文章编号:1671-4598(2018)07-0128-04 DOI:10.16526/j.cnki.11—4762/tp.2018.07.028 中图分类号:TP273 文献标识码:A

云计算架构中恶意代码入侵自动监测系统设计

郭 雅,骆金维,李泗兰
(广东创新科技职业学院 信息工程学院,广东 东莞 523960)

摘要:为了解决云计算架构中恶意代码以各种形式入侵产生损害,不能及时发现、维护而造成云计算架构安全性能降低,无法正常使用的问题,建立一套基于BP神经网络的入侵监测系统,实现对云计算架构中恶意代码入侵的自动监测,对及时监测入侵恶意代码及有效增加云计算架构安全有着直接而又重要作用;系统以STM32F103ZET6为主控芯片构建MUC主控单元,并通过EZ—USB FX2 USB2.0控制芯片将各个模块与其相连;采用LM2575系列的稳压器,为系统提供电源;软件设计过程中,采用BP神经网络法计算各恶意代码入侵的输出值,降低监测误差;通过实验测试表明,该系统可实现云计算架构中入侵恶意代码的自动监测功能,且具有扩展性强、操作方便等特点,对云计算架构的使用安全性具有重要的应用价值。

关键词:云计算架构;恶意代码;入侵;自动;监测;系统

Design of Malicious Code Intrusion Automatic Monitoring System in Cloud Computing Architecture

Guo Ya, Luo Jinwei, Li Silan
(School of Information Engineering, Guangdong Innovative Technical College, Dongguan 523960, China)

Abstract: In order to solve the malicious code of cloud computing architecture in various forms of intrusion damage, can not be found in time and maintenance caused by cloud computing architecture, safety performance is reduced, the normal use is disrupted, Based on a BP neural network intrusion detection system, realize the calculation of automatic monitoring in the framework of the invasion of the malicious code on the cloud, have an important role in the direct and timely monitoring of security computing architecture intrusion malicious code and effectively increase the cloud system; using STM32F103ZET6 as main control chip of the main control unit of MUC, and the EZ—USB FX2 USB2.0 control chip is connected with each module; using LM2575 series voltage regulator, power supply system; software design process, the output of the calculation of the invasion of the malicious code the value of using BP neural network method, reduce the monitoring error; the experiments show that the system can achieve the cloud The automatic monitoring function of intrusion malicious code in the architecture has the characteristics of strong expansibility and easy operation, and has important application value to the security of the cloud computing architecture.

Keywords: cloud computing architecture; malicious code; intrusion; automatic; monitoring; system;

0 引言

恶意代码又称恶意软件,是在未明确提示用户或未经用户许可的情况下,在用户计算机或其他终端上安装运行,侵犯用户合法权益的软件[1]。其入侵手段多样,造成的损失成上升趋势,共享与安全的矛盾逐渐凸显[2],已成为国家网络经济发展的关键[3]。据统计:信息窃贼在过去几年中以250%速度增长,超过90%的大公司都发生过恶意代码入侵事件[4]。恶意代码入侵自动监测系统作为保证计算机安全的重要手段,对其的研究逐渐成为相关专家学者研究的热点课题[5]。

为了优化恶意代码入侵监测系统,达到监测的高效性及有效性,提出基于BP神经网络的云计算架构中恶意代码入侵自动监测系统设计方法,实验结果表明,所提方法进行恶意代码入侵监测,监测的准确度较高,丢包率较少,推动了该课题向应用领域迈进。

1 监测系统整体方案设计

云计算架构中恶意代码入侵自动监测系统主要由STM32主控板、传感器、指南针模块、信号调节电路、数据转换模块等模块组成,具体系统设计的参数如表1所示。

表1 云计算架构中恶意代码入侵自动监测系统参数

项目	数值
控制板	STM32
调节精度	2pm
采样率	250Hz
系统复用能力	可接入512个FBG传感器

收稿日期:2017-09-06; **修回日期**:2017-11-29。

作者简介:郭 雅(1980-),男,广东信宜人,实验师,主要从事计算机网络,网络安全,云计算方向的研究。

1.1　整体框架设计

由图 1 可知，系统所用的传感器电路都已模块化，监测到的信号输出为高低电平，可以实现直接与 ARM 芯片的通信，通过对云计算构架中的数据信号进行滤波放大和 A/D 转换，从而实现对云计算构架中信号的预处理，在此基础上，对云计算构架中信号进行监测，确定云计算环境下恶意代码入侵信号，完成对恶意代码入侵的自动监测。

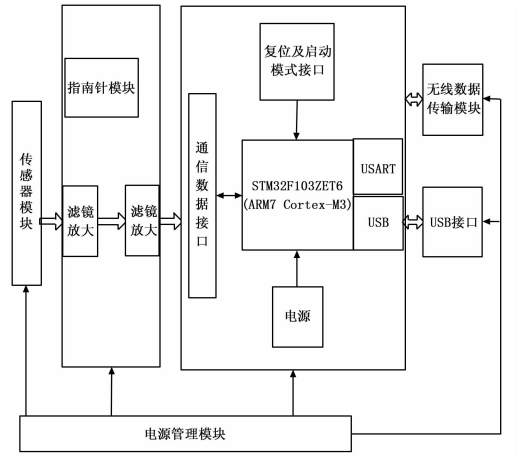

图 1　整体框架设计

1.2　MUC 主控单元

本文设计的云计算构架中恶意代码入侵自动监测系统以 STM32F103ZET6 为主控芯片，STM32 系列[6]以 ARM Cortex－M3 为核心，具有提高系统的性能，降低系统的成本和功耗的优点，STM32F103 作为 STM32 的增强型，是同类产品中具有最高性能的产品，其优点主要体现在以下几方面。

1）超低的产品价格。

2）外设较多。

3）具有较好的实时性。

4）功耗较低。

因此，该芯片符合恶意代码入侵自动监测系统需求的处理速度快，实时性好等内容。

1.3　USB 接口控制芯片

USB 协议[7]的复杂性意味着 USB 外设必须具有智能，因此利用控制芯片实现对 USB 端口事件进行监测，芯片的选择取决于芯片所要执行的功能，本文选用的 USB 接口控制芯片是由 Cypress 公司推出的带智能 USB 接口的 EZ－USB FX2 USB2.0 控制芯片，包含智能串行接口，能完成所有基本的 USB 功能。

1.4　电源电路

在上图恶意代码入侵自动监测系统电源电路中，为了保证系统电压的稳定性和精度，本文采用 LM2575 系列的稳压器实现对 12 V－5 V 的电路转化，LM2575 系列芯片的最大输出电路为 45 V，输出电压为 5 V，利用电源电路，保证系统正常运行。

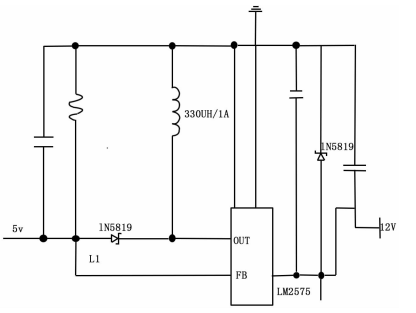

图 2　系统电源电路

1.5　时钟电路

为了保证系统自动监测的及时性，需要对系统的时钟电路进行设计，本文设计的恶意代码入侵自动监测系统时钟电路如图 3 所示。

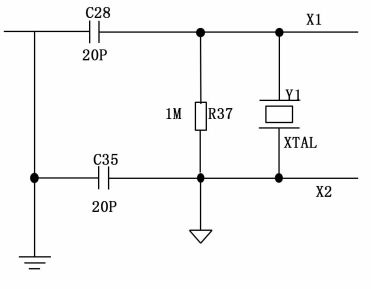

图 3　恶意代码入侵自动监测系统时钟电路

在云计算构架中恶意代码入侵自动监测系统时钟电路中，本文采用的振荡源是 12 MHz，其两个引脚连接 X1、X2 引脚，从而形成闭合回路，并配合内部的震荡工期实现恶意代码入侵自动监测系统时钟电路。并且，将晶振的两个引脚与匹配电容和匹配电阻进行连接，从而提高恶意代码入侵自动监测系统的稳定性。

1.6　复位电路

为实现恶意代码入侵自动监测系统复位，需要对系统的复位电路进行设计，本文设计的系统复位电路如图 4 所示。

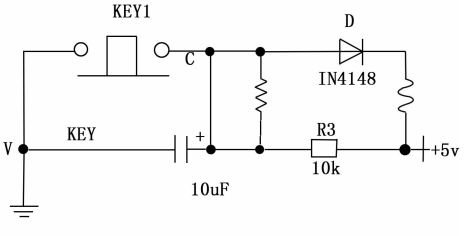

图 4　复位电路设计

上图中，恶意代码入侵自动监测系统复位电路是利用 TMS320LF2407A 进行初始化，在系统运行过程中，实现对恶意代码入侵的监测，恶意代码入侵自动监测系统复位电路主要可以分为手动复位和自动复位两种，本文中为实现

自动监测，并保证监测效率，采用了手动复位和自动复位相结合的复位方式，根据系统运行的实际勤快，选择自动复位和手动复位。

1.7 数据采集处理模块

数据采集和预处理是整个恶意代码入侵自动监测系统的核心组件，通过从云计算构架中获取网络数据报文，为其他模块的顺利进行奠定基础。数据采集模块的性能直接影响采集的准确性。

本文设计的数据采集模块是基于数据平面开发套件技术实现的。在此基础上，通过对采集的数据进行 IP 报文重组以及 TCP 流汇聚，主要目的是保证应用层数据的连续性，方便监测模块进行监测。

1.8 数据监测模块

恶意代码入侵自动监测系统入侵监测是通过监测引擎模块、脚本运行模块、特征库模块和实施关联引擎组成的，通过这四个模块配合，实现入侵监测系统的攻击监测流程。

监测引擎模块是入侵监测的核心模块，通过数据模式匹配，实现对恶意代码的识别。脚本运行引擎模块是通过 Y 语言开发的，利用特征库模块，对云计算构架中恶意代码入侵的行为特征进行定义，从而识别相应的攻击事件。关联事件与监测引擎监测到的基本监测事件是相对应的，通过关联引擎实现对云计算构架中跨会话的和复杂的会话内的恶意代码入侵监测，并且，还可以利用关联引擎实现多种日志过滤功能。

2 软件设计

在进行云计算架构中恶意代码入侵自动监测系统设计过程中，监测的准确性和及时性对系统的性能具有重要影响。误差逆传播网络（BP 网络）具有较强的映射能力，BP 网络是一个多层次网络，其中最基本的网络拓扑结构是通过输入层、隐含层、输出层三个神经元层次组成，通过将相邻层的神经元之间进行连接，从而实现 BP 神经网络。

BP 神经网络是一种监督式的学习算法[8]，其思想如下：BP 神经网络由模式顺传播、误差逆传播、记忆训练、学习收敛四个过程组成，其通过连续不断的在相对于误差函数斜率下降的方向上计算网络权值和变差变化而逐渐逼近目标[9]，从而提高云计算构架下恶意代码入侵自动监测系统监测的准确度。

BP 神经网络所用到的计算过程如下所述：

设定输入节点的输入为 x_j，隐含节点的输出可以表示为：

$$y_i = f(\sum_j w_{ij}x_j - \theta_i) = f(net_i) \tag{1}$$

式中，w_{ij} 表示连接权值，θ_l 表示云计算构架中节点阈值，$f(\cdot)$ 表示传递函数，$net_i = \sum_j w_{ij}x_j - \theta_l$。输出节点的输出可以表示为：

$$O_l = f(\sum_i T_{ij}y_i - \theta_l) = f(net_l) \tag{2}$$

式中，T_{ij} 表示输出节点的实际输出值。

设定 t_1 表示云计算中输出节点的期望输出值，则对其进行误差控制的过程可以表示为：

$$E = \sum_{k=1}^{P} e_k < \varepsilon \tag{3}$$

式中，P 表示监测的样本数，n 表示 BP 神经网络的输出节点数，ε 表示目标误差，$e_k = \sum_{l=1}^{n} | t_l^{(k)} - o_l^{(k)} |$ 表示误差系数。

BP 神经网络的误差公式可以表示为：

$$\delta_l = (t_l - o_l) \times o_l \times (1 - o_l) \tag{4}$$

权值修正公式可以表示为：

$$T_{ij}(k+1) = T_{ij}(k) + \eta\delta_l y_i \tag{5}$$

式中，k 表示权值修正的迭代次数，η 表示神经网络的学习系数。阈值修正可以表示为：

$$\theta_l(k+1) = \theta_l(k) + \eta\delta_l \tag{6}$$

输出节点的误差公式可以表示为：

$$E = \frac{1}{2}\sum_l (t_l - o_l)^2 = \sum_l \left[t_l - f(\sum_i T_{ij} f(\sum_j w_{ij}x_j - \theta_i) - \theta_l)\right]^2 \tag{7}$$

为了实现云计算架构中恶意代码入侵监测系统设计，训练了一个 BP 神经网络，首先对云计算构架中网络加权输入矢量、网络输出以及误差矢量进行计算，并求得误差平方和[10]，将所训练矢量的误差平方和与目标误差进行对比，当小于目标误差，则停止训练，否则在输出层计算误差变化，以反向传播学习规划实现对目标权值的调整，并重复次过程，直到误差平方和小于目标误差。

基于 BP 神经网络的云计算架构中恶意代码自动入侵监测系统的监测流程可以表述为：首先初始化网络，并采集云计算架构中的恶意代码入侵数据，给出训练样本，利用 BP 神经网络计算各神经元的输出值，从而确定监测的误差，根据监测的误差，调整网络权值，降低监测的误差，从而提高监测的准确度。通过上述论述，实现系统的软件设计，并结合 2.1，从而完成云计算架构中恶意代码入侵自动监测系统设计。

3 系统测试分析

3.1 实验参数与环境

为了证明本文所提方法设计的基于 BP 神经网络的云计算架构中恶意代码入侵自动监测系统的使用效果，进行了一次实验，实验过程中，本文采用基于 WNIDS 的实验系统，测试平台如表 2 所述，实验对象如图 5 所示，通过将不同方法应用至该试验对象，观察不同方法的整体性能。

表 2 实验测试平台配置

配置	监测主机
CPU 主频	Celeron－1.1GHz
硬盘容量	40GB
RAM 容量	256MB
操作系统	Windows 2000 Advanced server
网络适配器	Realtek Rtl81399(A)PCI Fast Ethernet Adapter

1）恶意代码入侵自动监测系统监测的丢包率是判断恶意代码入侵自动监测系统运行性能的重要指标，图 6 是不同方法设计的系统监测的丢包率对比。

2）在恶意代码入侵自动监测系统中通过正常节点与恶意节点的信任度确定网络的安全度，图 7 是本文所提方法正常节点与恶意节点的信任度对比。

3）在恶意代码入侵自动监测系统中，监测的及时性是评价监测系统的另一重要指标，其保证了安全数据的正常流入及恶意代码入侵的及时识别，图 5 是不同方法监测的响应时间对比。

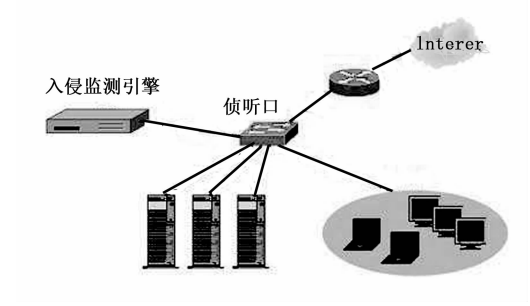

图 5　实验对象

3.2　实验结果

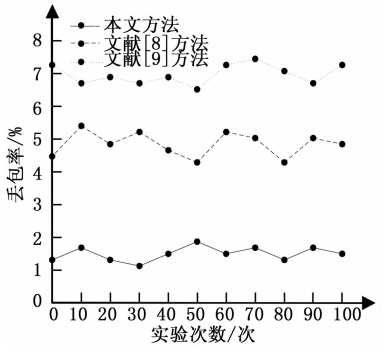

图 6　不同方法设计的系统监测的丢包率对比

通过图 6 可以看出，本文所提方法设计的系统丢包率低于文献［8］和文献［9］方法设计的系统监测的丢包率，说明本文所提方法设计的系统能够全面的对云计算构架中的访问进行监测，本文所提方法设计的系统利用 BP 神经网络算法，对监测过程中的误差进行调整，提高了监测的范围，因此具有较低的丢包率。

通过对图 7 的分析可知，本文所提方法设计的系统在监测过程中，正常访问的信任度之不低于 70%，恶意代码入侵访问的信任度不超过 40%，因此，本文所提方法能够准确对云计算架构中恶意代码入侵进行识别，由于本文所提方法设计的系统增加了数据采集处理模块和数据监测的模块，因此提高的监测的准确性。

通过图 8 可以看出，本文所提方法设计的系统响应速度快于文献［8］和文献［9］方法设计的系统监测的响应速度，因此本文所提方法能够较好的保证系统对云计算架构中恶意代码入侵监测的及时性。综上所述，本文所提方法设计的系统能够较好的保证监测的准确度和及时性，为该课题的研究发展奠定基础。

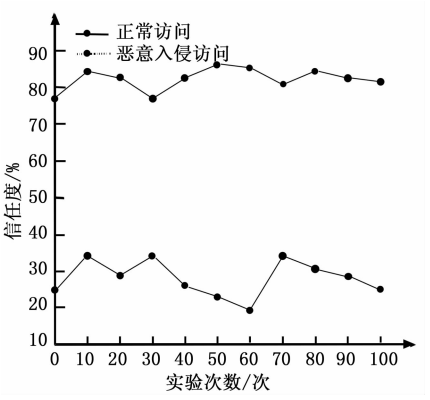

图 7　本文所提方法正常节点与恶意节点的信任度对比

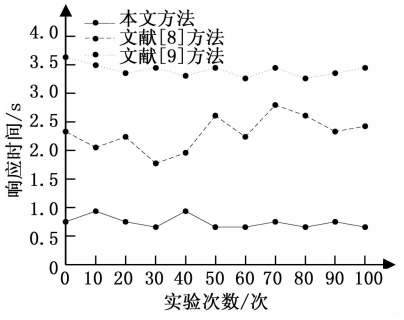

图 8　不同方法监测的响应时间对比

4　结束语

在云计算架构中，恶意代码及其它入侵形式都需要有监测，监测自动进行就显得尤为重要。本文介绍了自动监测系统在云计算架构中恶意代码入侵中的实际应用。从系统整体结构、软硬件设计及系统测试角度对云计算架构中恶意代码入侵自动监测系统进行深入介绍，利用仿真及实测相结合的形式证明了系统的可行性。

参考文献：

[1] 王世运．弱关联规则下的联合数据库入侵检测方法研究［J］．科技通报，2015，31（3）：184－187.

[2] 王　萍，卢明立，杨志明，等．大型刮板输送机哑铃销断裂检测系统设计［J］．科学技术与工程，2016，16（10）：109－111.

[3] 陈　琳，李　勇，王　磊．面向物联网的 Sybil 入侵防御系统设计与实现［J］．计算机测量与控制，2017，25（3）：180－183.

[4] 赵晓君，王小英，张咏梅，等．基于恶意代码行为分析的入侵检测技术研究［J］．计算机仿真，2015，32（4）：277－280.

[5] 林　辉．基于粒子群和模糊数学的入侵检测系统的研究［J］．电子设计工程，2016，24（14）：24－26.

（下转第 136 页）