2) Division by monitoring contents: there are the monitoring of Web application and the monitoring of resource status. The monitoring of Web service resource, time and quality demand, QoS constraint index, event semantics, Web service response time and security event statistical information is beneficial to calculate current Web service risks of cloud computing system.

The monitoring model in this paper adopts a mixed model of in-depth risk analysis and dynamic operation status monitoring, mainly monitoring from Web service layer, analysis of event log and operation status of virtual machine. The analysis of event log is divided into statistical analysis and semantic analysis, thus forming the identification of risk degree. The monitoring objects are categorized as follows:

(1) Category of operation status of virtual machine: system call and loading conditions, capacity and utilization rate of hard disk, rate of idleness, memory capacity and its utilization rate, disk I/O, CPU clock speed and utilization rate, etc.

(2) Analysis of event log: statistical analysis of safety event log of virtual machine's operating system, and LSA-GCC risk identification based on the log.

(3) Web service monitoring mainly includes: operation status of Web service program and service quality of WebService and capacity of time response. The index is similar to performance index of virtual machine in nature. Therefore, performance index is classified into item of performance index of virtual machine, while quality of service and time index are separately classified.

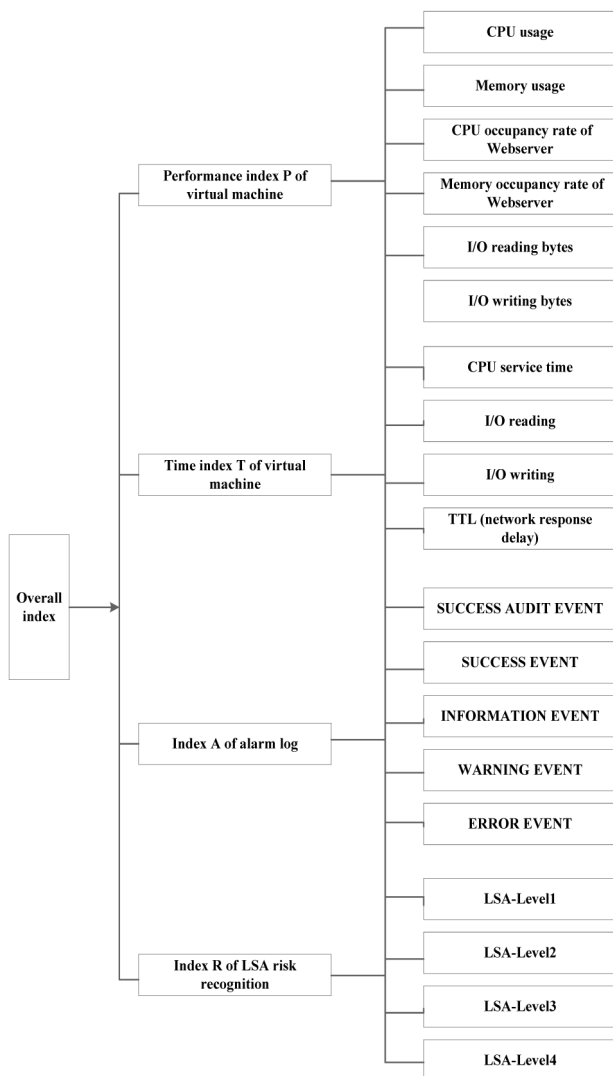


Figure 4. AHP Layering Risk Index Architecture

4. Cloud Computing Service oriented CSOMA Model

4.1. Cloud Computing Service oriented Monitoring Structure

The collaboration, virtualization resource, cloud application and cloud computing provided by cloud computing among cloud customers rely on the SLA agreement establishment therein. The essence of

SLA agreement is a QoS constraint for cloud computing service and a constraint-based service selection. When constructing the system model, this paper adopts a cloud computing service-oriented risk evaluation system, enabling monitoring capacity in the status of virtual machine in cloud computing system, identifiability in event risk, predictability in operating risk of virtual machine, assessment in overall risk of the system and controllability in service selection behavior.

For this reason, we present the Cloud Service Oriented Monitor Architecture. It mainly adopts a distributed monitoring agent to analyze and identify potential safety threats of clouding computing system, and provides basic data for real-time risk assessment layer to realize the dynamic, real-time and large-scale monitoring of virtual machine resources; it also conducts status monitoring, event analysis, risk identification, risk prediction and risk assessment of various kinds of virtual components, meeting the demand for overall risk evaluation of cloud computing service.

This system is composed of Cloud Client, Risk Recognizing Engine, Risk Predicting Agent and Risk Assessment Center.

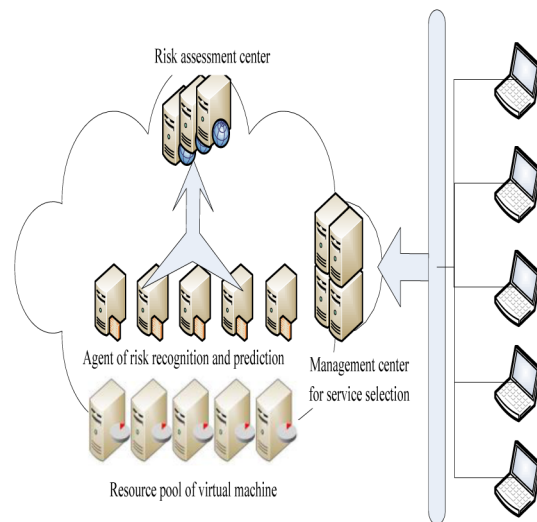


Figure 5. Structural Figure of Risk Assessment Based on Virtualized Resource

Cloud Client: referring to the client, making requests of available service with low risk for cloud computing system.

Risk Predicting Agent: referring to the monitoring agent of virtual machine, to accomplish time index, prediction of risk identifying index, blending and collecting statistical index of event log and performance index. It takes parallelization as a way of acceleration, and adopts the RBF prediction method.

Risk Recognizing Engine: it takes the method of clustering analysis, combining LSA with machine learning to recognize risks. It is composed of risk recognition algorithm and event analysis engine.

Risk Assessment Center: It synthesizes originally collected information and risk prediction values to provide the constraint basis for QoS service selection strategy, and is also used to evaluate overall risk of comprehensive indicator to obtain the attributes P, T, A, and R.

4.2. Risk Evaluating Model Based on Virtual Components Monitoring

The system model designed in this paper provides a cloud computing client with QoS service selection function based on risk assessment, and evaluates the behavioral risk of using cloud computing service for users resorting to monitoring and evaluating measures. Under the condition of taking full consideration of distributed and virtualized features of cloud computing and based on the above-mentioned design principles, this paper designs a three-layer monitoring architecture of “evaluating center, collector, monitoring, agent” as shown in Figure 6:

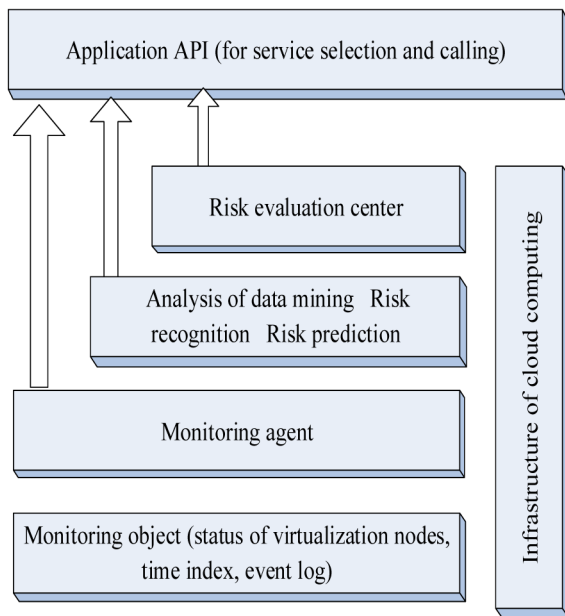


Figure 6. Hierarchical Structure of Risk Monitoring

For risk monitoring which is considered as general service, it is only required to regulate the demand of monitoring service for application program in the upper layer before calling risk monitoring data and realizing purposeful risk monitoring. Therefore, designers can concentrate on business logic layer of the system. To achieve this objective, there are multiple monitoring agents in monitoring system, which respectively maintains a monitoring list and is attached to respective resource of virtual machine, providing

updating status for application program in the upper layer and taking charge of monitoring real-time operating status of virtualized resource respectively.

In this system, the monitoring objectives in the bottom layer contain virtualized virtual machine, key Web service process in a virtual machine, and snapshot information of operating status of system event log of virtual machine. The monitoring agent is above the monitoring object, and mainly responsible to collect the security event log of an object, for original state information system and for the hierarchical communication of virtual machine state information in a cloud computing system. For the collected original information, the data mining analysis layer is made to be relatively independent, and there are two different modes of analyzing and handling: (1) transmit to aggregation node directly without modifying original status information, and risk evaluating center analyzes and judges the status of monitored node; (2) conduct in-depth data analysis and transmit analysis result to superior monitoring and aggregation node. In case computing capacity of virtual machine group of risk evaluating center is insufficient and processing capacity of virtual machine being monitored is redundant, it is optional to adopt the second way to optimize the system. On the contrary, if the computing capacity of the node being monitored is limited and the completion of in-depth analysis task alone could affect the normal operation of virtual machine, then the mode of distributive computation is adopted to complete the analysis cooperatively. This provides higher flexibility for the implementation of risk monitoring architecture and the structure Figure is as follows:

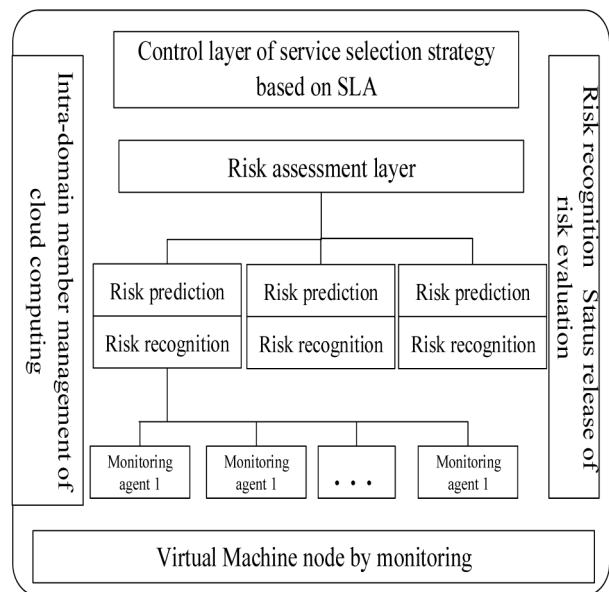


Figure 7. Model for Cloud Computing System Monitoring Nodes of Virtual Machine

Each monitored entity has a monitoring agent, and it collects original status data of the monitored entity, which is located at the terminal of a system. The collector will monitor and transmit relevant information of the object to risk identification components in the upper layer. The risk identification component implements the risk prediction based on a hierarchical analysis method. Since the time interval of status collection is relatively short and approximately 30 seconds, it is unable to reflect real risk conditions of node operation in a macro way. Therefore, in the identification and prediction environment in the upper layer, the time interval is amplified and the predictable risk change of the node is obtained through more data analysis.

The part of risk identification utilizes the method of data mining to identify and classify the level of risk of a monitored entity, and synthesizes the operating status, time status, safety event statistical information and risk identification result to make prediction of risk tendency and to form single-point risk predictive value. When risk prediction level corresponds to abnormal situation, the abnormal situation is processed by Web service selection strategy control center to conduct response for risk warning in advance. If risk level is normal, a value is returned, and conditions of such value are set by QoS constraint of target system to confirm specific rules of service selection. For example, there are four status switches of the monitored virtual machine, which are respectively expressed by (P, T, A, R) four groups of monitoring indexes, performance, time, alarming and risk identification degree, and each group of monitoring index is composed of respective monitoring parameters. The overall risk vector refers to the level of capacity risk of such node at certain time.

4.3. Risk Evaluation and Management Structure of Cloud Computing System

In the cloud computing environment, since a large number of virtualization computing nodes can be scheduled cross-domain and the audit strategy of business computing environment is relatively loose, it provides convenience for attackers. Different from former attack node groups through Botnet or deploying Trojan to structure internet network attack node group, attackers in the cloud computing environment can directly invade, control or rent large-scale computing nodes of the cloud, and then initiate attacks to Web service of another cloud computing system. There are typical cases such as an attacker component virtualization cluster and a victim cluster. Where distributed DDoS based on XML/HTTP is adopted, the attackers of two controlled cloud computing net-

works conduct large-scale XML message attack of the Webservice service layer of a threatened cloud computing system.

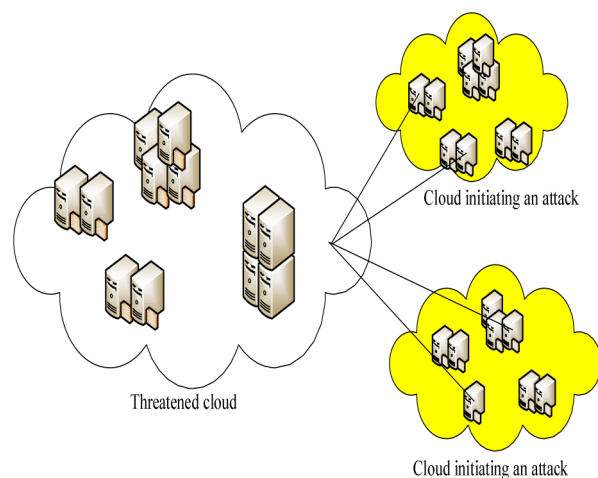


Figure 8. Model of Threat Attack of Cloud Computing System

Each server of cloud computing system is virtualized and divided into several virtualized devices (CPU, memory, I/O, etc). Therefore, the model for risk assessment of cloud computing system can be placed in the boundary of cloud computing network environment to conduct the filtering, tracing and analyzing of potential attack behaviors, and to make the risk identification, risk prediction and risk evaluation of service interface layers under attack, providing risk warning for boundary layer of cloud computing and achieving the QoS quality constraint selection of normal users for cloud computing services.

The safety risk monitoring and service selection management technologies in a cloud computing environment contain basic attributes and features of service-oriented distributed system as follows: (1) loose coupling: CSOMA is composed of standard XML markup language and HTTP/SOAP protocol, which means it can be operated and handled on different platforms; (2) based on interface message, the interface is located among client, service provider and CSOMA for the convenience of deploying the filtering, intercepting, and tracing components; (3) dynamic overlay: CSOMA provides service assembly required by risk control; it can flexibly and dynamically overlay the monitored service access point with the help of dynamic deployment ability of virtualized resource, and meet the demand for different QoS constraint service selections; (4) based on the deployment of virtualization technology, it is convenient to conduct management of dynamic load balancing of resource.

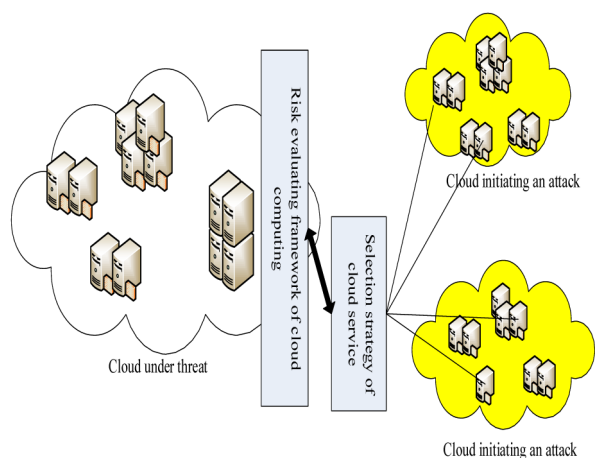


Figure 9. Defense Model of Cloud Computing after Adopting Risk Monitoring Architecture

Conclusions

Based on the virtualization feature of cloud computing, this paper takes the virtualization components as the core and the cloud computing-oriented WebService safety as the objective to conduct the structural design of risk assessment model. In the architecture design, the problem of DDoS threat in a WebService environment is firstly researched, and the structural features of WS-Security standard model are discussed and the defects in the environment of safety risk control of cloud computing are explained. A technology of cloud safety defense based on monitoring and tracing is also proposed. This technology is used to conduct modeling of virtualization components, and takes the method of hierarchical risk management to build an abstract and logical model. A cloud computing-oriented CSOMA risk monitoring and analyzing model is designed. The model adopts the mode of dynamic monitoring, central analysis and overall assessment to conduct the status monitoring, event log statistics and analysis, risk identification and risk prediction and to finally submit parameters of each index to the risk evaluating center to realize qualitative risk assessment. This model can be effectively deployed in the dynamic and distributive environment of cloud computing, making full use of free nodes to conduct the MapReduce distributed, parallel and accelerated computation and to realize real-time perception of risk status of cloud computing system.

Acknowledgements

The Project was supported by the National Natural Science Foundation of China (No. 61402386, No. 61305061 and Grant No. 61402389). And we wish to thank the anonymous reviewers who helped to improve the quality of the paper.

References

1. E-crime survey 2009[EB/OL]. <http://www.kpmg.com/FR/fr/IssuesAndInsights/ArticlesPublications/Documents/20090501-e-crime-survey-2009.pdf>. The 7th Annual e-Crime Congress in partnership with KMPG.
2. Stewart J. HTTP DDoS Attack Mitigation Using Tarpitting[J]. Securework. com, <http://www.secureworks.com/research/threats/ddos>, 2007.
3. Chonka A, Xiang Y, Zhou W, et al. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks[J]. Journal of Network and Computer Applications, 2011, 34(4): 1097-1107.
4. Padmanabhuni S; Singh V. Senthilkumar KM, Chatterjee A. Web services, preventing service oriented denial of service (PreSODoS): a proposed approach. In: Proceedings of the ICWS apos;06, international conference on volume , issue, September 2006. p.577-84.
5. Jensen M, Gruschka N, Herkenhoner R, et al. SOA and web services: New technologies, new standards-new attacks[C]. Web Services, 2007. ECOWS'07. Fifth European Conference on. IEEE, 2007: 35-44.
6. Zhang Faquan, Zhang Zhaoshi, zebing wang, etc. The security of the Web services [J]. Journal of computer age, 2003, 4:1-3. Zhang Faquan, Zhang Zhaoshi, zebing wang, etc. The security of the Web services [J]. Journal of computer age, 2003, 4:1-3.
7. In PuYi. [D]. Web services security research and practice of China university of geosciences (Beijing), 2007.
8. Bells. Web services security technology [D]. The research and implementation of national university of defense technology, 2004.
9. Xiao Tao, jackyang xiaosu Chen. Web services security guarantee mechanism study [J]. Journal of Huazhong University of science and technology, 2004, 4.
10. The Road to Web Services [EB/OL]. <http://www.w3.org/2001/03/WSWS-popa/paper63>.
11. Yeh. Trusted network computing system monitoring and trust model research [D]. PhD thesis of Chongqing University, 2012, 10.
12. Full gentleman. Open software behavior under the network environment monitoring and analysis research [D]. PhD thesis, central south university, 2010, 5.
13. Wendy tj wang. R-Net grid monitoring system (RNMS) and node management for the monitoring information in research and design [D]. Master degree theses of master of Beijing university of posts and telecommunications, 2006, 2.