

Security Risk Measurement, Evaluation and
Management on Cloud Computing

云计算

安全风险度量评估与管理

..... 姜茸 杨明 马自飞 廖伊婕/著



科学出版社

云计算安全风险度量评估与管理

姜 茸 杨 明 马自飞 廖伊婕 著

科学出版社

北 京

内 容 简 介

本书从隐私风险、技术风险、商业及运营管理风险三个维度建立了云计算安全风险属性模型,在此基础上用信息熵、马尔可夫链、模糊集、支持向量机等理论和方法建立了云计算安全风险度量与评估模型,并通过若干案例研究验证了模型的可行性,最后给出了云计算安全风险管理和对策和建议。

本书可供信息管理、计算机、管理学等专业的博士和硕士研究生学习,也可供云计算安全管理相关领域的科研人员参考。

图书在版编目(CIP)数据

云计算安全风险度量评估与管理 / 姜茸等著. —北京:科学出版社, 2016. 11

ISBN 978-7-03-050445-6

I. ①云… II. ①姜… III. ①计算机网络-安全风险-评估②计算机网络-安全管理 IV. ①TP393.08

中国版本图书馆 CIP 数据核字 (2016) 第 264468 号

责任编辑:李 敏 杨逢渤 / 责任校对:钟 洋

责任印制:张伟 / 封面设计:无极书装

科学出版社 出版

北京东黄城根北街 16 号

邮政编码:100717

<http://www.sciencep.com>

北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2016 年 11 月第 一 版 开本: 720×1000 B5

2016 年 11 月第一次印刷 印张: 9 1/2

字数: 200 000

定价: 78.00 元

(如有印装质量问题, 我社负责调换)

作者简介

姜 茸，男，1978年2月生，理学（信息管理领域）博士，云南省中青年学术和技术带头人后备人才，云南省优秀教师，云南财经大学教授，硕士生导师。

中国计算机学会（CCF）高级会员、CCF 服务计算专业委员会委员、CCF 形式化方法专业委员会委员、CCF 会员代表、云南省系统工程学会理事。国家自然科学基金项目评审专家、云南省科技项目评审专家、云南省应用基础研究计划项目评审专家、云南省教育科学规划项目评审专家、昆明市科技项目评审专家。

近年，主持国家自然科学基金项目2项，国家社会科学基金项目、中国博士后科学基金面上项目、教育部人文社会科学研究青年基金项目、云南省应用基础研究面上项目、云南省哲学社会科学规划项目各1项；撰写学术专著1部，于中国社会科学院的经济管理出版社出版；主编“十一五”、“十二五”规划教材3部，于科学出版社出版；在 *Journal of Information Science and Engineering*、*Entropy* 等期刊独撰或以第一作者身份发表论文20余篇，其中，SCI收录4篇，EI收录7篇，CSSCI期刊5篇，中文核心期刊若干；第一发明人专利3项，第一完成人计算机软件著作权4项；获“昆明市科学技术进步奖”“红云园丁奖”“优秀教师”“科学研究成果奖”“教学成果奖”“优秀班主任”“讲课比赛第一名”等各种奖励30余项。

杨 明，男，1987年3月生，理学（信息管理领域）博士，云南财经大学讲师。

主持云南省应用基础研究青年项目1项，云南省软件工程重点实验室开放基金项目1项，任项目副组长承担完成云南省哲学社会科学规划项目1项，参与完成国家级项目2项，云南省应用基础研究面上项目1项；发表论文8篇，其中EI收录1篇，CSSCI期刊2篇，ISTP检索1篇，中文核心期刊2篇，科技核心期刊2篇，获得“昆明市科学技术进步奖”1项。

马自飞，男，1990年3月生，理学（信息管理领域）博士，云南大学博士研究生。

在读期间，主持云南省教育厅科学研究基金项目、第七届云南大学研究生科研创新项目各1项，参与国家自然科学基金项目、国家社会科学基金项目、教育部人文社会科学研究青年基金项目；发表论文3篇，其中，CSSCI期刊2篇，中文核心期刊1篇；获“优秀团员”“优秀党员”“优秀学生干部”“优秀毕业生”“省政府奖学金”等各种奖励。

廖伊婕，女，1976年6月生，历史学（唐宋经济史领域）博士，经济师，云南开放大学资产管理与评价处副处长。

曾在中国人文社会科学核心期刊《思想战线》发表过论文“基于人口发展预测的我国生育政策调整方案研究”、“试论中国古代近海市场”。

前 言

云计算是近年来全球信息产业界、学术界、政府等各界最热门、最关注的高新技术之一，是新一代信息技术变革的核心，它代表 IT 领域向集约化、规模化与专业化道路发展的趋势，是 IT 行业不可阻挡的发展大趋势。世界各强国都把云计算作为未来战略产业的重点，云计算是国家战略需要。

云计算环境中，用户甚至不需投资基础设施就可获得强大的计算能力，只要向云服务商提出请求和交纳低廉的费用即可。它使得用户从基础设施投资、管理与维护的沉重压力中解放出来，可以更专注于自身核心业务发展。

然而，安全风险已成为云计算发展的一大障碍。著名机构 Gartner、IDC、Unisys 分别对全球安全风险作调查。Gartner 调查显示：70% 以上受访首席技术官（CTO）认为近期不采用云计算的首要原因是安全风险问题；IDC 调查显示：75% 的受访者一致认为安全风险是云计算发展的最大挑战，是其最关心的问题；Unisys 调查显示：72% 的受访者认为阻碍云计算的首要原因是安全风险问题。日本调查显示，用户采用云计算的最大顾虑是安全风险问题。Forrester Research 调查显示，90% 以上德国和法国 CIO 声称，安全风险性保障是他们采用云计算的前提。

安全风险问题严重阻碍云计算的发展，其根源在于云计算的特点、云计算安全技术 and 风险管理理论的不够完善。因此，要大规模应用云计算技术与平台，发展更多用户，推进云计算产业发展，就必须开展云计算安全风险理论研究，度量和评估该风险刻不容缓。但是，目前这方面理论研究极为匮乏！

鉴于此，本书探索用信息熵、马尔可夫链、模糊集、支持向量机等理论和方法度量和评估云计算安全风险。

第 1 章介绍了本书研究的背景、意义、主要内容及创新成果、本书组织及各章概要。第 2 章阐述了本书相关研究的基础理论，并对本书研究内容的国内外研究现状进行了综述。第 3 章将云计算安全分为隐私风险、技术风险、商业及运营管理风险三个维度，建立了云计算安全风险属性模型。第 4 章结合信息熵原理和

马尔可夫链针对云计算风险的大小展开了深入的研究和探讨,提出了云计算安全风险度量模型。第5章基于信息熵和模糊集理论,建立了云计算安全风险评估模型。第6章结合信息熵和马尔可夫链方法围绕风险的损失影响、威胁频率和不确定性程度针对云计算安全风险进行了详细的量化评估,建立了风险评估模型。第7章提出了基于信息熵和支持向量机的云计算安全风险分类和评估的方法,为风险评估提供了新的思路。第8章基于前面章节,围绕云计算安全在用户隐私保护、技术规范、法规约束、管理制度等多方面,提出了若干管理对策和建议。第9章回顾、总结本书所做工作,并对未来进行展望。

作者的研究得到国家自然科学基金项目(No. 61263022、61303234)、国家社会科学基金项目(No. 12XTQ012)的支持,本书得到云南财经大学博士学术基金全额资助出版,在此表示谢意!

本书的出版得到伏润民教授、费宇教授、赵丽珍老师的支持,该研究得到廖鸿志教授、李彤教授、夏幼明教授等专家的指导与帮助,项目研究过程中张秋瑾女士做了部分工作,在此一并表示感谢!

由于作者水平和时间有限,书中不当之处敬请读者批评指正。

著 者

2016年7月于云南财经大学

目 录

前言

第1章 绪论	1
1.1 研究意义	2
1.2 主要研究内容	4
1.3 主要创新成果	6
1.4 本书组织结构	7
第2章 相关理论概念及研究综述	10
2.1 信息熵	10
2.2 马尔可夫链	12
2.3 云计算	14
2.4 风险理论	15
2.5 云计算安全风险	16
2.6 本章小结	19
第3章 云计算安全风险属性模型	21
3.1 概述	21
3.2 云计算安全风险因素分析	24
3.3 云计算安全风险属性模型的建立	35
第4章 基于信息熵和马尔可夫链的云计算安全风险度量	38
4.1 度量模型	38
4.2 案例研究	49
4.3 模型的优势及合理性	58
第5章 基于信息熵和模糊集的云计算安全风险评估	61
5.1 云计算安全风险的模糊集	61
5.2 基于模糊集合熵权的云计算安全风险评估	63
5.3 案例研究	65
5.4 本章小结	71

第6章 基于信息熵和马尔可夫链的云计算安全风险评估	73
6.1 评估模型	73
6.2 案例研究	81
6.3 模型的优势及合理性	93
第7章 基于信息熵和支持向量机的云计算安全风险评估	96
7.1 云服务安全目标及技术	97
7.2 云服务各层次安全问题	101
7.3 评估模型	105
7.4 案例研究	111
7.5 模型的优势、特点及合理性	121
第8章 云计算安全风险管控对策和建议	123
8.1 云计算发展的需求及管理对策建议	123
8.2 各部门职能及任务要求	128
第9章 结论与展望	133
9.1 研究工作回顾	133
9.2 未来工作展望	134
参考文献	136

第 1 章 绪 论

20 世纪 60 年代云计算的思想早已萌生, John McCarthy 作为云计算的先驱, 曾预示在未来计算机能力也能够像水、电、煤气等商品一样, 以一种按需服务的模式被人们所公共取用和购买。如今, 随着传统数据采集和存储方式的转变, 过去无法实现的海量数据存储在今天已经成为了可能。在此基础上, 为了应对当前计算量越来越庞大、数据结构越来越复杂、实时变化越来越快的用户业务需求, 云计算以一种崭新的姿态出现在大众眼前, 它改变了大众对于互联网业务的认识, 凭借其强大的计算能力和高效低廉的便捷服务特点受到各行各业的青睐。随着国内外云计算研究的深入和互联网知识的普及, 越来越多全新的服务和应用模式正逐渐显现, 为当前的政府、企业或个人业务需求的处理带来了极大的方便。

云计算是网格计算、并行计算、虚拟化等技术进一步发展而来的产物, 是时代发展的需求, 也是时代所赋予我们的机遇和挑战。目前, 云计算正向着更贴近用户需求、更多样化、更便捷的服务方向发展, 被众多学者认为是又一次重大的技术产业革命, 势必会对未来信息化产业的发展带来长远的影响。云计算的市场潜力巨大, 对传统产业的转型升级和新兴企业的成长具有重大的意义, 全世界许多国家都对其发展寄予厚望, 将云计算列为国家产业发展的战略重点。

然而, 作为一种基于互联网的新兴产业模式, 云计算的发展仍处于起步阶段。它是由传统技术发展和融合的产物, 虽然在技术支撑上其并不缺乏, 但是在多技术运用的过程中却难免会产生技术上的疏漏。另外, 许多企业对于云计算的实施和应用都处于尝试的阶段, 未能妥善地做好风险的预防和控制措施, 在面对突发的风险时, 由于自身经验的不足通常会显得措手不及, 从而造成不必要的经济损失。可见, 虽然云计算能够为用户提供强大的计算能力, 但是云计算多租户、资源共享、跨区域分布等特点也为用户的隐私安全带来了隐患。近年来不乏用户信息被盗、数据丢失、数据泄露的相关消息被报道, 一时间用户的隐私安全成为了云用户最为关心的问题。除了用户隐私的保护外, 在执行云计算服务的过程中, 管理和技术的支撑也必不可少, 突发的网络攻击、负载过重、自然灾害等

都会导致服务的中断,给风险的维护造成困难,形成经济损失。更进一步,即使不考虑风险的管理与技术因素,服务商所采取的运营方式和所处的环境对当前云计算安全也是重大的威胁。已知在当前服务双方的关系中,用户只能够凭借自身的认识和经验去判断某服务商所能够提供的服务及其安全性,在使用过程中也只具有部分管理和控制权限。服务商则具有较大的管理和控制权限,服务双方的这种不平衡势必为用户的隐私安全埋下隐患。一旦风险发生,双方都将受到直接的危害,此时对于风险的责任应该如何判定,赔偿应该如何执行,当前的相关法律法规都没有明确说明。法规的缺失导致了风险纠纷处理的困难,同时也为犯罪分子带来了可乘之机,威胁着整个云计算服务的安全。综上所述,云计算虽然有较好的发展前景,是未来经济发展的重要支点,但当前云计算技术运用的不规范、管理方案的落后、运营经验的不足、服务双方的不理解、法规的不完善、监督部门的缺失等原因却成为了制约当前云计算推广和发展的关键。

要彻底解决以上问题,加快当前云计算发展的脚步,就需要深入地对当前云计算风险环境进行全面剖析。但是传统的风险研究理论却并不能很好地适用于云计算风险环境的描述和研究,而目前对于云计算安全风险的研究又较为笼统和匮乏,大部分都是经验型的定性分析,未能通过数据的对比解释和说明各风险的特征及其相互关联。即使有定量的分析,也只是集中于以上诸多问题中的一个问题,并且在量化分析的过程中存在较大的人为主观因素影响,导致研究结果与真实数据之间存在差异,不能够准确反映和说明当前云计算所处的风险环境。为此,本书拟在现有相关风险理论和云计算研究的基础上,结合系统科学理论、系统工程的实践方法、信息论以及相关的数学计算方法综合地对云计算安全进行探讨和研究,克服以往研究过程中所存在的问题,围绕当前云计算发展过程中所遇到的问题通过调查研究进行风险因素的梳理和分析,并在此基础上建立云计算安全风险的度量与评估模型,最终为风险的管理和决策提供合理、可靠的实施方案。

1.1 研究意义

(1) 云计算是国家战略需要

云计算是近年来全球信息产业界、学术界、政府等各界最热门、最关注的新

技术之一,是新一代信息技术变革的核心,它代表 IT 领域向集约化、规模化与专业化道路发展的趋势,是 IT 行业不可阻挡的发展大趋势。我国“十二五”“十三五”规划纲要都将云计算列为重点发展的战略性新兴产业,规划纲要指出,应在未来鼓励企业间的相互合作、通过资源集中努力打造云计算产业链,推动市场经济的发展。以云计算为驱动力的绿色低碳和公共效用 IT 已受到世界各国政府的极大关注和重视(冯登国等,2011),世界各强国都把云计算作为未来战略产业的重点,国家支持云计算关键技术研发和重大项目建设,云计算是国家战略需要。

(2) 对于用户云计算成本低、能力强、使用便捷、管理轻松

云计算环境中,用户不需投资基础设施就可获得强大的计算能力(Ward and Sipior, 2010),只要向服务商提出请求和交纳低廉的费用即可。它使得用户从基础设施投资、管理与维护的沉重压力中解放出来,可以更专注于自身核心业务发展(冯登国等,2011)。

(3) 云计算市场潜力巨大

IDC 调查显示,未来 5 年云计算服务市场将增长 3 倍(Ward and Sipior, 2010)。2012 年权威机构 Gartner 预测,未来世界云计算总收入并以每年约 30% 的速度增长,是传统 IT 行业增长速度的 6 倍,在 2015 年将突破 2400 亿美元(Wyld, 2010)。计世资讯(CCW Research)的数据表示,2012 年我国云计算市场规模达到 181.6 亿元,2013 年达到 266.2 亿元,在 2014 年已经到达 383.6 亿元,每年同比增长高达 40% 以上。云计算市场范围广阔,市场潜力巨大,IDC 表示云服务市场正进入一个“创新阶段”,将会有越来越多的全新的云服务形式出现,其涉及的领域和范围也将越来越广。

(4) 安全风险是云计算发展的最大障碍

云计算有很好的前景和优势,但是,目前用户对其接受程度很低,更多人抱以观望态度,它在应用推广上遇到巨大困难,安全风险问题是云计算发展的最大障碍(Morrell and Chandrashekar, 2011; Sun, 2011)。著名机构 Gartner、IDC、Unisys 分别对全球作调查(Ahmad, 2010),Gartner 调查显示:70% 以上受访 CTO 认为近期不采用云计算的首要原因是安全风险问题(Ahmad, 2010);IDC

调查显示: 75% 的受访者一致认为安全风险是云计算发展的最大挑战, 是其最关心的问题 (Ahmad, 2010); Unisys 调查显示: 72% 的人认为阻碍云计算的首要原因是安全风险问题。日本调查显示 (Tanimoto et al., 2011), 用户采用云计算的最大顾虑是安全风险问题。Forrester Research 调查显示, 90% 以上德国和法国 CIO 声称, 安全风险性保障是他们采用云计算的前提。

可见, 安全风险问题已经成为云计算发展的桎梏, 是很多人不愿意采用云计算服务的首要原因 (Subashini and kavitha, 2011)。

(5) 结论

安全风险问题严重阻碍云计算的发展, 其根源在于云计算的特点和云计算环境下的安全风险管理决策理论匮乏 (Grobauer et al., 2010)。因此, 要大规模应用云计算技术与平台, 发展更多用户, 推进云计算产业发展, 就必须开展云计算环境下的安全风险理论研究, 度量和评估该风险刻不容缓 (Sangroya and et al., 2010)。

但是, 目前这方面理论研究极为匮乏 (Grobauer et al., 2010)。本书的研究不但可以缓解云计算风险理论研究极为匮乏的局面, 而且可供政府、企业和用户应用或参考, 从而推动云计算的推广普及。因此, 本书的研究具有较大的理论和实际意义。

1.2 主要研究内容

风险的度量与评估是当前云计算风险研究的重点, 也是云计算普及、发展和延伸的客观需求, 通过风险的度量与评估将能够为风险的识别、风险的分析、风险的管理控制以及风险的应对提供科学的依据, 从而提升云计算服务本身的质量, 打造能够支持云计算服务长期稳定运作的安全风险环境。对此, 本书拟在“有限目标、重点突出”的思想指导下, 系统深入地研究云计算环境下的安全风险度量与评估模型。然而, 要建立此模型, 首先需要根据云计算安全风险的特点, 展开详细的风险因素研究, 通过对这些风险因素的梳理为风险的度量和评估奠定基础, 最终根据风险的度量与评估结果解释当前云计算的风险环境, 针对所存在的关键问题提出合理的管理对策及建议。总的来说, 本书的主要研究内容包括以下方面。

(1) 风险因素的梳理研究

a. 云环境下隐私风险因素

隐私安全一直是用户在考虑选择某云计算服务时最为关心的首要因素。云计算复杂的风险环境决定了其隐私安全必然会受到诸多因素的影响。本书将围绕用户的隐私安全,从不同的角度探讨在云计算服务和应用过程中可能对用户隐私形成威胁的风险因素,包括用户隐私数据的窃取、泄露、公开和丢失等风险问题。

b. 云环境下技术风险因素

技术因素是支撑云计算应用安全的关键,也是实现云计算长远发展的关键。采用哪些技术能够降低风险?不采用某种技术将会存在何种风险隐患?当前的技术支持存在哪些弊端?围绕这些问题本书将通过调查研究和实例分析的方法凝练云计算环境下技术风险的主要因素。

c. 云环境下运营管理风险因素

云计算作为一种新兴的商业模式,在管理制定和运营规范上显得较为落后。云计算商的经验不足,对于云计算服务的实施和管理都处于摸索阶段,面临运营管理中突发的风险将难以应对;另外,目前法律法规的不完善,也为云计算的安全带来了隐患。这就导致当前云计算系统在实际的运营管理过程中存在诸多的风险可能,对此本书将整理和列举这些有关风险因素,为后续的风险度量和评估做支撑。

(2) 云计算安全风险属性模型

要研究云计算安全,首先需要解决的就是进行风险的识别,并梳理它们之间复杂的关系,建立系统的研究体系。对此本书站在用户和服务商双方的角度,围绕云计算安全用户隐私安全、系统运行技术支撑以及商业环境威胁等安全问题展开了详细的探讨,凝练了云计算环境下数据隐私、技术支撑、商业及运营管理等三个维度的若干风险因素,并在此基础上结合系统科学理论的研究方法,根据它们之间的交叉关系建立后续用于度量和评估的云计算安全风险属性模型。

(3) 云计算安全风险度量模型

风险的度量是本书研究的核心内容之一,风险度量的任务就是量化风险的大小(整体、局部或单个风险因素)。鉴于风险是一个抽象的概念,要对其进行度量势必会存在人为主观的界定,如何有效降低风险度量过程中人为主观偏差的影

响,是本书风险度量所需要解决的关键问题。对此,本书将在所建立安全风险属性模型的基础上,结合传统风险理论和信息熵计算方法,从不同层次、不同角度综合地对云计算风险大小进行度量,从而建立云计算安全风险度量模型,将该模型代入具体安全中进行案例分析,并从理论上对所提出模型的科学性和合理性进行论证。

(4) 云计算安全风险评估模型

风险的度量解决了抽象风险量化分析的问题,而风险的评估则是在此基础上对云计算风险环境进行评价和分析的研究。本书所采取的风险评估是一种定性定量相结合的方法,通过风险的评估能够定量描述当前云计算环境的安全性程度,为用户提供一个可供参考比较的评估结果,同时也能够为云计算运营商风险的管理和控制提供最直接有效的科学依据。

(5) 云计算安全风险管理的对策及建议

最终,在经过风险的度量和评估以后,本书将针对当前云计算服务过程中所存在的主要问题,结合未来云计算发展的客观需求,围绕法律法规的制定、技术运用的规范、用户隐私的保护及管理制度的完善等方面提出若干合理的管理对策及建议,从而规范当前云计算市场,酿造安全的云计算服务环境,加速当前云计算技术的发展和推广应用。

1.3 主要创新成果

本书围绕云计算安全展开了深入的研究,所取得的主要创新成果包括以下方面:

1) 通过风险的梳理,从隐私保护、技术支撑和运营管理三个维度列举和说明了可能存在的若干风险因素,并在此基础上考虑各风险因素之间的关联,建立云计算安全风险属性模型,实现对云计算风险环境系统全面的描述。

2) 本书采用信息熵的计算方法,有效地降低了对风险大小进行评估界定时人为主观偏差较大的影响,所得风险度量结果较为客观,缩小了度量结果与真实数据之间的差异。

3) 相对以往的研究,本书所提出的风险度量模型,引入了对风险多种随机可能状态变化的描述和考虑(即各风险同时发生或单独发生不确定性的考虑),

并结合马尔可夫链原理计算风险发生的稳态概率，克服了以往对于云计算安全风险之间不确定性研究不足的缺点。

4) 采用定性定量相结合的方法，针对不同的问题提出了多种云计算安全风险的评估研究方法，实现了对云计算安全的多层次、多角度评估，做到了具体问题，具体分析。

1.4 本书组织结构

本书整体的研究思路如图 1-1 所示。

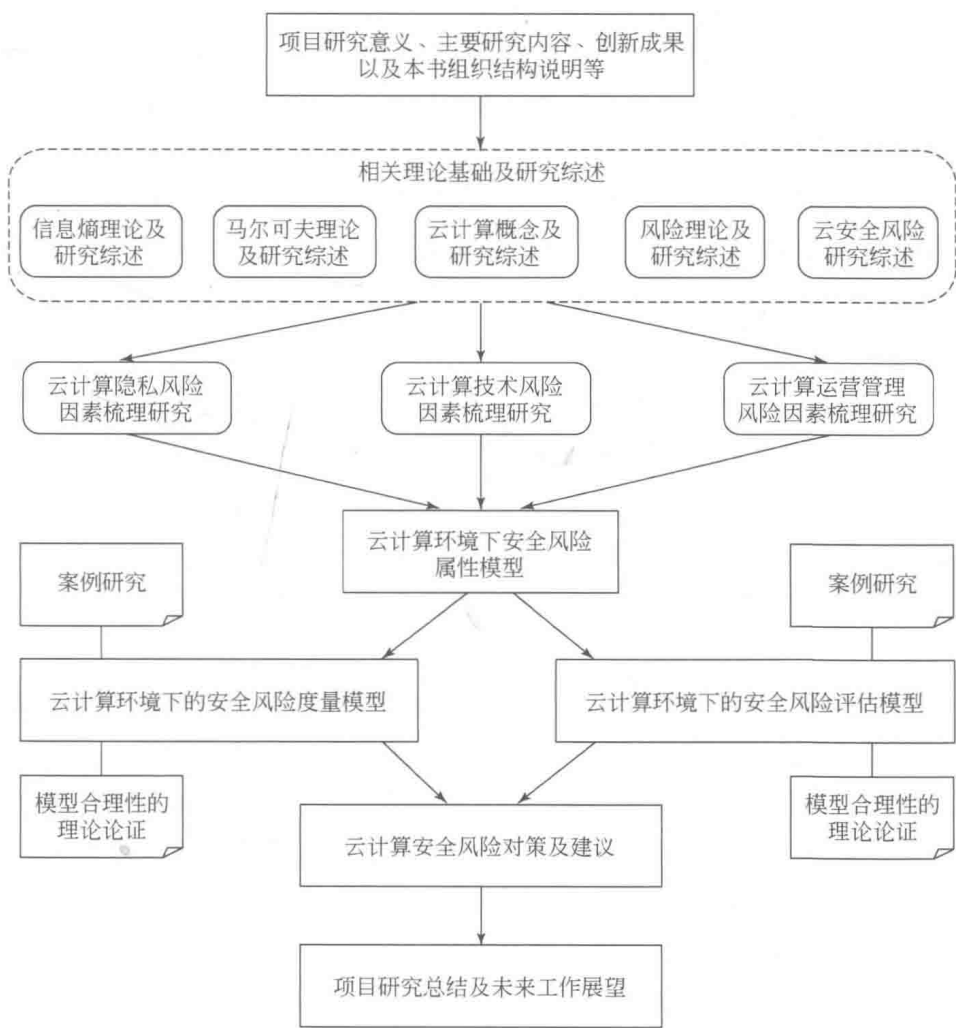


图 1-1 本书整体研究思路图

按照项目的研究思路,本书共9章,各章的具体内容编排如下:

第1章,绪论:介绍了本书研究的背景和意义、主要研究内容,论述了本书的主要创新成果,最后介绍了本书的组织结构安排和各章主要内容。

第2章,相关理论概念与研究综述:本章阐述了本书相关研究的基础理论,并对国内外当前研究现状进行了综述。主要包括:信息熵原理、马尔可夫原理、云计算概念、风险理论及云计算安全风险研究的相关基础理论介绍和研究综述,探讨了本书研究工作中所需要解决的问题,最后结合本书研究的特点,论述了这些相关基础理论对本书研究工作的意义,指出了本书后续研究工作的方向。

第3章,云计算安全风险属性模型:本章将围绕用户隐私保护、系统技术支撑和服务运营管理,将云计算安全分为隐私风险、技术风险、商业及运营管理风险三个维度,并通过对当前云计算理论和应用状况的调查、研究和分析,结合现有的风险理论,提出了若干风险因素,并将这些风险因素进行梳理,建立了云计算安全风险属性模型。

第4章,基于信息熵和马尔可夫链的云计算安全风险度量:本章在所建立的云计算安全风险属性模型基础上,围绕各风险因素特点和相互关联,结合信息熵原理和马尔可夫链针对云计算风险的大小展开了深入的研究和探讨,提出了云计算安全风险度量模型,最终将模型代入具体的案例中进行实证分析,并从理论上对模型的科学性和合理性进行了论证。

第5章,基于信息熵和模糊集的云计算安全风险评估:本章基于模糊集理论,围绕云计算安全风险因素的损失影响和威胁频率,建立了用于评估的风险因素集、评价集和隶属度矩阵,并结合熵权理论针对各风险因素进行了权重赋值,最终通过计算定义了云计算安全风险的等级,为云计算安全的风险评估提供了有效的方法。

第6章,基于信息熵和马尔可夫链的云计算安全风险评估:本章根据用户所关心的问题,将云计算安全分为数据安全、网络安全、物理环境安全、管理控制安全、软件应用安全和商业安全等六个方面,结合信息熵和马尔可夫链方法围绕风险的损失影响、威胁频率和不确定性程度针对云计算安全风险进行了详细的量化评估,最终建立了风险的评估模型,并对该模型的科学合理性进行了论证,实现了对云计算安全多层次、多角度的评估。

第7章,基于信息熵和支持向量机的云计算安全风险评估:本章以云计算安全技术风险为例,针对样本数据较少的特殊情况,提出了基于信息熵和支持向量