

云环境下基于信任的入侵防御研究

汪双兔, 韩坚华, 罗 军

(广东工业大学 计算机学院, 广东 广州 510006)

摘要: 云计算从提出以来就具备着动态性、虚拟化和开放性, 频频出现的各种大型的云安全事故使得云环境中的安全性受到质疑. 为了能够确保云环境的安全, 将入侵防御技术与可信计算的信任理论相结合, 提出了一个云环境下基于可信计算的入侵防御框架模型. 该模型从入侵防御的原理出发, 首先实时监控采集、获取行为特征, 然后将这些特征进行规范化, 并逐步确定各个特征的权重后得出用户节点的可信度. 利用多种云端的集群服务器引擎进行检测防御以及综合分析决策和聚类分析, 使云端能够及时快速、高效地抵御恶意行为的攻击, 改变传统入侵防御各自为营, 检测防御滞后的状况, 为云用户提供最大安全限度的入侵防御服务, 同时也能够确保云端抵御攻击, 做到云端和云用户双向安全的效果.

关键词: 入侵防御; 云计算; 信任理论

中图分类号: TP311.13

文献标志码: A

文章编号: 1007-7162(2014)03-0055-07

Research on Intrusion Prevention Based on Trust in Cloud Environments

Wang Shuang-tu, Han Jian-hua, Luo Jun

(School of Computers, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: Cloud computing has the nature of being dynamic, virtual and open since it was used, and all kinds of large-scale cloud security incidents make the safety of cloud environments frequently questioned. To ensure the security of cloud environments, it proposed an intrusion prevention framework model, based on trusted computing in cloud environments, by combining intrusion prevention technologies and trusted computing ideas. The model began with the principle of intrusion prevention with access to behavioral characteristics. Then, these features were gradually normalized, and the weight of each feature was determined to obtain user nodes' credibility. Next, it used a variety of cloud cluster server engines to detect defense and make integrated decision analysis and cluster analysis, enabling the cloud to make timely fast intrusion prevention, which avoids the drawbacks of the traditional intrusion prevention, such as minding only their own business, lagging behind in detecting and preventing attacks. The model provides cloud users with the maximum intrusion prevention services, and ensures that the cloud can withstand attacks, making the cloud and cloud users secure.

Key words: intrusion prevention; cloud computing; trust theory

从2006年谷歌CEO埃里克·施密特提出云计算的概念开始, 云计算就一直是业界炙手可热的研究课题. 面对着云计算的快速发展以及攻击者们恶意攻击手段的先进化和持续变化, 传统的入侵检测系统已经无法应对随机多样的网络攻击和破坏行为, 可信云^[1]和云环境下入侵防御的概念也随之诞

生. 它以云终端用户为出发点, 与可信网络^[2]的思想相结合, 对用户或者某应用程序的行为的特征进行检测、评估、聚类分析、综合决策和安全监控. 云环境下基于可信计算的入侵防御不是传统入侵检测系统的被动检测, 而是依靠云的超强计算和超大存储能力的特点, 实时采集用户或者程序代码行为特征样本,

收稿日期: 2014-04-28

基金项目: 国家自然科学基金资助项目(61142012)

作者简介: 汪双兔(1987-), 男, 硕士研究生, 主要研究方向为服务计算及其应用.

快速进行评估分析,高效处理决策.

1 国内外研究现状

1.1 可信计算及信任理论概述

1983年美国国防部制定了世界上第一个《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteria, TCSEC),第一次提出了可信计算机(Trusted Computer)和可信计算基(Trusted Computing Base, TCB)的概念,并以TCB作为计算机系统安全的基础.到了1999年,由美国IBM、Intel、HP等知名IT公司发起,成立了可信计算平台联盟(Trusted Computing Platform Alliance, TCPA).2003年将TCPA改组成为可信计算组织TCG^[1](Trusted Computing Group),这是一个非盈利性的组织,它的出现也标志着可信计算技术和应用领域的进一步扩大.

可信原本是社会学中出现的概念,而社会学中的概念往往是带有模糊性质的,可信计算把可信的概念引向了计算机科学的领域.TCG对可信的定义是:如果一个实体总是能够以预期的方式达到预期的目标,那么这个实体就是可信的.也就是说,可信强调实体行为的预期性,同时还要注重系统的安全与可靠.

信任是一种对应的二元关系,这种关系可以是一对一、一对多,也可以是多对一、多对多的.获得信任的方法主要有以下几种:直接信任,推荐信任,多级推荐信任,合并推荐.信任根是可信计算的基础,是计算机系统可信的基点.TCG认为一般的可信计算平台必须要包含3个信任根:

(1) 可信度量根 RTM(Root of Trust for Measurement)是平台启动时首先启动的一段软件,它被称为可信度量根核(Core Root of Trust for Measurement, CRTM).

(2) 可信存储根 RTS(Root of Trust for Storage)是可信平台模块(Trusted Platform Module, TPM)芯片中的一组被称为平台配置寄存器(Platform Configuration Register, PCR)的存储器和存储根密钥(Storage Root Key, SRK).

(3) 可信报告根 RTR(Root of Trust for Report)是可信平台模块TPM芯片中的平台配置寄存器PCR和背书密钥(Endersement Key, EK).

云计算中的信任管理问题是云计算环境交互的基础,本文也将会把基于模糊数学的信任理论思想拓展到云环境的入侵防御模型中来.

1.2 入侵防御技术概述

入侵防御系统是目前应用广泛的基本工具之一,可以用来防范来自入侵者对网络设备和主机的攻击,它是传统的入侵检测系统与防火墙技术的有机结合.通常情况下,入侵防御系统主要分为:基于网络的入侵防御系统(Network Intrusion Prevention System, NIPS),基于主机的入侵防御系统(Host Intrusion Prevention System, HIPS),混合的入侵防御系统和基于应用的入侵防御系统.

误用检测和异常检测是入侵防御系统常用的两种技术.异常检测是将采集的数据与之前存储的异常行为进行比较来检测可疑的入侵行为,即根据行为的欧几里得距离和标准偏差值的阈值来检测异常,高阈值说明该行为异常.与误用检测相比,异常检测有着更高的准确率,但误报率更高.常用的异常检测技术主要如下:

(1) 机器学习:系统自适应的学习来改善性能,它关注于建立一个能够在循环中优化并且根据反馈信息改变执行策略的系统.最常用技术是基于系统调用的序列分析、贝叶斯网络和马尔科夫模型.

(2) 数据挖掘:系统能够分析关联、异常、变更的重要事件来提高入侵防御的过程.分类、聚合以及关联规则发现是在IDPS技术中常用的数据挖掘技术^[2].近些年,国内外学者们都对入侵防御做了更加深入的探讨与研究,表1是最近的研究成果.

误用检测是将采集的数据与已知签名的数据库比较来检测入侵,一旦匹配就发出警报;它很大程度上依赖于数据库的更新;它的前提是所有的网络攻击的行为和方法都具有一定的模式或者特征.常用的误用检测技术有专家系统、特征分析和模型推理.

表1 研究成果

Tab. 1 Research Achievements

引用文献	年份	检测技术	审计源	管理架构	数据架构	防御能力
[3]	2009	Hybrid-signature & anomaly	主机和网络	协同	分布	无
[4]	2010	anomaly	网络	协同	分布	有
[5]	2010	anomaly	无	无	分布	无
[6]	2011	anomaly	主机	单个	分布	无
[7]	2011	anomaly	网络	协同	分布	有
[8]	2012	Hybrid-signature & anomaly	主机和网络	协同	分布	无

2 基于信任的入侵防御模型分析

云计算拥有很强的计算能力和很大的存储能

力^[4],它所提供的网络资源、服务、应用以及云用户之间的协同工作的能力对他们之间建立起来的信任关系依赖性很强.在构建入侵防御系统模型时,与可信计算思想结合,做到实体行为特征的可采集检测、行为的结果可评估、行为特征可聚类分析

2.1 模型的物理构建

Daoli^[5]是华中科技大学、武汉大学、清华大学等国内知名大学与 EMC 公司合作的并进行深入研究的项目, Daoli 项目便逐渐发展成为以可信计算支撑的云计算服务系统.在该系统中将进行恶意破坏行为的隔离部件划为 TCB, 这些就是保证系统平台安全的基础.结合 Daoli 系统,规划设计出如图 1 所示的模型中的云中 TCB 的构成.

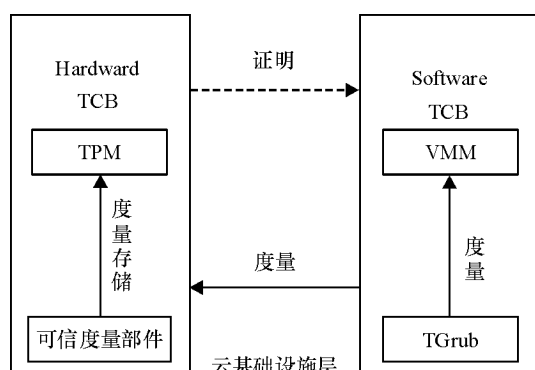


图1 云基础设施中 TCB (CTCB) 的构成

Fig. 1 Constitutes of cloud infrastructure TCB (CTCB)

在图 1 的结构中, BIOS、TPM 就是硬件的可信基. 根据 TCG 的设计, CRTM 一般是在 BIOS 中实现的, 因此图 1 中已将 CRTM 融入了模块 HTCB 中. 另外, 按照 TCB 的设计意图和思想, 它是一组核心软硬件的组合, 根据文献 [6] 可知, SRK 是 TPM 密钥管理体系中的存储根密钥, 利用该密钥的与 TPM 平台进行了有效绑定不会导出 TPM 之外的性质, 使用该密钥进行密文封装之后的数据, 即使离开了 TPM 平台依旧是无法正常的使用的. TCG 为了能够实现这一设想, 在 TPM 内部产生了一段随机数, 称为 tpmProof, 它是由 TPM 的内部来产生的, 不会导出至 TPM 之外, 同时在密文封装过程中, tpmProof 被打包到加密信息中, TPM 是无法获知 tpmProof 信息, 也就无法解密该信息的秘密. 因此本文将 VMM 和 TGrub 作为了软件可信基重要组成部分 STCB 中, 与此同时 HTCB 与 STCB 必须以一种耦合关系存在, 实现自我保护能力.

基于可信计算的云入侵防御总体模型框架如图 2 所示.



图2 基于可信计算的云入侵防御系统总体模型框架

Fig. 2 Overall model framework of trusted cloud intrusion prevention system

集群文件检测服务器将多引擎检测技术与虚拟化技术相结合, 对所有的可疑应用程序文件的行为特征进行采集并全面综合检测, 将检测的结果反馈给用户, 由云用户自己来做最后决策. 可信度评估服务器是结合图 2 中 CTCTB, 对某用户的信任度进行评估计算, 为云端提供安全策略. 综合分析服务器将这些特征进行规范化, 然后结合可信计算的信任理论进行特征综合的分析决策. 聚类分析服务器是对规范化的特征进行聚类关联分析.

2.2 模型工作步骤

该模型充分利用了云的超强计算能力和存储能力, 为海量的云用户提供安全的入侵防御服务, 对用户和用户提交的文件都进行安全性评估判断, 其主要的工作流程如图 3 所示.

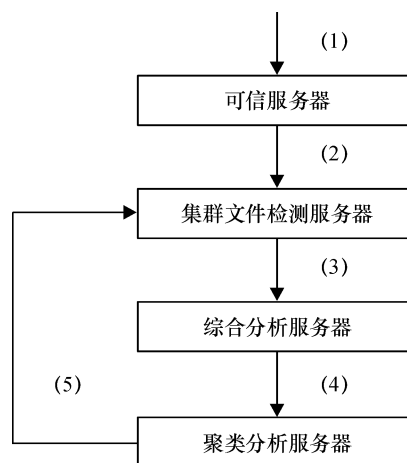


图3 模型工作步骤

Fig. 3 Model work steps

工作步骤如下: (1) 用户登录云端向云请求服务之前, 可信度评估服务器对未知可信度的用户进行评估计算, 从而确定该用户是否为可信用户. (2) 集群文件检测服务器对授权登录用户提交的文件进

行特征行为的收集,若是已知特征的恶意行为,则将结果反馈给用户,由用户最终决策,否则执行步骤(3)。(3)对未能够检测出来特征的文件即新的特征,综合分析服务器对未知文件的行为特征进行综合决策分析来判断该文件是否安全。(4)聚类分析服务器对文件的行为特征进行分类。(5)聚类分析服务器将分类结果反馈给集群检测服务器并存储到云中,使得集群检测服务器更加便捷快速来进行工作。

2.3 模型相关描述

定义1 设度量用户或者应用程序的可信程度有 n 项测量因素,即对应有 n 种行为特征集 $U = \{u_1, u_2, u_3, \dots, u_n\}$, 其测量判断集 $V = \{v_1, v_2, v_3, \dots, v_m\}$ 。

定义2 设对 n 个因素 $u_i (i = 1, 2, 3, \dots, n)$ 的判断,得到 V 上模糊集 $(r_{i1}, r_{i2}, r_{i3}, \dots, r_{im})$ 且对所有因素的判断模糊集构成了一个矩阵

$$R = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix},$$

且满足 $r_{ij} = (i = 1, 2, \dots, n; j = 1, 2, \dots, m)$, 则 r_{ij} 限定了 U 上元素和 V 上元素的关系,确定了一个模糊关系 $U \xrightarrow{R} V, U \times V \rightarrow [0, 1], (u, v) \mapsto R(u, v)$ 。

定义3 设 $A = (a_1, a_2, a_3, \dots, a_n)$ 是 U 上的模糊集, $a_i (i = 1, 2, 3, \dots, n)$ 表示第 i 个因素对其他因素的重要性,即表示对各个因素的权数分配且满足:

$$\sum_{i=1}^n a_i = 1, 0 \leq a_i \leq 1.$$

定义4 设 $U = \{u_1, u_2, u_3, \dots, u_n\}$ 为待分类的全体, $g_{ij} = G(u_i, u_j)$ 表示 u_i 和 u_j 之间的模糊相似关系,则利用最大最小法可得

$$g_{ij} = \frac{\sum_{k=1}^m \min(x_{ik}, x_{jk})}{\sum_{k=1}^m \max(x_{ik}, x_{jk})}.$$

2.4 行为特征的规范化

在进行行为特征的规范化之前,必须对用户提交的文件获取其相应的行为特征^[1],因此可以根据系统运行状况对系统的软硬件进行检测来获得。获取行为特征的方法也有很多,主要的获取方法有:入侵检测系统,如 snort 就能够监测多种网络攻击和检测;专业化的病毒查杀软件的病毒库和网络数据采集工具,如 360 云查杀、Flunk 和 NetFlow Tracker 等等。

在获取了行为特征之后,会发现所有行为特征都有着不同的表现形式,如二进制代码、具体数值等。为了便于计算用户或者应用程序的数值特征,则需要将其全部规范为 $[0, 1]$ 区间内沿正向递增的无量纲值^[12-13]。规范化过程如图4所示。

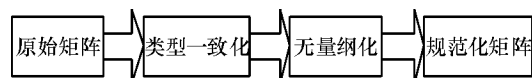


图4 规范化流程

Fig. 4 Standardization process

设初始矩阵为 $B = (b_{ij})_{n \times m}$, 则其规范矩阵为 $ET = (et_{ij})_{n \times m}$ 。若特征是以二进制表示的,则有

$$et_{ij} = \begin{cases} b_{ij}, b_{ij} \text{ 正向递增,} \\ 1 - b_{ij}, b_{ij} \text{ 正向递减.} \end{cases}$$

若特征是以具体的数值来表示的,那么就采用极差变换法^[13]规范化公式,则有

$$et_{ij} = \begin{cases} \frac{b_{ij} - (b_{ij})_{\min}}{(b_{ij})_{\max} - (b_{ij})_{\min}}, b_{ij} \text{ 正向递增,} \\ \frac{(b_{ij})_{\max} - b_{ij}}{(b_{ij})_{\max} - (b_{ij})_{\min}}, b_{ij} \text{ 正向递减,} \end{cases}$$

其中 $(b_{ij})_{\max}$ 和 $(b_{ij})_{\min}$ 分别表示获取特征的最大值和最小值。

3 特征的综合决策和聚类分析

3.1 综合决策及算例分析

综合决策服务器是在可信度评估服务器确认用户为正常用户后的基础上,负责对用户提交的未知安全文件的行为特征因素做决策分析,判断该行为是否是可信的安全行为。根据上文中的模型相关定义,用 U 上的模糊集 A 与 R 进行合成,就能够得到用户或者某些应用程序行为特征的综合决策结果

$$A \circ R = T = (t_1, t_2, t_3, \dots, t_m),$$

其中, $A = (a_1, a_2, a_3, \dots, a_n)$, $\sum_{i=1}^n a_i = 1, 0 \leq a_i \leq 1$,

$R = (r_{ij})_{n \times m}, r_{ij} \in [0, 1]$ 。那么可以得到 $t_j = \sum_{i=1}^n a_i r_{ij}, j = 1, 2, 3, \dots, m$, 如果 $\sum_{j=1}^m r_{ij} = 1$, 就有 $\sum_{j=1}^m b_j = \sum_{j=1}^m (\sum_{i=1}^n a_i r_{ij}) = \sum_{i=1}^n a_i \sum_{j=1}^m r_{ij} = \sum_{i=1}^n a_i \cdot 1 = 1$ 。

如某应用程序有 3 个因素,其因素集为 $U = \{u_1, u_2, u_3\}$ 。 u_1 表示文件一直以来正常运行, u_2 表示文件捆绑了非必须插件, u_3 表示文件携带了恶意木马病毒。根据文献^[4]划分与其对应的判断集信任等级 $V = \{v_1, v_2, v_3, v_4\}$, v_1 表示文件非常可信, v_2

表示文件可信, v_3 表示文件可信未知, v_4 表示文件为恶意文件.

决策过程为: 对于 u_1 因素若有 70% 的情况认为文件非常可信, 20% 的情况认为文件可信, 10% 认为不太可信, 则判断集为 (0.7, 0.2, 0.1, 0.0). 对于若有 u_2 因素若有 20% 的情况认为文件非常可信, 30% 的情况认为文件可信, 40% 认为不太可信, 10% 认为不可信, 那么判断集为 (0.2, 0.3, 0.4, 0.1). 对于 u_3 因素若有 30% 的情况认为文件非常可信, 40% 的情况认为文件可信, 20% 认为不太可信, 10% 认为不可信, 则判断集为 (0.3, 0.4, 0.2, 0.1). 综合得到判断矩阵

$$R = \begin{bmatrix} 0.7 & 0.2 & 0.1 & 0.0 \\ 0.2 & 0.3 & 0.4 & 0.1 \\ 0.3 & 0.4 & 0.2 & 0.1 \end{bmatrix}.$$

同时, 若某一云用户给出的权重为 $A = (0.3, 0.5, 0.2)$, 则对此应用程序的判断为: $AR = (0.37, 0.29, 0.27, 0.07)$. 按照最大隶属原则^[2], 该应用程序是非常可信的.

3.2 用户信任度计算

对于云用户本身的信任度, 也需要进行评估, 对用户的信任度进行判断的评估, 可以通过借鉴层次分析法^[13] (Analytic Hierarchy Process, AHP) 进行. 其中, 设所有相关特征组成的并进行了规范化处理证据矩阵为

$$ET = (et_{ij})_{n \times m} = \begin{bmatrix} et_{11} & et_{12} & \cdots & et_{1m} \\ et_{21} & et_{22} & \cdots & et_{2m} \\ \vdots & \vdots & & \vdots \\ et_{n1} & et_{n2} & \cdots & et_{nm} \end{bmatrix},$$

与其相对应的权重矩阵为

$$W = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1m} \\ w_{21} & w_{22} & \cdots & w_{2m} \\ \vdots & \vdots & & \vdots \\ w_{n1} & w_{n2} & \cdots & w_{nm} \end{bmatrix},$$

那么就有 $ET \cdot W^T =$

$$\begin{bmatrix} et_{11} & et_{12} & \cdots & et_{1m} \\ et_{21} & et_{22} & \cdots & et_{2m} \\ \vdots & \vdots & & \vdots \\ et_{n1} & et_{n2} & \cdots & et_{nm} \end{bmatrix} \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1m} \\ w_{21} & w_{22} & \cdots & w_{2m} \\ \vdots & \vdots & & \vdots \\ w_{n1} & w_{n2} & \cdots & w_{nm} \end{bmatrix}^T,$$

则 $ET \cdot W^T$ 主对角线上的值就是对用户信任度的判断评估值. 设该判断评估值的向量为 H , 与其对应的权重向量为 W_H . 那么由此得到该用户信任度为

$$H^T \cdot W_H =$$

$$(h_1, h_2, h_3, \cdots, h_n) (w_{h1}, w_{h2}, w_{h3}, \cdots, w_{hn})^T = \sum_{i=1}^n h_i \cdot w_{hi}.$$

对于云环境来说, 会有多个引擎来计算用户的信任度, 包括历史信任度和即时信任度, 云环境中对用户信任度的计算是基于多引擎计算机制. 若有 n 个引擎的计算结果向量为 $X = \{x_1, x_2, x_3, \cdots, x_n\}$, 则综合用户信任度为

$$\frac{H^T \cdot W_H \cdot X}{n} = \frac{\sum_{i=1}^n h_i \cdot w_{hi} \cdot x_i}{n}.$$

对未知信任度的用户, 可信服务器会将此结果反馈给集群文件检测服务器.

每当有用户发出申请服务后, 云端都会计算该用户的当前信任度. 若该用户是老用户, 那么需要对该用户的历史信任度和当前信任度进行结合更新信任度, 并计算出综合信任度; 若该用户是新用户, 则根据当前信任度即可. 实施对用户信任度的计算, 对用户进行行为的安全监控, 能够全面地提升云计算环境下共享资源中面对恶意攻击和破坏行为的入侵防御能力.

3.3 特征的聚类分析及算例分析

云聚类分析是在图2中综合决策分析服务器分析的特征结果的基础上, 聚类分析服务器对行为特征因素进行分类的过程, 将有相似或者相同特征的行为划为一类, 以此来决定哪些行为是可信的, 哪些是不可信的. 聚类分析主要有模糊等价关系聚类 and 直接聚类. 同时, 聚类分析前首先要建立起模糊相似关系, 建立模糊相似关系的方法有很多, 如: 数量积法、相关系数法、最大最小法、算术平均最小法、几何平均最小法等等. 下面的过程中将采用模糊等价关系聚类方法, 建立模糊相似关系采用最大最小法.

聚类分析过程: 采用模糊等价关系聚类时, 模糊相似矩阵 G 一般只满足自反性和对称性. 因此, 可以使用平方法求出 G 的传递闭包 $\hat{G}$, 则 $\hat{G}$ 即为模糊等价矩阵, 利用 $\hat{G}$ 便可以对 U 进行聚类分析. 例如, 对 5 个应用程序文件 $U = \{u_1, u_2, u_3, u_4, u_5\}$ 进行分类, 根据上文的综合决策过程的应用程序的因素集: 文件正常运行, 文件捆绑了插件, 文件携带木马病毒. 对这 3 个因素进行评价打分, 分数范围是 $[0, 1]$. 如得到下面 5 个评价向量: (0.5, 0.6, 0.3), (0.6, 0.7, 0.4), (0.8, 0.6, 0.2), (0.9, 0.5, 0.1), (0.7, 0.5, 0.8). 用最大最小法建立相似关系, 可以得到

$$G = \begin{bmatrix} 1.0 & 0.8 & 0.7 & 0.6 & 0.6 \\ 0.8 & 1.0 & 0.7 & 0.6 & 0.7 \\ 0.7 & 0.7 & 1.0 & 0.8 & 0.6 \\ 0.6 & 0.6 & 0.8 & 1.0 & 0.6 \\ 0.6 & 0.7 & 0.6 & 0.6 & 1.0 \end{bmatrix}.$$

然后使用平方法求传递闭包,发现

$$G^4 = G^8 = \begin{bmatrix} 1.0 & 0.8 & 0.7 & 0.7 & 0.7 \\ 0.8 & 1.0 & 0.7 & 0.7 & 0.7 \\ 0.7 & 0.7 & 1.0 & 0.8 & 0.7 \\ 0.7 & 0.7 & 0.8 & 1.0 & 0.7 \\ 0.7 & 0.7 & 0.7 & 0.7 & 1.0 \end{bmatrix},$$

因此 G^4 便是 G 的传递闭包,即为所求的等价矩阵,接着对 G^4 进行聚类.

$$G_{1.0} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

那么相应的分类为: $\{u_1\}, \{u_2\}, \{u_3\}, \{u_4\}, \{u_5\}$.

$$G_{0.8} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

相应的分类为 $\{u_1, u_2\}, \{u_3, u_4\}, \{u_5\}$. 同时

$$G_{0.7} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

相应的分类为 $\{u_1, u_2, u_3, u_4, u_5\}$. 由此能够得到:

(1) 当 $0 \leq \lambda \leq 0.7$ 时,将 U 分为 1 类. (2) 当 $0.7 \leq \lambda \leq 0.8$,将 U 分为 3 类. (3) 当 $0.8 \leq \lambda \leq 1.0$,将 U 分为 5 类.

当然,在求解传递闭包之前需要求证该传递闭包是否存在以及在采用平方法求传递闭包时工作量太大,无法实时进行防御都是未来研究中需要解决的问题.

4 结论

本文从云计算环境出发,结合可信计算的信任理论,提出了一个云环境中基于可信计算的入侵防御模型. 该模型将应用程序多种行为特征因素进行

检测分析,然后综合决策和进行聚类分析,分类出哪些行为是可信的,哪些是恶意攻击行为. 该模型还结合层次分析法(AHP)对用户的可信度进行计算,确保该用户本身是安全可信的,不会对其他用户造成恶意攻击的威胁. 未来的研究重点:一是针对判断特征因素过多时,如何采用合适的多级判断来合理地决定出权数分配. 二是如何解决云环境中信任管理问题来保证云环境中的安全交互. 三是在聚类分析被分类的对象过多时,如何去解决用模糊等价关系进行聚类问题.

参考文献:

- [1] 李虹,李昊. 可信云的安全关键技术与实现 [M]. 北京:人民邮电出版社,2010.
- [2] 张焕国,赵波. 可信计算 [M]. 武汉:武汉大学出版社,2011.
- [3] 张巍,刘峰,滕少华. 改进的 PrefixSpan 算法及其在序列模式挖掘中的应用 [J]. 广东工业大学学报,2013, 30(4): 49-54.
- [4] Zhang W, Liu F, Teng S H. Improved prefixspan algorithm and its application in sequential pattern mining [J]. Journal of Guangdong University of Technology, 2013, 30(4): 49-54.
- [5] Vieira K, Schuler A, Westphal C. Intrusion detection for grid and cloud computing [J]. IT Professional, 2010, 12(4): 38-43.
- [6] Takahashi T, Kadobayashi Y, Fujiwara H. Ontological approach toward cybersecurity in cloud computing [C] // 3rd International Conference on Security of Information and Networks. Russian Federation Taganrog, Rostov-on-Don: [s. n.], 2010: 318-323.
- [7] Smith D, Guan Q, Fu S. An anomaly detection framework for autonomic management of compute cloud systems [C] // 34th Annual Computer Software and Applications Conference Workshops (COMPSACW). Seoul: [s. n.], 2010: 376-381.
- [8] Xin W, Ting lei H, Xiao-yu L. Research on the Intrusion detection mechanism based on cloud computing [C] // 2010 International Conference on Intelligent Computing and Integrated Systems (ICISS). Guilin: [s. n.], 2010: 125-128.
- [9] Dhage S, Meshram B, Rawat R, et al. Intrusion detection system in cloud computing environment [C] // International Conference & Workshop on Emerging Trends in Technology. USA New York: IEEE, 2011: 235-239.
- [10] Jin H, Xiang G, Zou D, et al. A VMM-based intrusion prevention system in cloud computing environment [J]. The Journal of Supercomputing, 2013, 73(3): 679-694.

- [10] 雷葆华,饶少阳. 云计算解码 [M]. 北京: 电子工业出版社, 2011.
- [11] 秦攀. 云防御系统中多引擎检测机制研究 [D]. 武汉: 华中科技大学计算机学院, 2012.
- [12] 徐小龙, 吴家兴, 杨庚. 一种基于 Cloud-P2P 计算模型的恶意代码联合防御网络 [J]. 计算机应用研究, 2012, 29(6): 2215-2217.
Xu X L, Wu J X, Yang G. Malicious code united. defense network based on Cloud-P2P model [J]. Application Research of Computer, 2012, 29(6): 2215-2217.
- [13] 胡明礼, 范成贤, 史开全. 区间数决策矩阵规范化方法的性质分析 [J]. 计算机科学, 2013, 40(10): 203-207.
Hu M L, Fan C X, Shi K Q. Character analysis of standardization methods of decision matrix with intervals [J]. Computer Science, 2013, 40(10): 203-207.
- [14] 周茜, 于炯. 云计算下基于信任的防御系统模型 [J]. 计算机应用, 2011, 31(6): 1532-1535.
Zhou Q, Yu J. Defense system model based on trust for cloud computing [J]. Journal of Computer Applications, 2011, 31(6): 1532-1535.
- [15] 刘新宪, 朱道立. 选择与判断-AHP 层次分析法 [M]. 上海: 上海科学普及出版社, 2008.

(上接第 48 页)

- [1] 张光卫, 李德毅, 李鹏, 等. 基于云模型的协同过滤推荐算法 [J]. 软件学报, 2007, 18(10): 2403-2411.
Zhang G W, Li D Y, Li P, et al. A collaborative filtering recommendation algorithm based in cloud model [J]. Journal of Software, 2007, 18(10): 2403-2411.
- [2] Ma H, King I, Lyu M R. Effective missing data prediction for collaborative filter [C] // Proceedings of the 30th Annual International ACM SIGIR Conference. Netherlands Amsterdam [S. n], 2007: 39-46.
- [3] Ganesan P, Garcia-Molina H. Exploiting hierarchical domain structure to computer similarity [J]. ACM Transactions on Information Systems, 2003, 21(1): 64-93.
- [4] 王茜, 王均波. 一种改进的协同过滤推荐算法 [J]. 计算机科学, 2010, 37(6): 226-234.
Wang Q, Wang J B. Improved collaborative filtering recommendation algorithm [J]. Computer Science, 2010, 37(6): 226-234.
- [5] 韦素云, 业宁, 朱健, 等. 基于项目聚类的全局最近邻的协同过滤算法 [J]. 计算机科学, 2012, 39(12): 149-152.
Wei S Y, Ye N, Zhu J, et al. Collaborative filtering recommendation algorithm based on item clustering and global similarity [J]. Computer Science, 2012, 39(12): 149-152.
- [6] 汪静, 印鉴. 一种优化的 Item-based 协同过滤推荐算法 [J]. 小型微型计算机系统, 2010, 31(12): 2337-2342.
Wang J, Yin J. Optimized item-based collaborative filtering recommendation algorithm [J]. Journal of Chinese Computer Systems, 2010, 31(12): 2337-2342.
- [7] 杨兴耀, 于炯, 吐尔根·依布拉音, 等. 综合用户和项目预测的协同过滤模型 [J]. 计算机应用, 2013, 33(12): 3354-3358.
Yang X Y, Yu J, Ibrahim T, et al. Collaborative filtering model combining users and items predictions [J]. Journal of Computer Applications, 2013, 33(12): 3354-3358.