



文章编号:1671-251X(2013)04-0047-04

DOI:

聂晓. 基于云计算的物联网安全研究[J]. 工矿自动化, 2013, 39(4): 47-50.

基于云计算的物联网安全研究

聂晓

(广东机电职业技术学院 信息工程学院, 广东 广州 510515)

摘要:介绍了云计算与物联网的概念,分析了二者结合的必然性与结合模式,提出了基于云计算的物联网体系结构,研究了基于云计算的物联网所面临的安全威胁问题,并针对安全威胁给出了相应的解决方案,即构建可信的物联网环境和如何保证“云”中的物联网数据安全,指出了基于云计算的物联网安全研究的技术难点和研究现状。

关键词:云计算; 物联网; 安全威胁; 数据安全; 同态加密技术

中图分类号:TD67

文献标志码:A

网络出版时间:

网络出版地址:

Security research of Internet of Things based on cloud computing

NIE Xiao

(College of Information Engineering, Guangdong Jidian Polytechnic, Guangzhou 510515, China)

Abstract: The paper introduced concepts of cloud computing and Internet of Things, analyzed inevitability and combination mode of the cloud computing and the Internet of Things. It proposed architecture of the Internet of Things based on cloud computing and studied security threats of the Internet of Things based on the cloud computing and gave corresponding security solution including how to construct trusted environment for the Internet of Things and how to protect data security in the cloud of the Internet of Things. It pointed out technical difficulties of the security research and research status of the Internet of Things based on the cloud computing.

Key words: cloud computing; Internet of Things; security threats; data security; homomorphic encryption technology

0 引言

近年来,云计算与物联网、智慧地球等概念备受关注,物联网和云计算已成为我国非常重视的战略新兴产业。物联网产业有巨大的发展潜力和广泛的应用领域,而在其推进过程中,通过传感器收集信息已不是难题,感知信息在网络上的传输也不是问题,实质的难点在于如何对海量信息进行分析和处理,并对物体实施智能化的控制。要解决这个问题,

就必须建立一个功能强大的智能处理平台,而云计算正是这样一个具备海量信息存储和处理的平台,因此,二者的结合将是未来的趋势。本文在研究物联网与云计算结合的基础上,着重对基于云计算的物联网安全进行研究。

1 云计算与物联网概述

1.1 云计算

云计算是由分布式计算、网格计算、虚拟化技术

收稿日期:2013-01-08。

作者简介:聂晓(1976—),男,湖南娄底人,讲师,硕士,现主要从事计算机应用技术方面的科研与管理工作,E-mail:Brenner@21cn.com。

等诸多网络技术发展而来的新兴技术,自2006年首次提出这个概念以来,云计算已成为IT行业研究的热点,但长期以来没有标准定义,目前业界高度认可的云计算定义如下:云计算是一种服务或资源的交付和使用模式,通过这种模式可以减少管理资源的工作量,降低用户和服务提供商之间的交互^[1]。

云计算所提供的服务既可以是基础设施(IaaS:基础设施即服务)和软件(SaaS:软件即服务)、平台(PaaS:平台即服务),也可以是其他服务,这说明计算能力也可像日常的商品一样通过互联网进行流通使用。

1.2 物联网

物联网属于新一代的信息技术,即“The Internet of Things”,指通过传感等设备,把任何物品与互联网依照约定的协议连接起来,并进行实时信息交换和通信,最终实现智能化控制和管理的一种网络。是一种基于互联网的、物-物相连的网络。

实现物联网的关键技术包括RFID技术、传感技术、无线传感网络技术、人工智能技术、虚拟机技术、云计算平台。其中云计算平台是物联网发展的技术支撑,可以为物联网提供海量信息的存储、计算能力。

1.3 云计算与物联网的结合

(1) 二者结合的必然性。云计算具备无处不在的网络访问能力、超强的计算能力、大量信息的存储能力、高可伸缩性等优势^[2],而物联网恰恰需要一个这样的智能处理平台,因此,物联网采用云计算平台进行智能处理,必将最大限度地发挥物联网与云计算的优势,促进物联网产业和云计算的强劲发展。

(2) 结合模式。目前云计算与物联网的结合主要采用以下几种模式:①单中心、多终端模式;②多中心、大量终端模式;③信息、应用分层处理、海量终端模式^[3]。参考文献[4]已有论述,在此不再赘述。

(3) 二者的关系。实质上,从物联网的角度来看,云计算平台为物联网提供海量信息存储和智能处理的功能,本文将此功能划分到物联网应用层。而从云计算平台的角度来看,物联网是云计算平台所提供的一种云应用,换言之,物联网是一种带有传感器的云应用。

2 基于云计算的物联网体系结构

根据物联网对信息的感知、传输和处理的过程,将其划分为3层结构,即感知层、网络层和应用层,如图1所示^[4]。

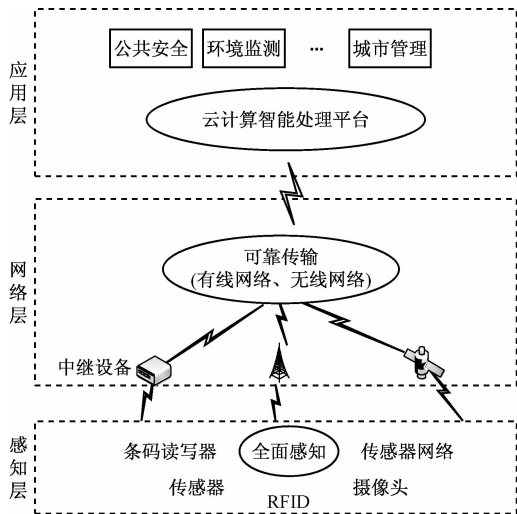


图1 基于云计算的物联网体系结构

(1) 感知层。利用感知设备在任何时间、对任何地点的物体实现识别,完成信息的采集。

(2) 网络层。通过现有的通信和互联网络,将感知到的物体信息可靠地传递给用户,实现信息的传输。

(3) 应用层。利用云计算平台对用户的数据和信息进行智能处理,实现对物体的控制,完成物与物、人与物之间的信息交换。

3 基于云计算的物联网安全威胁

3.1 感知层安全威胁

在感知层,由于节点的硬件结构相对简单,存储能力和计算能力较弱,传统的保密技术难以在节点上实现,因此,容易受到各种攻击^[4]。这些攻击包括节点控制、节点捕获、拒绝服务攻击及认证攻击。

3.2 网络层安全威胁

在网络层,由于网络的异构,可能导致跨网认证攻击、认证攻击(如中间人攻击等),同时随着网络规模增大以及对于分布式信息的处理,容易受到拒绝服务攻击、路由攻击等威胁。

3.3 应用层安全威胁

物联网应用层除了终端用户的认证外,重点是来自云计算平台的安全威胁。

3.3.1 针对云计算平台的安全威胁

云计算平台提供的服务应是无处不在、无时不在的,要保证云计算平台具备高可靠性,即保证云计算平台提供的服务不中断,在面临恶意攻击时避免系统崩溃的风险,因此,云计算平台应具备抵抗外来攻击的能力。

3.3.2 “云”中的物联网数据安全

(1) 数据的隐私问题。终端用户的数据上传到“云”中之后,随机地存储在云计算平台的服务器上,而这些服务器可能分布在世界各地,终端用户无法知道自己的数据具体被存储在什么位置,因此,云计算平台要保证终端用户的数据存储安全性。另一方面,当终端用户把自己的数据交付给云计算平台之后,由于云计算平台要对数据进行分析 and 处理,因此,享有了对数据的优先访问权,导致数据的拥有者失去了数据的完全控制能力。所以,要防止云计算平台在对数据进行分析和处理的过程中泄密,保证物联网用户数据在传输和使用过程中的机密性变得非常重要。

(2) 虚拟化管理带来的安全问题。目前云计算平台主要通过虚拟化技术实现多租户共享资源,多个虚拟机可能被绑定到同一个物理资源上,如果云计算平台无法实现用户之间数据的有效隔离,那么用户的数据就可能被其他用户非法访问,云计算平台就无法使用户相信自己的数据是安全的。

4 基于云计算的物联网安全研究

4.1 安全体系结构

针对上述物联网体系结构中每一层所面临的安全威胁,给出相应的解决方案和关键技术难点研究,如图2所示。

其中感知层和网络层的关键技术目前已有大量研究并取得较快的进展,本文着重分析物联网应用层,即云计算平台的安全方案,从以下几个方面考虑。

4.1.1 构建物联网可信环境

云计算平台要为物联网应用提供安全的数据存储、超强的计算能力,必须保证云计算平台本身的可靠,即构建物联网的可信环境。一方面云计算平台应与传统计算平台一样采取严密的安全措施,从物理安全、系统安全、网络安全、数据库安全等方面做

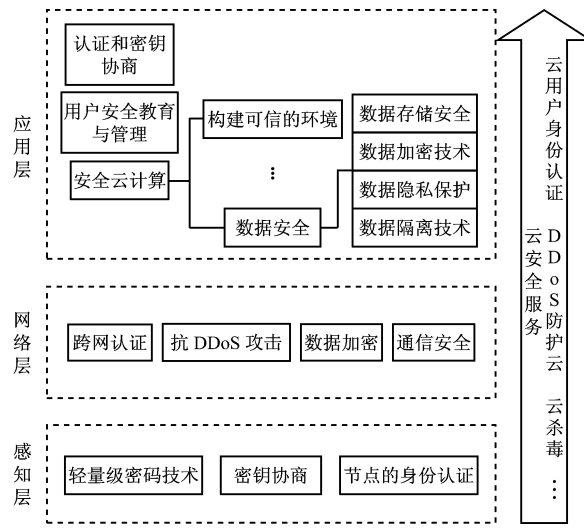


图2 基于云计算的物联网安全体系结构

好安全防范工作,保证云计算平台本身具备抗攻击能力;另一方面,云计算平台要向物联网用户证明自己具备数据隐私保护能力,首先自己无法破坏用户数据,其次攻击者得到数据也无法理解用户数据,例如可采用密文保存数据^[5]。

4.1.2 基于云计算的数据安全防护

(1) 保证数据存储的安全性。用户数据存储在世界各地的服务器,要保证数据存储的安全性,除在构建物联网可信环境的基础上,还要采取数据备份的方法保护数据,数据备份系统要充分考虑到数据的兼容性,存储设备的高扩展性以及大量物联网应用实体并发访问时的服务能力等。

(2) 数据的机密性和完整性防护。为了保护数据隐私,物联网用户要采取加密手段,使得敏感数据以密文的形式存储在服务器上,然而数据经过加密成为密文之后,会导致云计算平台的大多数数据分析方法失效,因此,研究如何高效率地对密文进行分析和处理显得非常重要,目前对密文处理的研究集中在同态加密算法设计上。

(3) 数据隐私保护。用户的数据从被感知开始,到进入云计算平台,从传输到使用的过程,都存在泄漏用户隐私的风险,因此,采取数据隐私保护技术是必需的。

(4) 数据隔离技术。在虚拟化条件下,存储在同一物理服务器上的不同虚拟机之间可能存在非法访问,云计算平台要使用户相信数据是安全的,必须对用户的数据提供有效隔离,防止同一物理设备上的其他用户非法访问,更加有效地保护数据安全。

同时物联网作为云计算平台的一种应用,也可以在各个阶段享受云安全服务,例如云用户身份认证、DDoS(Distributed Denial of Service)防护云、云杀毒等。

4.2 技术难点及研究现状

4.2.1 同态加密技术

在使用加密技术^[6]保护用户数据隐私的同时,云端存储的是敏感信息的密文,因此,如何高效地对密文进行处理和使用则成为关键。同态加密技术将是解决这一问题的首选方案。使用同态加密技术,可以使数据总是处于加密状态,这样攻击者即使得到数据,也无法理解数据的内容。同态加密的思想起源于私密同态,同态加密方案需要支持2种最基本的运算——加法和数量乘法,目前研究较多的同态加密算法^[7]包括希尔密码算法(Hill Cipher)、迭代的希尔密码算法(Iterated Hill Cipher, IHC)和MRS(Modified Rivest'S Scheme)算法等。近期IBM研究人员Craig Gentry已研究出一种完全同态加密方案,该方案可以让用户充分地操作加密状态的数据,高速地完成对密文的检索和处理,即不需要解密就能对已加密的数据进行处理,实现与对原始数据直接进行处理相同的效果。此方案已在理论上取得一定突破,预期将得到实用化进展。同态加密技术在物联网认证与访问控制、云计算等方面的应用,将是今后研究的重点。

4.2.2 隐私保护技术

在物联网各个阶段都涉及数据隐私的保护,目前研究较多的隐私保护技术有k-匿名算法、图匿名、空间加密等,参考文献[5]讨论了国外在隐私处

理技术上的研究进展,参考文献[6]对匿名算法做了详细分析。有关保护用户隐私方面的安全技术还有很大的研究空间。

5 结语

云计算平台是物联网大规模发展的有力支撑,同时物联网的发展也为云计算平台的广泛应用提供大量的用户,因此,二者的结合势在必行,而基于云计算的物联网安全研究将为二者的发展提供最可靠的保障,也是二者能够大规模应用的必要条件。在分析了二者结合的必然性之后,给出了基于云计算的物联网体系结构,针对其面临的安全威胁,对数据安全做了重点研究。

参考文献:

- [1] 王霄飞. 云计算在我国的发展现状及在军事上的应用展望[J]. 价值工程, 2012(6):164-165.
- [2] 张慧,邢培振. 云计算环境下信息安全分析[J]. 计算机技术与发展, 2011, 21(12):164-171.
- [3] 梅海涛. 基于云计算的物联网运营平台浅析[J]. 电信技术, 2011(5):66-68.
- [4] 丁超. IoT/CPS的安全体系结构及关键技术[J]. 中兴通讯技术, 2011, 17(1):11-16.
- [5] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报, 2011, 22(1):71-83.
- [6] 周水庚,李丰,陶宇飞,等. 面向数据库应用的隐私保护研究综述[J]. 计算机学报, 2009, 32(5):847-861.
- [7] 刘良,蒋天发. 同态加密技术及其在物联网中的应用研究[J]. 网络信息安全, 2011(5):61-64.