|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| 武汉大学logo | | | | |
|  | | | | |
| 分布并行计算机技术课程报告 | | | | |
|  | 研究生姓名 | ： | 陈小龙 |  |
| 学号 | ： | 2019282110194 |
| 指导教师姓名、职称 | ： | 黄传河教授 |
| 专业名称 | ： | 计算机科学与技术 |
| **(备注：选课失败，需要黄老师您手动添加姓名学号到成绩系统)** | | |
|  | | | | |
| 二〇一九年十二月 | | | | |

# 

# 摘要

本文主要对边缘计算概念、典型应用场景、研究现状及安全需求等方面进行统性的介绍，说明边缘计算的发展还处在初级阶段，在实际的应用中还存在很多问题需要解决研究，包括优化边缘计算性能、安全性、互操作性以及安全性。

关键词：边缘计算；安全性；万物互联

目录

[摘要 I](#_Toc28606293)

[引言 1](#_Toc28606294)

[1边缘计算体概述 2](#_Toc28606295)

[1.1边缘计算背景 2](#_Toc28606296)

[1.2边缘计算体系架构 2](#_Toc28606297)

[1.2边缘计算范例 2](#_Toc28606298)

[1.2边缘计算的优势 3](#_Toc28606299)

[2边缘计算的典型应用 3](#_Toc28606300)

[3边缘计算安全需求 5](#_Toc28606301)

[3.1边缘计算安全的必要性 5](#_Toc28606302)

[3.2物理安全需求 5](#_Toc28606303)

[3.2网络安全需求 6](#_Toc28606304)

[3.3数据安全需求 6](#_Toc28606305)

[3.4应用安全需求 7](#_Toc28606306)

[4边缘计算安全挑战 7](#_Toc28606307)

[4.1身份认证 7](#_Toc28606308)

[4.2访问控制 8](#_Toc28606309)

[4.3入侵检测 8](#_Toc28606310)

[4.3隐私保护 9](#_Toc28606311)

[5结束语 9](#_Toc28606312)

[参考文献 10](#_Toc28606313)

[致谢 11](#_Toc28606314)

# 引言

随着单片机嵌入式系统和无线通信技术的发展，物联网技术近年来得到了长足的发展和普及，其实际应用包括智能家居、智慧交通、无人驾驶等。近年来，除了“物”与“物”的互联，还增加了“物”与“人”的互联，其显著特点是“物”端具有更强的计算能力和语境感知能力，将人和信息融入到互联网中，该趋势使得人类社会正在迈入万物互联（IoE）的时代。万物互联的核心在于收集来自于终端设备的海量数据，利用以大数据、机器学习、深度学习为代表的智能技术，去满足不同行业的业务需求，如制造、交通、医疗、农业等各行各业。在此背景下，所需要连接的终端设备数量达到数十亿甚至数万亿，其产生的数据呈爆炸式增长。

目前，海量数据的存储和处理主要依赖于集中式的云计算模型，其特征主要表现为数据和存储均位于部署在偏远地区的云计算中心。尽管云数据中心以堆叠硬件的方式具有较强的计算和存储能力，但是万物互联背景下，网络边缘的终端设备产生的数据已经达到海量级，这给云计算模型带来诸多挑战。

边缘计算模型成为新兴万物互联应用的支撑平台，目前已是大势所趋。本文中，我们从概念、关键技术、典型应用、现状趋势和挑战等几个方面对边缘计算展开详细介绍。

# 1边缘计算体概述

## 1.1边缘计算背景

对于边缘计算，不同的组织给出了不同的定义。美国韦恩州立大学计算机科学系的施巍松等人把边缘计算定义为：“边缘计算是指在网络边缘执行计算的一种新型计算模式，边缘计算中边缘的下行数据表示云服务，上行数据表示万物互联服务”。边缘计算产业联盟把边缘计算定义为：“边缘计算是在靠近物或数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力的开发平台，就近提供边缘智能服务，满足行业数字在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求”。

因此，边缘计算是一种新型计算模式，通过在靠近物或数据源头的网络边缘侧，为应用提供融合计算、存储和网络等资源。同时，边缘计算也是一种使能技术，通过在网络边缘侧提供这些资源，满足行业在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。

## 1.2边缘计算体系架构

边缘计算通过在终端设备和云之间引入边缘设备，将云服务扩展到网络边缘。边缘计算架构包括终端层、边缘层和云层[1

终端层。终端层是最接近终端用户的层，它由各种物联网设备组成，例如传感器、智能手机、智能车辆、智能卡、读卡器等。为了延长终端设备提供服务的时间，则应该避免在终端设备上运行复杂的计算任务。因此，我们只将终端设备负责收集原始数据，并上传至上层进行计算和存储。终端层连接上一层主要通过蜂窝网络。

边缘层。边缘层位于网络的边缘，由大量的边缘节点组成，通常包括路由器、网关、交换机、接入点、基站、特定边缘服务器等。这些边缘节点广泛分布在终端设备和云层之间，例如咖啡馆、购物中心、公交总站、街道、公园等。它们能够对终端设备上传的数据进行计算和存储。由于这些边缘节点距离用户距离较近，则可以为运行对延迟比较敏感的应用，从而满足用户的实时性要求。边缘节点也可以对收集的数据进行预处理，再把预处理的数据上传至云端，从而减少核心网络的传输流量。边缘层连接上层主要通过因特网。

云层。云层由多个高性能服务器和存储设备组成，它具有强大的计算和存储功能，可以执行复杂的计算任务。云模块通过控制策略可以有效地管理和调度边缘节点和云计算中心，为用户提供更好的服务。

## 1.2边缘计算范例

与边缘计算类似的范例，如雾计算、移动边缘计算等，虽然与边缘计算不尽相同，但它们在动机、节点设备、节点位置等上与边缘计算范例类似。协同边缘计算是一种新的计算范例，它使用边缘设备和路由器的网状网络来实现网络内的分布式决策。决策是在网络内部通过在边缘设备之间共享数据和计算而不是将所有数据发送到集中式服务器来完成的。这与通常执行集中计算的现有计算范例不同，并且诸如网关的边缘设备仅用于收集数据并将数据发送到服务器以进行处理。

## 1.2边缘计算的优势

边缘计算模型将原有云计算中心的部分或全部计算任务迁移到数据源附近，相比于传统的云计算模型，边缘计算模型具有实时数据处理和分析、安全性高、隐私保护、可扩展性强、位置感知以及低流量的优势。

实时数据处理和分析。将原有云计算中心的计算任务部分或全部迁移到网络边缘，在边缘设备处理数据，而不是在外部数据中心或云端进行；因此提高了数据传输性能，保证了处理的实时性，同时也降低了云计算中心的计算负载。

安全性高。传统的云计算模型是集中式的，这使得它容易受到分布式拒绝服务供给和断电的影响。边缘计算模型在边缘设备和云计算中心之间分配处理、存储和应用，使得其安全性提高。边缘计算模型同时也降低了发生单点故障的可能性。

保护隐私数据，提升数据安全性。边缘计算模型是在本地设备上处理更多数据而不是将其上传至云计算中心，因此边缘计算还可以减少实际存在风险的数据量。即使设备受到攻击，它也只会包含本地收集的数据，而不是受损的云计算中心。

可扩展性。边缘计算提供了更便宜的可扩展性路径，允许公司通过物联网设备和边缘数据中心的组合来扩展其计算能力。使用具有处理能力的物联网设备还可以降低扩展成本，因此添加的新设备都不会对网络产生大量带宽需求。

位置感知。边缘分布式设备利用低级信令进行信息共享。边缘计算模型从本地接入网络内的边缘设备接收信息以发现设备的位置。例如导航，终端设备可以根据自己的实时位置把相关位置信息和数据交给边缘节点来进行处理，边缘节点基于现有的数据进行判断和决策。

低流量。本地设备收集的数据可以进行本地计算分析，或者在本地设备上进行数据的预处理，不必把本地设备收集的所有数据上传至云计算中心，从而可以减少进入核心网的流量。

# 2边缘计算的典型应用

边缘计算在很多应用场景下都取得了很好的效果。比如，车辆互联、智能建筑控制、医疗保健、海洋监测以及无线传感器和执行器网络与边缘计算结合的场景[2]。

医疗保健。边缘计算可以辅助医疗保健，例如可以针对患有中风的患者辅助医疗保健。研究人员最近提出了一种名为U-fall的智能医疗基础设施，它通过采用边缘计算技术来利用智能手机。在边缘计算的辅助下，U-fall借助智能设备传感器实时感应运动检测。边缘计算还可以帮助健康顾问协助他们的病人，而不受其地理位置的影响。边缘计算使智能手机能够从智能传感器收集患者的生理信息，并将其发送到云服务器以进行存储、数据同步以及共享。

视频分析。在万物联网时代，用于监测控制的摄像机无处不在，传统的终端设备——云服务器架构可能无法传输来自数百万台终端设备的视频。在这种情况下，边缘计算可以辅助基于视频分析的应用。在边缘计算辅助下，大量的视频不用再全部上传至云服务器，而是在靠近终端设备的边缘服务器中进行数据分析，只把边缘服务器不能处理的小部分数据上传至云计算中心即可。

车辆互联。通过互联网接入为车辆提供便利，使其能够与道路上的其他车辆连接。如果把车辆收集的数据全部上传至云端处理会造成互联网负载过大，导致传输延迟，因此，需要边缘设备其本身具有处理视频、音频、信号等数据的能力。边缘计算可以为这一需要提供相应的架构、服务、支持能力，缩短端到端延迟，使数据更快地被处理，避免信号处理不及时而造成车祸等事故。一辆车可以与其他接近的车辆通信，并告知他们任何预期的风险或交通拥堵。

移动大数据分析。无处不在的移动终端设备可以收集大量的数据，大数据对业务至关重要，因为它可以提取可能有益于不同业务部门的分析和有用信息。大数据分析是从原始数据中提取有意义的信息的过程。在移动设备附近实施部署边缘服务器可以通过网络高带宽和低延迟提升大数据分析。例如，首先在附近的边缘服务器中收集和分析大数据，然后可以将大数据分析的结果传递到核心网络以进一步处理，从而减轻核心网络的压力。

智能建筑控制。智能建筑控制系统由部署在建筑物不同部分的无线传感器组成。传感器负责监测和控制建筑环境，例如温度、气体水平或湿度。在智能建筑环境中，部署边缘计算环境的建筑可以通过传感器共享信息并对任何异常情况做出反应。这些传感器可以根据其他无线节点接收的集体信息来维持建筑气氛。

海洋监测控制。科学家正在研究如何应对任何海洋灾难性事件，并提前了解气候变化。这可以帮助人们快速采取应对措施，从而减轻灾难性事件造成的严重后果。部署在海洋中某些位置的传感器大量传输数据，这需要大量的计算资源和存储资源。而利用传统的云计算中心来处理接收到的大量数据可能会导致预测传输的延迟。在这种情况下，边缘计算可以发挥重要作用，通过在靠近数据源的地方就近处理，从而防止数据丢失或传感器数据传输延迟。

智能家居。随着物联网技术的发展，智能家居系统得到进一步发展，其利用大量的物联网设备实时监测控制家庭内部状态，接收外部控制命令并最终完成对家居环境的调控，以提升家居安全性、便利性、舒适性。由于家庭数据的隐私性，用户并不总是愿意将数据上传至云端进行处理，尤其是一些家庭内部视频数据。而边缘计算可以将家庭数据处理推送至家庭内部网关，减少家庭数据的外流，降低数据外泄的可能性，提升系统的隐私性。

智慧城市。预测显示：一个百万人口的城市每天将可能会产生200PB的数据。因此，应用边缘计算模型，将数据在网络边缘处理是一个很好的解决方案。例如，在城市路面检测中，在道路两侧路灯上安装传感器收集城市路面信息，检测空气质量、光照强度、噪声水平等环境数据，当路灯发生故障时能够即时反馈给维护人员，同时辅助健康急救和公共安全领域。

# 3边缘计算安全需求

安全是指达到抵抗某种安全威胁或安全攻击的能力，横跨云计算和边缘计算，需要实施端到端的防护。万物互联系统在紧密耦合网络系统与物理世界中的关键性作用决定了安全属性和隐私保护的相关需求要比在以往任何信息系统中更加重要[3]。

## 3.1边缘计算安全的必要性

万物互联系统中终端设备具有超大规模、低成本设计、资源受限、设备异构等特性。同时，开发商重视功能优于安全的事实、用户更高的隐私要求、更难的信任管理使得保证万物互联系统的安全性显得更具挑战性。

2017年6月1日正式生效的《中华人民共和国网络安全法》特别强调了关键信息基础设施的运行安全，而能源、交通、制造等关键基础设施的工业控制环境无疑将是安全建设的重中之重。2016年中国信息通信研究院云计算白皮书指出：公有云服务提供商向用户提供大量一致化的基础软件（如操作系统、数据库等资源），这些基础软件的漏洞将造成大范围的安全问题与服务隐患。安全已经成为阻碍万物互联和云计算发展的最大因素。

边缘计算是万物互联的延伸和云计算的扩展，三者的有机结合将为万物互联时代的信息处理提供较为完美的软硬件支撑平台，为能源、交通、制造、医疗等行业带来飞跃式发展。而通过边缘设备将类似云计算的功能带到了网络的边缘，可能引入新的安全挑战，一些传统的安全解决方法，例如基于非对称密钥协议和基于网际协议地址（IP）的解决方案，无法有效地应用于边缘计算系统，进而带来了一系列全新的安全需求。

综上所述，网络边缘高度动态异构的复杂环境也会使网络难于保护，从而带来新的安全挑战。边缘计算同时又为资源、能量受限的终端设备提供一套全新的安全解决方案。因此，研究边缘计算场景的安全和隐私保护的相关问题是万物互联系统得到进一步发展的首要前提条件。

## 3.2物理安全需求

物理安全是保护智能终端设备、设施以及其他媒体避免自然界中不可抗力（如地震、火灾、龙卷风、泥石流）及人为操作失误或错误所造成的设备损毁、链路故障等使边缘计算服务部分或完全中断的情况。物理安全是整个服务系统的前提，物理安全措施是万物互联系统中必要且基础的工作。

对于边缘计算设备来说，其在对外开放的、不可控的甚至人迹罕至的地方运行，所处的环境复杂多样，因此更容易受到自然灾害的威胁。且在运行过程中，由间接或者自身原因导致的安全问题（如能源供应；冷却除尘、设备损耗等），运行威胁虽然没有自然灾害造成的破坏彻底，但是如果缺乏良好的应对手段，仍然会导致灾难性的后果，使得边缘计算的性能下降，服务中断和数据丢失。

## 3.2网络安全需求

网络安全是指通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性，以使系统连续可靠正常地运行，网络服务不中断。

大数据处理背景下，海量终端设备通过网络层实现与边缘设备的数据交互传输，边缘设备可以通过接入网络层实现更加广泛的互联功能。而大量设备的接入，给网络管理带来沉重负担的同时，也增加了边缘设备被攻击的可能性。文献[4-5] 中所采用的攻击方式大都是在无线传输途中采用窃听、截获数据包等方法进行流量分析，然后篡改或伪造数据包来达到控制目标的目的。

相较于云计算数据中心，边缘节点的能力有限，更容易被黑客攻击。虽然单个被破坏的边缘节点损害并不大，并且网络有迅速找到附近可替代节点的调度能力；但如果黑客将攻陷的边缘节点作为“肉鸡”去攻击其他服务器，进而会对整个网络造成影响。现有大多安全保护技术计算保护流程复杂，不太适合边缘计算的场景。所以，设计适合于万物互联背景下边缘计算场景中轻量级的安全保护技术是网络安全的重大需求。

## 3.3数据安全需求

数据信息作为一种资源，具有普遍性、共享性、增值性、可处理性和多效用性，而数据安全的基本目标就是要确保数据的3个安全属性：机密性、完整性和可用性。

要对数据的全生命周期进行管理的同时实现这3个安全属性才能保证数据安全。整个生命周期包括6个阶段：创建，数据的产生和采集过程；存储，数据保存到存储介质的过程；使用，数据被浏览、处理、搜索或进行其他操作的过程；共享，数据在拥有者、合作者、使用者之间交互的过程；存档，极少使用的数据转入长期存储的过程；销毁，不再使用的数据被彻底删除和擦除的过程。

在边缘计算中，用户将数据外包给边缘节点，同时也将数据的控制权移交给边缘节点，这便引入了与云计算相同的安全威胁。首先，很难确保数据的机密性和完整性，因为外包数据可能会丢失或被错误地修改。其次，未经授权的各方可能会滥用上传的数据图谋其他利益。虽然相对于云来说边缘计算已经规避了多跳路由的长距离传输，很大程度地降低了外包风险；但是边缘计算设备部署的应用属于不同的应用服务商，接入网络属于不同的运营商，导致边缘计算中多安全域共存、多种格式数据并存。因此属于边缘计算的数据安全问题也日益突出，如在一个边缘节点为多个用户服务时，如何确保用户数据的安全隔离？在如此复杂多变的环境中，一个边缘节点瘫痪后，如何实现安全快速地迁移数据？当多个边缘节点协同服务时，如何能够在不泄露各自数据的情况下设计多方的协作服务？

另一个万物互联背景下边缘计算的数据安全需求就是用户隐私保护。比起云中心隐私数据泄露的风险，边缘计算设备位于靠近数据源的网络边缘侧，相对于位于核心网络中的云计算数据中心，可以收集更多用户高价值的的敏感信息，包括位置信息、生活习惯、社交关系甚至健康状况等，边缘计算是否会成为商业公司收集用户隐私数据的平台？物联网设备的计算资源难以执行复杂的隐私保护算法，边缘式大数据分析中如何在数据共享时保证用户的隐私？这些问题都将成为边缘计算发展的重要阻碍。

## 3.4应用安全需求

应用安全，顾名思义就是保障应用程序使用过程和结果的安全。边缘式大数据处理时代，通过将越来越多的应用服务从云计算中心迁移到网络边缘节点，能保证应用得到较短的响应时间和较高的可靠性，同时大大节省网络传输带宽和智能终端电能的消耗。但边缘计算不仅存在信息系统普遍存在的共性应用安全问题，如拒绝服务攻击、越权访问、软件漏洞、权限滥用、身份假冒等，还由于其自身特性存在其他的应用安全的需求。在边缘这种多安全域和接入网络共存的场景下，为保证应用安全，该如何对用户身份进行管理和实现资源的授权访问则变得非常重要。身份认证、访问控制和入侵检测相关技术便是在边缘计算环境下保证应用安全的重点需求。

# 4边缘计算安全挑战

通过对边缘计算安全需求的讨论分析可以看出：边缘计算的特性使其在构建安全保护方案时给系统开发人员带来了重大挑战。

## 4.1身份认证

身份认证，也称“身份验证”或“身份鉴别”，是验证或确定用户提供的访问凭证是否有效的过程。用户可以是个人、应用或服务，所有的用户都应在被认证后才能访问资源，从而确定该用户是否具有对某种资源的访问和使用权限，使系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

在边缘计算中，不同可信域中的边缘服务器、云服务提供商和用户分别提供和访问实时服务，其分散化、实时服务的低延迟需求和用户的移动性给身份认证的实现带来了巨大的障碍，很难保证所有涉及的实体都是可信的。在访问这些服务之前，应该对每个用户进行身份验证，以确保其真实性和可信性。身份认证应具备的功能包括：一方面应能够在分布式异构网络环境下，使用相关的协议、规范以及技术将分散的身份信息进行集中管理，实现单点登录，也可以方便地扩充跨身份标识域的访问等功能；另一方面应提供友好的体验环境，保护用户隐私，有效地对用户的行为进行审计。

身份认证是终端设备安全的基本要求，许多万物互联设备没有足够的内存和中央处理器（CPU）功率来执行认证协议所需的加密操作。这些资源有限的设备可以将复杂的计算和存储外包给可以执行认证协议的边缘设备，与此同时也会带来一定的问题：终端用户和边缘计算服务器之间必须相互认证，这种多安全域共存的情况下安全凭证从何而来？如何在大量分布式边缘服务器和云计算中心之间实现统一的身份认证和密钥管理机制？万物互联中存在大量的资源受限设备，无法利用传统的PKI体制对边缘计算设备或服务进行认证。边缘计算环境下终端具有很强的移动性，如何实现用户在不同边缘设备切换时的高效认证具有很大挑战。显然，轻量级的身份认证技术是保证边缘计算安全的前提和挑战。

## 4.2访问控制

区问控制是基于预定模式和策略对资源的访问过程进行实时控制的技术，按用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用。访问控制的任务是在满足用户最大限度享受资源共享需求的基础上，实现对用户访问权限的管理，防止信息被非授权篡改和滥用，是保证系统安全、保护用户隐私的可靠工具。在万物互的联背景下，需要访问控制以确保只有受信任方才能执行给定的操作，不同用户或终端设备具有访问每个服务的独特权限。

访问控制除了负责对资源访问控制外，还要对访问策略的执行过程进行追踪审计。在边缘计算中，访问控制变得更加艰难，主要原因在于：首先要求边缘计算服务提供商能够在多用户接入环境下提供访问控制功能；其次，访问控制应支持用户基本信息和策略信息的远程提供，还应支持访问控制信息的定期更新；最后，对于高分布式且动态异构数据的访问控制本身就是一个重要的挑战。

## 4.3入侵检测

入侵检测通过包括监测、分析、响应和协同等一系列功能，能够发现系统内未授权的网络行为或异常现象，收集违反安全策略的行为并进行统计汇总，从而支持安全审计、进攻识别、分析和统一安全管理决策。从企业角度看，任何试图破坏信息及信息系统完整性、机密性的网络活动都被视为入侵行为。入侵检测技术广泛应用于云系统中，以减轻内部攻击、泛洪攻击、端口扫描、虚拟机攻击和hypervisor攻击等入侵行为。

边缘计算中，外部和内部攻击者可以随时攻击任何实体。若没有实施适当的入侵检测机制来发现终端设备和边缘节点的恶意行为或协议违规，则会逐步破坏服务设施，进而影响整个网络。

但是，在万物互联环境下，由于设备结构、协议、服务提供商的不同，难以检测内部和外部攻击。此外，如何通过资源能力受限的边缘设备间的系统来进行全局的入侵检测，使其能够在大规模、广泛地理分布和高度移动的环境中得到应用，具有十分重要的意义。

## 4.3隐私保护

万物互联系统的目标是通过收集海量数据为用户提供多种个性化服务。由于终端设备资源受限，缺乏对数据加密或解密的能力，这使得它容易受到攻击者的攻击。

边缘计算将计算迁移到临近用户的一端，直接对数据进行本地处理、决策，在一定程度上避免了数据在网络中长距离的传播，降低了隐私泄露的风险。然而，由于边缘设备获取的用户第一手数据，能够获得大量的敏感隐私数据。如何能够保证用户在使用服务的同时又不泄露其敏感信息对边缘计算中的隐私保护算法提出了更高的要求。

# 5结束语

随着万物互联时代的到来，基于云计算模型的集中式大数据处理模式已经无法满足网络边缘设备所产生海量数据处理的实时性、安全性和低能耗等需求。为此，将原有云计算中心的部分或者全部计算任务迁移到数据源的附近执行，边缘计算在梯联网、工业机器人、无人驾驶、智慧交通等领域扮演着越来越重要的角色。作为一种新型的去中心化架构，它将云计算的存储、计算和网络资源扩展到网络边缘，以支持大规模的协同万物互联应用。本文主要从基本概念、应用场景、存在的挑战、安全需求等方面对边缘计算进行了系统性介绍。随着物联网和计算机技术的发展，在可以预见的将来边缘计算必将迎来快速的发展。

# 参考文献

[1] 施巍松，张星洲，王一帆，等.边缘计算：现状与展望[J].计算机研究与发展，2019，56(1):69-89.

[2] 边缘计算产业联盟,工业互联网产业联盟.边缘计算与云计算系统白皮书[R].2018

[3] 卿昱.云计算安全技术[M].北京:国防工业出版社,2016:53-54

[4] Kazman R, Bass L, Abowd G, Webb M. SAAM: A Method for Analyzing the Properties of Software Architecture. Los Alamitos: IEEE Computer Society Press, 1994. 81 −90.

[5] 云计算白皮书[EB/OL].[2018-12-20].http://www.199it.com/archives/764250.html

# 

# 致谢

本课程报告是基于黄授所授的“分布并行计算机技术”为基础完成。黄老师丰富的人生阅历，渊博的专业知识，严谨的治学态度，热情洋溢讲课方式，让我获益匪浅。不仅使我对分布并行计算机技术有更深的理解，而且扩展了我的知识视野，更重要的是让我对做人和求学有了不一样的理解，非常感谢黄老师。