北京大学

博士研究生综合考试报告

题目：云计算环境下的人工智能相关技术研究

姓　　名：李炎

学　　号：2001111305

院　　系：信息科学技术学院

专　　业：计算机软件与理论

研究方向：云计算与普适计算

导　　师：梅宏

二〇二一年四月

摘要

21 世纪 10 年代以来, 云计算和人工智能可谓计算机科学领域最为炙手可热的两个研究方向。以虚拟化、资源管理和服务化为代表的云计算核心技术在近十余年里取得了丰硕的研究成果。当前，云计算已成为工业化社会重要的信息基础设施，支撑并推动着大数据和人工智能产业的快速发展。与此同时，人工智能技术在近十年内也相继在计算机视觉、自然语言处理等多个领域取得了突破，“智能化”已然成为现代社会的重要标签之一。

本文将以上述两大技术的蓬勃发展为背景，研究云计算与人工智能相互影响、相互支持、相辅相成的相关技术。本文将按照如下几章展开。

第一章对相关的技术背景做出介绍。首先对云计算近十年的发展做简要回顾，并介绍具有代表性的若干核心技术。其次对人工智能近十年的发展做简要概述，阐述其在计算机视觉、自然语言处理等子领域的代表性科研成果。最后分析二者在交叉领域现有的相关研究。

第二章开始探究二者的关系，研究云计算环境中用以支持人工智能的系统软件技术。随着人工智能算法和系统研究的发展，其训练-测试-部署的流程愈发复杂。很多云厂商基于本地化的云原生技术，构建了一站式的人工智能开发-部署软件栈供用户使用。同时，伴随着新的云计算模式（如无服务计算 serverless）的产生，工业界和学术界也在探究将其应用在人工智能领域，使相关的应用在云上具有更高的弹性。

第三章讨论近些年来云环境下出现的新硬件（如 GPU，AI 专用芯片，Intel-SGX 等）为人工智能技术带来的新的机遇与挑战。硬件的发展（如 GPU，AI 专用芯片等）导致的算力的提升，也是人工智能近年发展迅速的重要原因之一。同时，某些硬件层面安全机制（如 Intel-SGX）的产生，使增强人工智能应用的安全性有的新的潜在解决方案。

第四章从另一角度，即“服务于云计算系统架构的 AI 技术”这一视角展开，研究人工智能对云计算的增强技术。云计算本质上是一个巨大的公共资源池，用户如何在资源池中选取资源，云厂商如何为不同的用户调度资源，是云计算领域两个重要的话题。近五年来，该领域的研究者开始尝试利用一系列基于机器学习的算法来辅助解决上述两个问题。

第五章总结了上述三个方向的重要文献和相关研究团队概况。

第六章介绍了作者下一步的研究计划。

关键词：云计算，人工智能，机器学习，新硬件

目录

第一章　引言

1.1　云计算的基本概念

云计算（Cloud Computing），根据美国国家标准技术研究所（NIST）的定义，指的是一种可以实现对可配置计算资源共享池（如网络、服务器、存储、应用和服务）进行随时随地、便捷、按需网络访问模型。这些资源可以迅速地配分配和释放，并且这个过程只需要足最低限度的资源管理工作以及与服务提供商最少的交互。美国亚马逊公司再 2006 年 3 月推出了 Amanzon Web Service（AWS），这一事件一般被认为代表着云计算时代的正式开启。经过十几年的发展，凭借着“方便易用、弹性伸缩、按需服务”的技术特征，云计算概念已被广泛接受，云计算产业取得了商业上的巨大成功，云计算平台已成为当今社会的关键信息基础设施，云计算技术为大数据、人工智能的领域的蓬勃发展特工了重要的支撑作用。

1.1.1　云计算的传统服务模型

NIST 将云计算分为了三种服务模型。

这三种服务模型分别是基础设施即服务（Infrastructure as a Service，IaaS）、平台即服务（Platform as a Service，PaaS）以及软件即服务（Software as a Service，SaaS）。IaaS 为消费者提供用来运行应用的计算资源，包括服务器、存储、网络等。其中虚拟机是云厂商提供的最核心的 IaaS 产品。与 IaaS 只提供最基础的底层资源不同，PaaS 强调为消费者提供云开发环境，除计算资源意外，PaaS 为用户提供中间件开发，运行平台及工具，帮助用户更方便地开、管理、测试和运行应用。SaaS 是厂商提供的基于云的软件，用户无需下载安装软件，通过浏览器即可访问服务。

图1.1给出了云计算三种服务模型的代表产品。亚马逊公司的 AWS EC2，谷歌公司的 Google Compute Engine 以及阿里云公司的 ECS 都是典型的 IaaS 产品。其主要服务形态是云厂商向消费者售卖虚拟机或者裸金属服务器以及连带的网络、存储等附属产品。PaaS 的代表性产品包括 AWS Beanstalk、Google App Engine、Microsoft Azure App Servics 等。此类韩品为用户提供再云中快速部署和管理应用的能力，提供包括应用扩容，负载均衡，应用监控和安全管理等功能。相比于 IaaS 仅售卖以虚拟机为主的基础设施，PaaS 降低了用户开发、管理、运维应用的成本，使得用户可以更加专注于构建应用本身。在云计算已经发展了十几年的当今时代，越来越多的 SaaS 产品涌现了出来。谷歌公司开发的 Google Docs、Google Maps 以及微软公司开发的 Microsoft Office 365

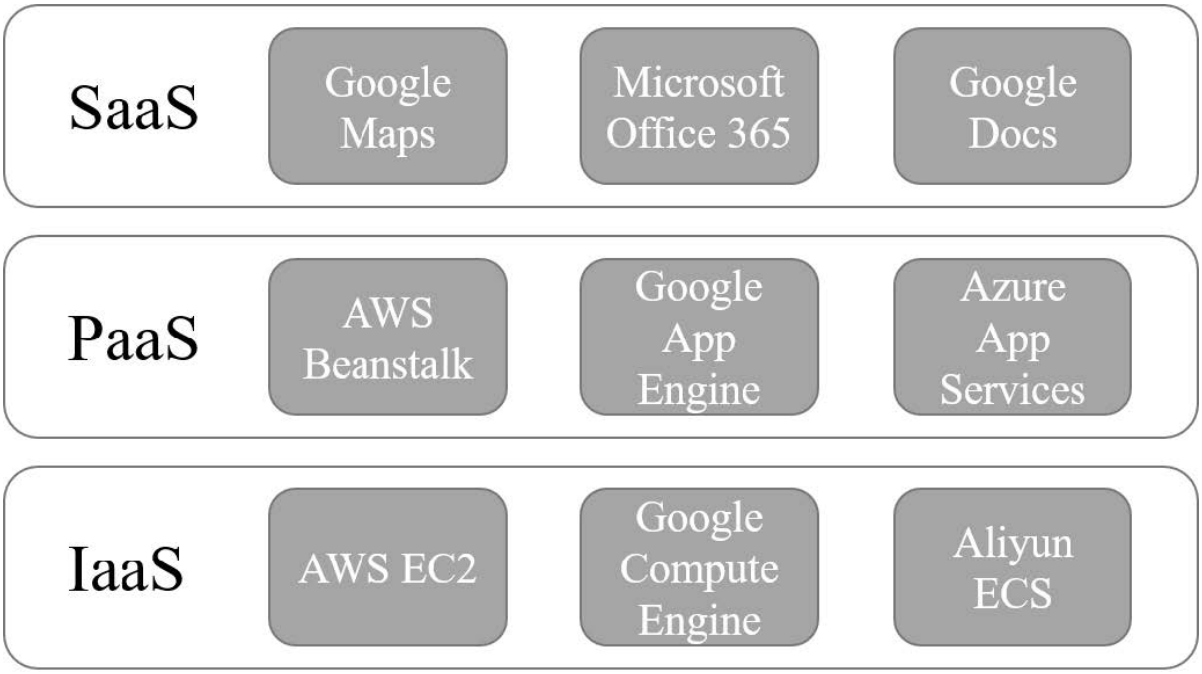

图 1.1　云计算服务模型代表产品

都是典型的 SaaS 产品。以 Google Docs 为例，与传统的文件处理办公软降相比，用户无需在本地花费大量存储空间来安装软件，只需要打开浏览器，输入 URL，即可使用 Google Docs 服务处理文件，并且所有的文件都会被及时同步保存到云端。另一个代表性的 SaaS 产品是 Google Maps。Google Maps 与 Google Docs 类似，为个人用户提供在浏览器中直接使用的地图服务。与传统软件相比，SaaS 在使用方式上具有方便灵活，跨平台的特性，同时用户存储在云端的数据经过云厂商的冗余备份也具有更高的可靠性。

1.1.2　云计算的新兴服务模型

云计算发展至今日，其服务模型已经不严格局限于 NIST 最初总结的这三种基本形态，世界各地各领域的研究者们已经提出了众多不同的 X as a Service，包括 Blockchain as a Service，Sensing as a Service，Workspace as a Service 等。与传统的三种服务形态相比，这些服务不单纯是硬件服务或者软件服务，其结合二者的特点，面向特定的领域方向进行更深度的定制，如区块链、物联网、分布式共识等。服务形态的日益丰富，服务内容的日益复杂体现了云计算更见领域化，精细化的发展趋势。而近几年来最热门的概念莫过于 FaaS，即 Fucntion as a Service。

FaaS 是一种新兴的计算模式，亦被称为 Serverless Computing。从字面理解，Serverless Computing 即为“无服务器计算”之意。然后，其并非意味着真的没有服务器，而已说开发者不用过多考虑服务器的相关问题。在传统的 IaaS 服务中，开发者需要自己

图 1.2　AWS Lambda 中示例程序：照片大小调整

惊醒服务器管理与运维，负责服务的发布，在流量变化时对服务器集群进行扩容或缩容。而在 FaaS 中，开发者只需要关注业务逻辑，至于服务的发布、管理、弹性伸缩等，则交由云厂商来完成。

FaaS 背后的机制一般是以容器技术为基础的。典型地，开发者上传自己的业务代码后，云厂商并不会直接收费。当对该服务的请求到来之时，云厂商将启动一系列容器来运行该服务，从而对用户的请求进行响应。通常而言，开发者指定的服务会与某些时间绑定（hook），在发生该事件时，立即触发开发者定义的服务。我们以 AWS 的 serverless computing 服务 Lambda 中的一个示例程序为例，讲述整个流程。图1.2所示的是一个为照片调整大小的服务。该服务与 AWS S3（AWS 的对象存储服务）的上传事件绑定，当云厂商检测到有用户向 S3 上传图片时，会立即触发开发者定义的图片大小调整函数。整个流程中，开发者需要关注的只有第四步的函数开发工作，至于该函数的横向拓展，全部由云厂商来负责。

主流的云厂商均提供了 FaaS 服务，例如 AWS 的 Lambda，阿里云的函数计算等，近年来越来越受到开发者的青睐。一方面是因为它的高弹性，易于开发。另一方面则是因为其细粒度的收费模式。通常而言，FaaS 的服务是按照请求次数进行收费。当函数闲置时，并不产生额外的费用。

1.2　人工智能技术近年的发展

TODO: 简介近些年人工智能技术的发展

1.3　云计算和人工智能交叉领域的常见研究问题

云计算和人工智能是两个息息相关的热门领域。一方面，以深度学习为典型代表的人工智能技术在当今社会被应用的越来月广泛，研发、调试、发布新的模型的需求日益增长。与这种发展趋势对应，多数主流的云厂商都提供了机器学习模型训练-测试-部

署的 pipeline。学术界也不断探索“云上机器学习”这一话题，利用新的计算模式（如 FaaS）在云上以更便捷、更经济高效地开展 ML 模型的训练和部署。同时得益于近年硬件技术的发展，多种新硬件（多体现为人工智能的加速芯片）在云环境中得到应用，进一步方便机器学习用户将整个开发流程迁移到云端。另一方面，机器学习技术也越来越多被用于解决云计算中常见的问题。例如使用推荐算法解决置优化问题和利用强化学习解云环境中的资源调度问题。下文对这几个常见问题做简单概述，具体研究将在后续几章展开。

1.3.1 基于公有云服务的机器学习平台

1. 产业界

主流的云厂商都提供了面向机器学习的平台系统，例如 AWS 和 Sagamaker[7, 10, 13]，Azure 的 Azure ML Studio[5] 等。这些基于云的平台提供了一站式调试、训练和部署 ML 模型的能力。一般而言此类平台被视为 SaaS 类的服务，因为其是基于云资源构建的上层软件栈，使得用户能够直接使用 web 的方式使用。例如 Sagemaker 就支持用户直接在浏览器中用 jupyter notebook 编写和调试模型代码。

2. 学术界

一般而言，产业界的平台系统面向的是一般性用户的普遍需求。因此，对于有特殊需求的用户，通常会有与产业界的解决方案并行的工作。例如，为了以尽可能低的成本在云上完成模型的训练，相关工作 [6, 9] 尝试利用云上的动态资源（价格低但是稳定性/可用性低）进行模型的训练，并辅以一定的策略增强其可靠性。再比如，机器学习模型的在线服务会有低延迟、高吞吐率的要求。为了实现上述需求，相关工作 [17] 利用云上的多种资源（如 IaaS，FaaS 等），根据负载的动态变化，敏捷地在不同资源之间切换，充分利用不同类型资源的优点，规避掉其缺点，实现高效、经济的模型在线服务。一般而言，学术界的此类研究构建于云厂商服务的上层，是一种 Cloud-of-Clouds 的模式。

1.3.2 利用新的计算模式在云上运行机器学习 pipeline

以 FaaS 为代表的新型云计算模式，以其高弹性、灵活的计费方式等特点吸引了众多研究者的注意。一般而言，用来训练机器学习模型的集群大小是固定的，很难动态地进行伸缩。同时，开发者还需要自行对该集群进行维护和管理，从而徒增一些不必要地时间和人力开销。因此，学术界开始探讨如何使得机器学习工作流享用到 FaaS 的诸多优点 [15]，从而使得其计算资源在模型训练时能按需伸缩，结束训练后自动将模型存储在持久化存储中，计算资源随即释放。

除了模型训练，也有部分研究者尝试利用 FaaS，以 serverless 的模式部署模型。虽然这一想法非常自然，但是还有诸多问题需要解决。例如，现有的 serverless 服务，如 AWS Lambda，其单个 instance 所能使用的内存有限，也无法使用 GPU 等加速芯片，同时其冷启动时间也较长（相比于服务对 latency 的要求）。如何优化 FaaS 的系统架构，使其更适合模型的部署，也是一个值得研究的问题。

1.3.3　新硬件对人工智能的影响

TODO：介绍新硬件对人工智能的影响

1.3.4　利用机器学习算法解决配置优化问题

公有云厂商所提供的计算资源类型和计费模式越来越复杂。据不完全统计，截至目前，AWS EC2 提供了超过 400 种配置的虚拟机，阿里云提供了超过 500 种虚拟机。除了虚拟机配置不同之外，其收费模型也存在多种。例如，除了传统的包年包月、按量付费等，还有抢占式实例（在 AWS 中成为 Spot Instance）等计费方式。在此场景中，用户所面临的一个重要问题在于如何为自己的应用程序/负载选择合适配置和收费方式的资源。

部分研究者利用机器学习算法来解决此类问题。有的将其看作一个推荐问题 [8]，用协同过滤等推荐系统中常用的算法为不同的应用程序匹配合适的配置。有的将其建模为回归问题 [12, 14, 16, 18]，将应用程序的信息、资源的配置信息等作为输入，预测在某种配置下某个应用程序的性能或者花费，从而得到最佳的配置。还有的将其视作在线优化问题 [1, 2]，利用贝叶斯优化等方法，通过有限次的尝试逐渐逼近最优解。

1.3.5　利用机器学习算法解决资源调度问题

资源调度是操作系统、分布式系统和云计算领域中的经典问题，其本质在于为系统中的每个任务分配合适的资源，从而使得系统达到某种状态，如资源利用率最高、闲置资源最少或者吞吐率最高等。近年来深度学习的流行，尤其是强化学习的兴起，使得部分研究者开始思考利用机器学习算法解决资源调度问题 [3, 4, 11]。一般而言，此类算法旨在从过去的任务执行记录中“学习”相关的规律，以指导为未来系统的调度动作。

第二章　面向人工智能的云计算系统软件研究

以深度学习为代表性技术的人工智能领域在 21 世纪 10 年代再度兴起，社会各界对于人工智能的需求也愈发旺盛。遍布超市和餐馆中的扫脸支付技术、智能手机上的语音智能助手、工厂中检测废件的自动检测装置等，都离不开人工智能技术的加持。具体的，上述场景都需要适当的机器学习模型在线部署以提供服务。

机器学习的工作流一般遵循如下几个步骤：1）模型开发与调试。在此阶段中，开发者根据具体的场景，编写并调试模型代码。2）模型参数调整。在这个步骤中，开发者使用训练集不断调整模型的超参数，使其在测试集上的表现符合某种标准（如准确率高于某个阈值）。3）模型部署，开发者将开发完成的模型部署到对应的场景中对外提供服务。

为了方便开发者专注到模型的开发流程中，各大主流云厂商均实现了支持机器学习模型开发-调试-部署整个流程的软件栈。同时，云厂商提供的一般性的平台可能无法满足用户特定的需求。因此针对具体场景，学术界也提出了一系列基于云服务的机器学习软件，以达到降低开发成本、提高模型在线服务的质量等目标。本章对上述内容涉及到的相关工作展开具体研究。

2.1　一站式的云上机器学习系统

2.1.1　AWS Sagemaker

AWS 作为公有云领域的龙头老大，在云计算的前沿技术领域一直处于领先的地位。其某些代表性技术甚至成为了多数公有云厂商所共识的标杆和规范。在机器学习系统这一分领域，其代表性系统为 AWS Sagemaker。

Sagemaker 是一个实现和产品化机器学习模型的框架 [7]，用户可以将其模型训练需要的数据存储到 AWS 的对象存储服务 S3 中。然后，用户可以通过 web 的方式访问部署在云端的 Jupyter Notebook 服务，在线访问数据、编写并调试代码。当模型训练完毕后，可以使用 Sagamaker 内置的推理服务对模型进行发布。用户在发布时还可以根据平台的不同（云端或边缘节点）将模型打包编译成不同的版本。此外，Sagamaker 还内置了一些常用的算法和数据集，方便开发者直接调用。

在训练算法和系统机制方面，Sagemaker 旨在解决工业规模的模型训练场景中的如下几个常见问题：

- **支持增量式的训练和模型更新**。在真实的工业场景中，几乎不存在完全静态的

数据集。用来训练模型的数据集大多都是不断增长的。例如电商网站的用户行为数据，每天都在以相当的速度增长。在这样的动态数据上训练模型，势必要进行如下权衡：在全量数据上进行训练，可以获得质量更高的模型，然而时间和经济上的开销却会非常高；在最新更新的数据上（例如最近几天的数据）进行训练，可以快速的得到新的模型，却有可能在一定程度上牺牲模型的准确性。

- **容易估算训练模型产生的花销。**对于体量非常大的数据集，用户需要较为准确地估计训练模型将会产生的时间和经济花销。当今的云计算一般遵循按量付费的收费模式，因此云上的机器学习用户会格外关注花销的问题。
- **支持暂停和恢复模型训练，有一定的弹性。**生产环境中，大模型的训练通常包含跨越数十甚至上百台机器的并发任务。在一些场景中，由于超参数调整的需要或者计算资源的限制，开发者需要对这些任务进行中断和恢复。这就要求云上的 ML 系统能够支持大型训练任务中断和恢复时中间结果的保存和复原。
- **能够处理非持久性数据。**在很多场景中，数据并不一定是持久化的，也会有很多“瞬时”的数据，例如直播时的视频流等。这些数据一般不会被持久化保存，因此如何支持对这些数据的挖掘和学习也是一个重要的问题。
- **支持自动调参。**自动调参是一项非常耗时耗力的工作，特别是在生产环境的大数据集下。因此，如何能够支持高效的自动调参，方便用户选取合适的模型，对于云上的 ML 系统而言也是非常重要的。

2.1.2 阿里云 Max Compute

2.2 基于公有云服务的模型训练系统

2.2.1 基于云厂商动态资源的模型训练系统

2.2.2 基于云厂商动态资源的自动调参系统

2.3 基于多种服务模式的模型部署系统

2.3.1 基于多种资源混用的模型部署系统

2.3.2 基于 FaaS 的模型部署系统

第三章　云环境中新硬件为人工智能带来的机遇与挑战

第四章　人工智能对云计算的增强技术研究

第五章　重要文献与研究团队总结

第六章　下一步的研究设想

参考文献

[1] Omid Alipourfard, Hongqiang Harry Liu, Jianshu Chen *et al.* "*Cherrypick: Adaptively unearthing the best cloud configurations for big data analytics*". In: *14th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 17)*. **2017**: 469–482.

[2] Maria Casimiro, Diego Didona, Paolo Romano *et al.* "*Lynceus: Cost-efficient Tuning and Provisioning of Data Analytic Jobs*". *arXiv: Distributed, Parallel, and Cluster Computing*, **2019**.

[3] Andrew Chung, Jun Woo Park and Gregory R. Ganger. "*Stratus: cost-aware container scheduling in the public cloud*". In: *Proceedings of the ACM Symposium on Cloud Computing*. **2018**: 121–134.

[4] Christina Delimitrou and Christos Kozyrakis. "*Quasar: resource-efficient and QoS-aware cluster management*". In: *Proceedings of the 19th international conference on Architectural support for programming languages and operating systems*. **2014**: 127–144.

[5] Leila Etaati. "*Azure Machine Learning Studio*". **2019**: 201–223.

[6] Aaron Harlap, Alexey Tumanov, Andrew Chung *et al.* "*Proteus: agile ML elasticity through tiered reliability in dynamic resource markets*". In: *Proceedings of the Twelfth European Conference on Computer Systems*. **2017**: 589–604.

[7] Ameet V Joshi. "*Amazon's Machine Learning Toolkit: Sagemaker*". **2020**: 233–243.

[8] Ana Klimovic, Heiner Litz and Christos Kozyrakis. "*Selecta: heterogeneous cloud storage configuration for data analytics*". In: *2018 {USENIX} Annual Technical Conference ({USENIX}{ATC} 18)*. **2018**: 759–773.

[9] Yan Li, Bo An, Junming Ma *et al.* "*SpotTune: Leveraging Transient Resources for Cost-efficient Hyper-parameter Tuning in the Public Cloud*". In: *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. **2020**.

[10] Edo Liberty, Zohar Karnin, Bing Xiang *et al.* "*Elastic Machine Learning Algorithms in Amazon SageMaker*". In: *Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data*. **2020**: 731–737.

[11] Hongzi Mao, Malte Schwarzkopf, Shaileshh Bojja Venkatakrishnan *et al.* "*Learning scheduling algorithms for data processing clusters*". In: *Proceedings of the ACM Special Interest Group on Data Communication*. **2019**: 270–288.

[12] Farnaz Moradi, Rolf Stadler and Andreas Johnsson. "*Performance Prediction in Dynamic Clouds using Transfer Learning*". In: *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. **2019**: 242–250.

[13] Valerio Perrone, Huibin Shen, Aida Zolic *et al.* "*Amazon SageMaker Automatic Model Tuning: Scalable Black-box Optimization.*" *arXiv preprint arXiv:2012.08489*, **2020**.

[14] Shivaram Venkataraman, Zongheng Yang, Michael Franklin *et al.* "*Ernest: efficient performance prediction for large-scale advanced analytics*". In: *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*. **2016**: 363–378.

[15] Hao Wang, Di Niu and Baochun Li. "*Distributed Machine Learning with a Serverless Architecture*". In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*. **2019**: 1288–1296.

[16] Neeraja J Yadwadkar, Bharath Hariharan, Joseph E Gonzalez *et al.* "*Selecting the best vm across multiple public clouds: A data-driven performance modeling approach*". In: *Proceedings of the 2017 Symposium on Cloud Computing*. **2017**: 452–465.

[17] Chengliang Zhang, Minchen Yu, Wei Wang *et al.* "*MArk: Exploiting Cloud Services for Cost-Effective, SLO-Aware Machine Learning Inference Serving*." In: *2019 USENIX Annual Technical Conference (USENIX ATC 19)*. **2019**: 1049–1062.

[18] Bingbing Zheng, Li Pan, Shijun Liu *et al.* "*An Online Mechanism for Purchasing IaaS Instances and Scheduling Pleasingly Parallel Jobs in Cloud Computing Environments*". In: *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. **2019**: 35–45.