文章编号：2096-1472(2017)-09-24-03

云计算路由平台入侵风险评估方法研究

黄凤辉
(广东环境保护工程职业学院实训中心，广东 佛山 528216)

摘　要：文章首先分析了云计算路由平台安全风险，总结为信道开放、传播受阻和数据泄露。在此基础上重点探讨云计算平台下入侵风险评估方法，通过实验分析结果来论证评估方法有效性，帮助提升云计算路由平台使用安全与信息计算速度，将风险隐患发生概率控制在规定范围内。

关键词：云计算；路由平台；风险评估
中图分类号：TP301　　**文献标识码**：A

Research on the Intrusion Risk Assessment Method of the Cloud Computing Routing Platform

HUANG Fenghui
(*Training Center,Guangdong Vocational College of Environmental Protection Engineering,Foshan* 528216,*China*)

Abstract: This paper firstly analyzes the sources of the security risks of the cloud computing routing platform,and summarizes the channel opening,transmission obstruction and data leakage.Additionally,the paper focuses on the intrusion risk assessment method of the cloud computing platform and validates the assessment method through the experimental results,which helps improve the security of the cloud computing platform and the speed of routing computation.The risk probability will be controlled within a prescribed range.

Keywords:cloud computing;routing platform;risk assessment

1 引言(Introduction)

云计算概念是由谷歌提出的，由2007年投入使用，立即在全球产生强烈反响，并且该项技术也成为网络信息发展中的重点研究内容。云计算对信息处理能力有明显提升，在同等时间内能够完成更全面的信息处理需求。云计算在风险环境下开展，建立一个长期工作目标对提升工作开展效率，浏览器对云计算环境的信息识别效率更高从，可以根据用户的信息使用需求来开展不同方法的控制环境中建立一个高级的信息共享模式，在最终软件应用模式下各项控制计划使用功能也能得到完善。对于不同运行模式下的信息共享，对于云计算环境中的各项资源控制，建立一个高效运行模式也是解决问题的有效措施。云计算环境下能够同时完成多项计算任务，通过建立长期工作环境来达到最佳控制效果，计算环境下能够实现对信息的高效存储、传输、运算、分析。对于系统中所存在的各项控制计划，云计算也是互联网功能实现的基本层面。客户使用中可以将大量数据信息存储在网络平台中，通过这种方法来减轻使用客户端的信息存储压力，保障用网设备能够更高效运行。

2 云计算带来的机遇(Opportunities presented by cloud computing)

信息存储方式改变后，云计算环境下的信息处理效率增快，使用者能够根据不同功能需求选择下载客户端，解放用网设备信息存储压力后可以下载更多应用软件。从全球范围内的局势分析，云计算模式发展进入到2020年后，将会达到超过500亿的市场规模，这对网络行业发展也是一次很大的突破。不同开发单位如果能够掌握住这一机遇进行数据开发，将会获得可观的市场收益，利用不同计算环境中的信息资源来增大存储效益，云计算带来的机遇非常大，利用好这一机遇进入到更广阔的市场应用环境中，能够帮助提升最终的市场发展效率。当前所应用的开发技术中存在一部分需要完善的内容，下面文章将针对这部分信息进行详细论述，帮助明确开发阶段应用大袋的标准，为云计算功能实现建立有效环境。

3 云计算路由平台安全风险来源(Cloud computing security risk source routing platform)

3.1 云计算平台下信道开放

基于云计算平台下所开展的信息共享，增大了信道开放程度，同时路由平台也是新颖的网络领域，风险控制正处于研究完善阶段。云计算是对信息获取形式的一次改变，在当前模式中应用这一方法能够在效率上提升，意味着信息获取通道得到开放，能够进入到更广阔的发展层面。用户通过浏览器来发现信息，并将其存储在网络环境中，方便再次使用查看。存储在云平台中的信息可以互相交流共享，从而达到

更高级的信息获取模式，发现影响因素后采取控制措施来帮助解决。信息获取信道增宽后用户存储在云空间中的信息容易丢失，或者受到黑客攻击损坏难以恢复。路由平台的接入端口均属于固定形式，信道开放虽然提升了云计算任务开展便捷性，但所获取信息的安全性却受到影响，风险用户发出请求后并没有被发现，而是继续传输信息，多数据共同传输增大了检测难度，安全性控制开展缺乏稳定环境，造成风险问题发生。信道在云计算环境下开放，很难达到对攻击者完成阻止，路由平台中所存储信息容易被窃取，对此需要建立风险评估体系，对信息窃取进行阻隔控制[1]。

3.2 路由信号传播减弱

路由信号传播在空气中，受传播环境中的阻碍因素影响可能出现减弱，使用端接收到的信号强度变弱，对信息传输连续性影响很大，网络信息有效范围更是不能确定。路由平台与云计算技术之间相互结合，决定信息获取效率的关键因素是信号在使用中是否能达到最佳控制标准。受传输过程中的空气环境和其他阻碍物影响，这种控制方法应用也很容易受到影响，解决工作期间不能保障结果信息的准确程度。信号减弱是造成风险隐患发生的主要原因，也是当前设计中应该重点解决的部分，通过建立一个长期稳定的运行环境来实现对最终处理方法的确定，也能达到最佳运行效果。信号减弱是造成最终风险问题的关键因素，当信号减弱后，使用端会自动搜集附近信号较强的路由共享网络，黑客利用这一特征入侵用户PC端，窃取重要信息，造成用户的财产损失。信号传播减弱仅仅是造成这一风险隐患的原因之一，云计算具有强大的数据存储与运算能力，路由信号传输作为信息共享途径，其安全性得不到保障对云计算功能实现也会造成阻碍影响。

3.3 云计算环境数据泄露

路由共享网络信号被搜索到之后，黑客经过程序运算来了解到IP地址等一系列隐私信息，能够模拟这一网络接入端，模拟合法用户进入到云计算环境中窃取重要信息，从而引发风险问题出现。数据泄露主要是技术方面的漏洞导致，在云存储环境下数据信息中存在的数据泄露严重威胁到路由平台使用安全性，云计算基于网络环境运行，同时路由平台也更加便捷，信息传输所受到的风险威胁因此而增大，这几种类型的风险发生概率较大，也是云平台环境下需要重点解决的部分。数据泄露造成的后果直接影响到用户对云计算技术的使用，而路由平台虽然带来了更多的便捷性，同时在入侵风险上也有明显提升。这一问题如果不能快速解决将影响到对平台的深入开发使用，需要从风险评估层面进行研究。通过建立完善风险评估体系，对于路由平台入侵风险能够更好防范，提升云计算技术应用效率，建立起更稳定的路由网络[2]。

4 路由平台入侵风险评估方法(Risk assessment methods for routing platforms)

4.1 危险识别法

(1)评估可能的云计算模式和提供商

云计算模式下信息获取渠道更丰富，达到风险评估效果，首先需要识别安全的提供商，面对不同风险隐患在评估系统建立中要体现出区别性，建立长期识别体系，并在云计算环境下不断更新，云计算针对信息运算处理需求大的用户，这部分用户也更吸引黑客攻击。风险识别任务自动化进行，能够更好地控制现场所存在的客户端使用风险问题，对于当前比较常见的技术性问题进行探究控制，也可以从提供商识别方面达到风险预防效果。对不同云计算模式与提供商进行评估，路由平台根据所得到的评估结果来选择适合的网络接入端口，并寻找到最佳的风险管理提供商，保障网络接入客户安全性，接下来各项控制任务开展也更安全可靠，评估可能的提供商和云计算模式只是初步方法，接下来还需要建立风险评估系统结构。

(2)云计算风险评估指标体系构建

识别风险首先要准确判断风险来源，基于云计算环境下对风险评估质指标体系进行详细构建，并帮助明确需要继续深入强化的技术方法，具体的指标构建体检见图1。

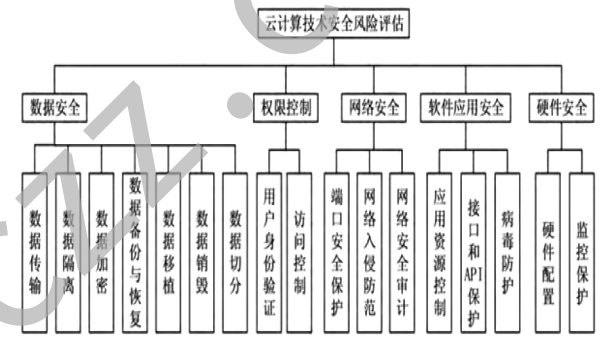

图1 云计算风险评估指标体系

Fig.1 Index system for cloud computing risk assessment

将路由平台入侵风险评估从五个层面进行，其中数据安全设计内容最多，数据的传输、隔离、加密和销毁切分等一系列处理措施均是帮助提升最终数据传输安全性，增加多道防御措施后所开展的云计算任务效率更快。权限控制时针对路由平台访问用户开展的，筛选合法用户连接网络端口，最大程度降低风险隐患发生概率。网络安全和软硬件安全需要对接口进行实时监控，发现非法接入后及时阻断处理，确保最终处理效果安全稳定，软件与硬件之间相互配合共同完成路由平台风险入侵的安全评估任务。

4.2 基于模糊集与熵权理论的评估方法

(1)模糊集合与隶属度矩阵

云计算过程复杂，在短时间内完成计算任务。则需要建立隶属矩阵，通过迷糊集合方法来提升数据处理速度，对访问请求安全性进行判断，非法请求会自动隔离在运行请求之外，避免非法用户接入到路由平台中。建立模糊集合的计算方法如下：设$A=\{u_1,u_2,u_3,\cdots,u_n\}$，共有n个计算因素，表示变化范围，可以根据实际情况展开调整，其中n为因素的个数。评判集运算组成模式表现为：安全风险来源范围$R=g(c,t,f)$，集合中的c、t、f分别表示资产威胁，系统威胁程度，脆弱程度三个不同内容。这三点也是云计算风险引发的主要原因，评估过程中主要从这三方面开展。表1中表示内容为三种风险程度表示的赋值。

表1 资产重要度、威胁频率、脆弱性严重程度赋值表

Tab.1 Asset importance,threat frequency,vulnerability severity assignment table

赋值	标识	资产重要度	威胁频率	脆弱程度
5	很高	非常严重	经常发生	完全损害
4	高	比较严重	可能发生	重大损害
3	中	中等严重	曾经发生	一般损害
2	低	低等严重	不太可能发生	较小损害
1	很低	并不严重	极罕见发生	可以忽略

矩阵构成要考虑是否具有突发性，将赋值表中的严重程度作为评估分析依据，从而达到最佳分析效果。矩阵是对风险发生可能性的一个综合评估，其结果中体现出真实情况，并且能够根据不同使用需求及时调整，掌握路由入侵平台风险，才能达到更理想的评估效果。

(2)路由平台安全风险值计算

对于路由平台可能出现的问题，计算选择常见风险问题来进行，云计算环境下技术人员可以对入侵风险进行模拟，反复试验记录路由平台系统参数，观察队网络系统造成的影响。通过数据记录来实现来综合判断风险比较常见的几个类型，进而实现评估体系与实际情况之间的结合，网络环境中很多风险问题是未知的，评估过程中也要考虑这一因素，确保最终控制模式能够应用在风险预防方面。路由平台的风险安全值计算，公式中所带入的信息参数要经过审核，达到安全性标准后才能开展接下来的评估计划，云计算带来的运算环境更广阔，开放环境下所造成的风险隐患可能性也会提升，风险发生概率计算是构建评估系统的依据，计算期间要考虑运行使用环境，将运行环境引入到平台控制中，无线网络信号传输所受到的环境因素影响在风险控制评估下能够降至最低，从而实现两者之间相互控制，这样即使在信号弱的环境下通过这种方法也能避免非法请求通过。

(3)分析威胁实验的关联性

关联性分析也是确定信息之间联系体系的有效方法，得到安全事件发生的可能性L(Probr,PV)。确定影响的资产，计算安全事件发生后的损失，由于损失取决于资产价值和安全事件可能出现概率，因此可以用函数F(As,L(Probr,PV))表示，最后可以计算出风险值R(L,F)，即R=F(As,Probr,PV))=F(As,L(Probr,PV))。

5 云计算路由平台入侵风险评估方法模拟实验(Simulation experiment for risk assessment methods of routing platforms)

5.1 实验环境选择与主要测试内容

首先根据云计算平台特征来选择风险入侵平台设计模式，观察所设计的内容中是否存在需要继续深入完善的部分，将黑客入侵引入到实验环境中，对路由平台进行模拟攻击[3]。将路由平台建立在具有风险隐患的环境中，并将其导通运行，分别建立几种不同的信号强度环境。在不同路由信号传输强度下，风险因素发生可能性也存在很大差异性，因此模拟出不同信号传输强度环境，有利于对风险等级进行确定。所采用的仿真实验共建立50个节点，分别对不同节点环境下的云计算路由平台信息变化做出计算，环境选择采用自动接入形式。用网设备会根据所搜索信息强度进行自动化选择接入，这样所测得的结果才能与实际情况更贴近，人为干预选择会造成信息参数与实际情况之间的误差。检测率(Detection Rate)是正确判断攻击行为数与正确判断攻击行为数与漏报的攻击数之和的比；误报率(False Alarm Rate)是系统将正常行为误报为攻击行为数与误报为攻击行为数与正确判断一个正常行为数之和的比；分组传递率(Packet Delivery Rate)是应用层信源发送的分组数目与信宿接收分组数目之比，它描述的是通过应用层观察到的报文丢失率，又反映了网络所支持的最大吞吐量，它是路由协议完整性和正确性的指标；平均延迟是报文从源节点到目标节点的平均传输时间，它也是反映了网络性能的重要指标[4]。

5.2 风险评估仿真进行

使用移动设备来接入到路由平台中，分别进行普通用户接入与非法攻击用户接入，观察接接入过程中是否均能够通过请求。根据风险评估计算结果所建立的安全控制体系，实验过程中表现出超强的灵敏度，将分发请求隔离处理，并在路由平台的控制端体现出这种变化，这预示所开展的计算中涵盖了常规风险。为更准确判断风险评估系统是否合理，接下来的模拟实验中采用更高级的入侵方法，首先针对用户IP进行定位，掌握提供商地质后试图进入到系统内部控制模块中，尝试对云计算数据库进行更改。风险发生后评估系统内迅速发出报警提示，实验结果表明所建立的风险评估体系有效，在方法应用中也符合大多数内容，能够达到安全的使用效果。

6 结论(Conclusion)

云计算路由平台今年来发展迅速，使用安全性也一直是重点研究的内容，文章中所论述的风险评估方法具有普遍性，但在实际落实应用中还需要根据系统反馈做出调整，为路由共享无线网络应用创造稳定基础，从而达到最佳控制管理效果，并为管理计划开展创造一个有利环境。未来的云计算路由平台发展，也会逐渐进入到更智能安全层面，应用方向也更加广阔，提升运算速度同时在功能应用范围上也会有明显增大。

参考文献(References)

[1] 刘绪崇,等.基于改进模糊C均值聚类算法的云计算入侵检测方法[J].中南大学学报(自然科学版),2016,47(7):2320-2325.

[2] 李红军.大规模网络入侵时联合云计算技术的协同预警技术研究[J].自动化与仪器仪表,2017(3):16-18.

[3] 赵静.云计算环境下联合移动代理技术的入侵检测系统研究[J].自动化与仪器仪表,2017(6):162-164.

[4] 曾振东,孙波.针对云端环境下入侵行为分析及网络安全技术实现[J].网络安全技术与应用,2016(5):51-52.

作者简介：

黄凤辉(1980-)，男，硕士，讲师.研究领域：计算机网络.