

Broadview[®]
www.broadview.com.cn

CSAI 希赛[®]
.cn

The Way To System Analyst

系统 分析师 之路



希赛教育研发中心 组编
张友生 主编



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

http://www.phei.com.cn

TP311.52
129

CSAI 希赛®
CSAI.cn

系统分析师 之路

希赛IT教育研发中心 组编
张友生 主编

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书由希赛 IT 教育研发中心组织编写,系《中国系统分析员》杂志的精华版本。内容包括技术讲座、系统分析与建模、项目管理、软件测试、过程改进、解决方案、信息化应用、教育认证和顾问之声共 10 个方面的知识,全部由活跃在软件领域中的高级工程师编写,是作者的实践经验总结,全面反映了系统分析员(系统分析员)的工作范围。

读者通过阅读本书,可以更好地了解系统分析师的工作,掌握系统分析、项目管理及架构设计等方面的技术和管理知识。

本书可作为系统分析师、信息系统项目管理师及系统架构设计师考试的参考书籍和软件工程师进一步深造并发展的学习用书,也可作为系统分析师日常工作的参考手册和计算机专业教师的教学和工作参考书。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

系统分析师之路 / 张友生主编. —北京: 电子工业出版社, 2006.6
ISBN 7-121-02496-9

I. 系… II. 张… III. 软件工程—系统分析—工程技术人员—资格考核—自学参考资料 IV. TP311.5

中国版本图书馆 CIP 数据核字(2006)第 036013 号

责任编辑: 毕 宁 bn@phei.com.cn

印 刷: 北京东光印刷厂

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

经 销: 各地新华书店

开 本: 787×1092 1/16 印张: 24 字数: 619 千字

印 次: 2006 年 6 月第 1 次印刷

印 数: 4000 册 定价: 48.00 元

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。联系电话:(010)68279077。质量投诉请发邮件至 zlts@phei.com.cn,盗版侵权举报请发邮件至 dbqq@phei.com.cn。

编写委员会

组 编 希赛 IT 教育研发中心

主 编 张友生

编 委 (按姓名拼音排序)

曹垣亮	曹 伟	陈 庆	陈徐梅	崔启亮
葛 梅	谷剑芳	贺忻忻	黄以宽	李 雄
刘保青	刘明晶	刘云楚	刘 兴	卢琳生
江玲英	马映冰	彭国荣	漆 英	任甲林
田 晖	田俊国	王胜祥	王树文	吴吉义
谢 顺	邢绍志	熊绳祖	徐 锋	徐荣胜
颜建强	杨 飞	杨晋辉	殷建民	张 华
张 骏	朱 勤			

前 言

中国系统分析员顾问团（CSAI，希赛）组建于 2001 年 12 月 28 日，是由通过国家考试的系统分析员 / 系统分析师、信息系统项目管理师、系统架构设计师，以及从事系统分析、架构设计、项目管理多年的人士组成的。CSAI 下设 10 个专业委员会，分别按横向和纵向组织，横向有金融信息化专业委员会、制造业信息化专业委员会、计算机教育专业委员会、电子商务与电子政务专业委员会、电信应用专业委员会；纵向有软件工程专业委员会、项目管理专业委员会、数据库应用专业委员会、架构设计专业委员会、网络应用专业委员会。

CSAI 的宗旨是加强全国 IT 高级人才之间的合作与交流，提高工作水平，积极推进国家信息化建设和软件产业化发展。希赛 IT 教育研发中心是 CSAI 计算机教育专业委员会的别名，是一个专门从事 IT 教育研究、教育产品开发、教育书籍编写的组织。为了培养出更多的 IT 高级人才，希赛 IT 教育研发中心组织编写了本书。本书内容来自历年的《中国系统分析员》杂志，作为《中国系统分析员》的精华版本。

《中国系统分析员》创刊于 2002 年 6 月，从最初的电子杂志发展成为今天的正式印刷版杂志，历经三载春秋，凝聚了 CSAI 人的心血。

3 年前，CSAI 华南区首席顾问马映冰先生感叹道：“系统分析员是寂寞的。”经过 CSAI 所有顾问的努力，今天，希赛网及《中国系统分析员》杂志已经成为一个让系统分析员充分展示自己，让社会了解系统分析员的平台。通过这个平台，让我们的能量被社会认识，让我们的能力被社会认可。从而使得系统分析员不再只是一纸证书，而是一群活跃在中国 IT 界、恪尽职守的精英！今天，我们可以自豪地说，系统分析员不再寂寞！系统分析员已经成为软件业年青一代发展的方向和努力的目标。

3 年前，CSAI 资深顾问刘兴先生有感而言：“援琴鸣弦发清商，短歌微吟不能长，一个人的声音是很微弱的。”可喜的是，有了《中国系统分析员》这块我们自己的园地，已经把一人之言变成了众人之言、群体之言。政府和社会已经意识到，在软件的产业化和行业的信息化进程中，拥有一支强大的生力军——系统分析员！

当然，正如 CSAI 华北区首席顾问田俊国先生所言，系统分析员不应该是一群容易满足的人，所以这一点成绩绝对不应该成为我们骄傲的资本，一个人能否有大的作为，关键在于他有多强的使命感和社会责任感，CSAI 也不例外。

当然，通过了系统分析员考试，并不意味着可以飘飘然而不思进取，自以为是。而应以此作为新的起点，不断修炼，获取经验和知识，紧跟时代发展的步伐和技术的进步，才能保证自己不会被社会淘汰，才能确保整个系统分析员群体的高素质，才能维护“中国软件产业的脊梁，各行业信息化的精英”的良好形象和口碑，才能履行时代赋予我们

的光荣职责。

要做一个出色的“敢于承担责任的人”，《中国系统分析员》需要广大系统分析员、项目管理人员和软件工程师的呵护。众人拾柴火焰高。笔者希望每一位顾问、每一位系统分析员都能为《中国系统分析员》杂志出谋划策，贡献高质量的稿件。

我们坚信，只要《中国系统分析员》坚持高标准、高质量原则和指导软件工程实践的正确主题，必将能够影响深远，成为软件领域媒体的旗舰，成为软件企业和软件工程技术人员的必读刊物，成为培养软件工程技术人才并促进国内软件工程技术实践水平的权威刊物。

本书由希赛 IT 教育研发中心组编，由张友生主编。第 1 章由朱勤、张友生、李雄、殷建民、王胜祥编写；第 2 章由徐锋、邢绍志、黄以宽、陈庆、刘云楚、杨飞、卢琳生、任甲林、曹伟、谷剑芳、杨晋辉编写；第 3 章由吴吉义、田俊国、徐荣胜、张华、任甲林编写；第 4 章由崔启亮、贺忻、张友生编写；第 5 章由陈徐梅、葛梅、刘保青、漆英、谷剑芳、王树文、谢顺编写；第 6 章由曹伟、吴吉义、王树文编写；第 7 章由王胜祥、颜建强、曹垣亮、彭国荣编写；第 8 章由熊绳祖、张友生、张骏、刘明晶编写；第 9 章由刘兴、张华、江玲英、吴吉义编写；第 10 章由刘云楚、田俊国、马映冰、刘兴、田晖编写。

在本书出版之际，笔者要特别感谢电子工业出版社郭立女士的大力帮助。

编写委员会
2006 年 3 月

目 录

第 1 章 技术讲座	1	1.4 复杂软件驱动系统的 UCM 与 UML	37
1.1 数据库安全技术	1	1.4.1 用例映射图	38
1.1.1 数据库安全概述	1	1.4.2 UCM 和行为图	41
1.1.2 数据库系统的安全需求	2	1.4.3 UCM 和结构图	44
1.1.3 数据库系统的安全模型	2	1.4.4 讨论	45
1.1.4 数据库系统安全机制	3	1.4.5 小结	46
1.1.5 总结与展望	11	1.5 面向对象的数据存储	47
1.2 常用软件开发模型比较分析	12	1.5.1 面向对象的思想	47
1.2.1 瀑布模型	13	1.5.2 对象的持久化保存	48
1.2.2 螺旋模型	13	主要参考文献	56
1.2.3 变换模型	14	第 2 章 系统分析与建模	62
1.2.4 喷泉模型	15	2.1 使软件需求分析规格说明书 更加有效	62
1.2.5 智能模型	16	2.1.1 总体思路	62
1.2.6 增量模型	16	2.1.2 面向客户: 确认需求	63
1.2.7 WINWIN 模型	17	2.1.3 面向开发人员: 规格化需求	67
1.2.8 原型实现模型	18	2.2 结对分析	69
1.2.9 RAD 模型	19	2.3 隐性需求	72
1.2.10 并发开发模型	20	2.3.1 隐性需求有哪些	73
1.2.11 基于构件的开发模型	21	2.3.2 发掘隐性需求	74
1.2.12 基于体系结构的开发模型	21	2.3.3 隐性需求的表达方法	75
1.2.13 XP 方法	22	2.4 软件需求, 实践的艺术	75
1.2.14 第 4 代技术	23	2.4.1 引言	75
1.2.15 小结	24	2.4.2 深入理解需求	76
1.3 软件成本估计方法综述	24	2.4.3 需求分析的实践艺术	78
1.3.1 基于模型的技术	25	2.4.4 小结	82
1.3.2 基于专家判定的技术	31	2.5 关于用例的思考	83
1.3.3 面向学习的技术	33	2.5.1 用例粒度取决于客户	83
1.3.4 基于动态的技术	34	2.5.2 为用例加入设计的内容	84
1.3.5 基于回归的技术	35	2.5.3 通过用例发现客户需求	85
1.3.6 组装技术	36		
1.3.7 小结	37		

2.5.4	主业务流程和候选业务流程	88	2.10	软件需求分析	121
2.5.5	在实际工作中如何把握	88	2.10.1	需求分析的任务	121
2.5.6	小结	89	2.10.2	需求分析过程	122
2.6	需求与设计评审	89	2.10.3	需求风险	123
2.6.1	评审的必要性	89	2.10.4	需求分析人员和用户的 合作关系	125
2.6.2	评审的作用和目的	90	2.10.5	需求文档	128
2.6.3	评审的概念	90	2.11	编写项目可行性分析报告	130
2.6.4	需求与设计评审的特点	91	2.11.1	从标准谈起	131
2.6.5	评审的形式	92	2.11.2	技术方面的可行性	132
2.6.6	需求与设计评审角色	93	2.11.3	经济方面的可行性	137
2.6.7	需求与设计评审的层次	95	2.11.4	使用方面的可行性	138
2.6.8	评审的流程	97	2.11.5	小结	138
2.6.9	评审准则	99	2.12	涉众驱动的需求过程	138
2.6.10	评审常见问题	100	2.12.1	引言	139
2.6.11	评审工作建议	101	2.12.2	用户方在需求过程中 的影响	139
2.6.12	他山之石	106	2.12.3	开发方在需求过程中 的影响	140
2.6.13	评审的持续改进	108	2.12.4	投资方在需求过程中 的影响	141
2.7	论软件产品设计中的需求分析	108	2.12.5	小结	141
2.7.1	软件产品设计的重要意义	109	2.13	使用 UML 为铁路连锁软件 建模	142
2.7.2	软件产品的分类及定位	109	2.13.1	UML 建模技术概述	142
2.7.3	软件产品的非功能性 需求定义	110	2.13.2	连锁软件的结构建模	143
2.7.4	软件产品的功能设计要点	110	2.13.3	连锁软件的动态建模	145
2.7.5	软件产品工程	112	2.13.4	小结	146
2.8	企业管理软件的需求获取方法	112	2.14	某装配型制造企业 ERP 系统 需求分析	146
2.8.1	需求获取的 2 个基本原则	112	2.14.1	项目背景	146
2.8.2	需求调研的 5 个步骤	113	2.14.2	总体目标及系统范围	147
2.8.3	需求获取的重点	113	2.14.3	需求分析	148
2.8.4	需求整理与表达的方法	114	2.14.4	详细需求分析	150
2.8.5	需求获取过程中的注意事项	114	2.14.5	小结	162
2.9	企业管理软件的需求描述方法	115	主要参考文献		163
2.9.1	构成企业管理信息系统的 要素	115			
2.9.2	阅读需求文档的读者	119			
2.9.3	需求描述的表达技巧	120			
2.9.4	小结	121			

第 3 章 项目管理	164	3.5.6 合理制定进度计划, 不提倡加班	178
3.1 优化软件企业项目管理	164	3.5.7 小结	179
3.1.1 软件企业项目管理中存在的主要问题	164	3.6 运用 IBM 模型法估算软件开发工作量实例	179
3.1.2 优化软件企业项目管理的关键	166	3.6.1 质量管理平台系统简介	179
3.1.3 小结	169	3.6.2 估算方法	182
3.2 项目沟通——小故事中的大道理	169	3.6.3 质量管理平台系统功能点估算	182
3.2.1 沟通与效率	169	3.6.4 估算过程及结果	184
3.2.2 沟通与成本	170	3.6.5 建议	184
3.2.3 沟通与专业技术	170	3.7 运用 UseCase 估算工时	185
3.3 项目管理中的放弃艺术	171	3.8 项目 3 要素的内在关系探讨	189
3.3.1 需求发生重大变化	171	3.8.1 项目工期编排与按期完成的概率	189
3.3.2 合作方出现重大问题	171	3.8.2 项目进度和成本的关系	190
3.3.3 核心技术问题难以解决或技术落后	172	3.8.3 项目质量和进度、成本的关系	191
3.3.4 不利的外部政策或产业结构的变化	172	3.8.4 小结	192
3.3.5 用户需要发生重大变更	172	3.9 软件项目估计	192
3.3.6 后续资金缺乏	172	3.9.1 软件项目估计的概念	192
3.3.7 企业战略调整	172	3.9.2 软件项目估计发展现状	194
3.4 项目挣值分析及其应用	173	3.9.3 软件项目估计的基本准则	195
3.4.1 基本概念	173	3.9.4 软件项目估计方法	196
3.4.2 挣值分析应用	174	3.9.5 小结	198
3.4.3 完成情况估计	176	3.10 软件项目管理的成功原则	199
3.4.4 小结	176	3.10.1 平衡原则	199
3.5 软件项目中的人文关怀	176	3.10.2 高效原则	200
3.5.1 形式多样的交流能激发每个人的潜能	177	3.10.3 分解原则	200
3.5.2 积极引导客户, 主动获取客户真正需求	177	3.10.4 实时控制原则	200
3.5.3 专业知识重要, 整体人文素养更重要	177	3.10.5 分类管理原则	201
3.5.4 不可缺少的周末总结交流	178	3.10.6 简单有效原则	201
3.5.5 改善工作环境, 排除干扰	178	3.10.7 规模控制原则	201
		3.11 选择与使用项目经理	202
		主要参考文献	204

第4章 软件测试	206	5.2.8 有效地控制评审会的进程	235
4.1 软件本地化外包测试流程分析	206	5.2.9 加强对发现问题原因的分析	236
4.1.1 国际化软件开发流程	206	5.3 软件企业如何引进 6σ	236
4.1.2 软件本地化测试阶段	207	5.3.1 6 σ 管理法	236
4.1.3 软件本地化测试流程	208	5.3.2 6 σ 管理法的改进模型和工具	237
4.1.4 本地化测试质量控制 流程分析	210	5.3.3 6 σ 管理法可用于软件企业的 哪些方面	238
4.2 软件测试过程及方法指南	213	5.3.4 高层领导的高度关注	238
4.2.1 前言	213	5.3.5 建立组织保障	238
4.2.2 引言	216	5.3.6 选择合适的 6 σ 项目	239
4.2.3 管理	216	5.3.7 软件企业实施 6 σ 的优势	240
4.2.4 测试计划	219	5.4 深入软件过程	240
4.3 基于 Web 的系统测试方法	224	5.4.1 前奏：风险、创新与赚钱	240
4.3.1 功能测试	224	5.4.2 第 1 幕：需求，简单吗	241
4.3.2 性能测试	225	5.4.3 第 2 幕：设计，民主与集中	242
4.3.3 可用性测试	226	5.4.4 第 3 幕：测试，那些幕后的 英雄们	243
4.3.4 客户端兼容性测试	227	5.4.5 第 4 幕：发布中的角力	244
4.3.5 安全性测试	227	5.4.6 质量，选择还是放弃	244
4.3.6 小结	227	5.4.7 面对过时，怎么办	244
主要参考文献	228	5.4.8 尾声：别了，昔日的战友	245
第5章 过程改进	229	5.4.9 小结	245
5.1 依照 CMM3 级要求的软件 过程定义	229	5.5 建立软件项目质量评估体系	245
5.1.1 项目定义软件过程裁剪方法	229	5.5.1 软件项目质量评估指标	245
5.1.2 项目软件过程定义	230	5.5.2 软件项目质量评估模型	247
5.1.3 小结	232	5.6 中国 CMM/CMMI 咨询机构 10 强 调查报告	248
5.2 实施有效的同行评审	233	5.6.1 前言	248
5.2.1 建立 3 种同行评审方式	233	5.6.2 调查参与者情况	249
5.2.2 避免管理人员参与同行评审	234	5.6.3 咨询机构影响力调查	249
5.2.3 限制参加的人数	234	5.6.4 对咨询机构进行综合评价	251
5.2.4 避免争论	234	5.6.5 市场调查部分	252
5.2.5 确定评审策略	235	5.6.6 调查声明	254
5.2.6 对同行评审进行度量	235	主要参考文献	254
5.2.7 制定同行评审检查单	235		

第 6 章 解决方案	255	7.2.2 COM 组件的线程安全	299
6.1 编写中小企业 ERP 项目的解决 方案书	255	7.2.3 微软设计的解决方案	302
6.1.1 引出问题	255	7.2.4 线程模型与套间的对应关系	307
6.1.2 服装行业中中小企业问题	256	7.2.5 总结时, 就是收获时	310
6.1.3 ERP 协同电子商务解决方案	257	7.3 基于构件的 J2EE 项目自动生成 技术	312
6.1.4 供应链管理的解决方案	259	7.3.1 自动生成框架的设计	312
6.1.5 工作流的描述	262	7.3.2 自动生成框架的实现	313
6.1.6 小结	264	7.3.3 小结	316
6.2 基于架构的省级林政管理业务 系统方案	265	7.4 需求推动下的高性能 RADIUS 软件架构设计	317
6.2.1 系统技术架构	265	7.4.1 原理介绍	317
6.2.2 应用系统功能设计	267	7.4.2 宽带业务需求	318
6.2.3 网络平台方案	268	7.4.3 软件架构设计	319
6.2.4 信息安全管理服务系统方案	269	7.4.4 测试与应用效果	320
6.2.5 小结	270	主要参考文献	320
6.3 IT 运维管理方法和技术初探	271	第 8 章 信息化应用	322
6.3.1 IT 运维管理基本知识介绍	271	8.1 ERP/CRM 与 TOM 的关系	322
6.3.2 IT 运维管理的基本理论	273	8.1.1 背景	322
6.3.3 IT 运维管理的基本技术	273	8.1.2 两种模型图	322
6.3.4 IT 运维管理系统探析	273	8.1.3 模型分析	324
主要参考文献	277	8.1.4 小结	325
第 7 章 软件设计	278	8.2 解决在线信息系统的 亚健康问题	325
7.1 为 C 语言程序设计一个异常 处理框架	278	8.2.1 为什么信息系统时常罢工或 慢得如蜗牛	326
7.1.1 异常处理机制的意义	278	8.2.2 如何才能做到真正有效的主动 性能管理	327
7.1.2 C++ 异常处理模型	279	8.2.3 主动把握系统稳定性的优化 解决方案	327
7.1.3 C 语言中的 setjmp 和 longjmp 函数	280	8.3 遗留系统的评价方法和 进化策略	328
7.1.4 为 C 语言程序设计一个异常 处理框架	284	8.3.1 遗留系统的评价方法	329
7.1.5 验证异常处理框架	294	8.3.2 遗留系统的进化策略	332
7.1.6 小结及注意事项	299	8.3.3 小结	333
7.2 COM 线程模型设计解密	299		
7.2.1 从线程说起	299		

8.4 基于数字签名技术的财务管理系统.....	333	9.3.4 下午试题二论文的备考建议.....	355
8.4.1 数字签名原理.....	334	9.3.5 小结.....	356
8.4.2 系统功能设计.....	334	主要参考文献.....	357
8.4.3 小结.....	336	第 10 章 顾问之声	358
8.5 数字图书馆系统应用平台体系结构.....	336	10.1 系统分析员的 8 项修炼.....	358
8.5.1 用户分层模型.....	337	10.1.1 关于访谈和沟通.....	358
8.5.2 应用系统模型.....	338	10.1.2 全局观念和系统思考.....	359
8.5.3 技术架构.....	340	10.1.3 成功主持有效的会议.....	359
8.5.4 进一步发展展望.....	343	10.1.4 提高文字表达能力.....	360
主要参考文献.....	343	10.1.5 训练口头表达能力.....	360
第 9 章 教育认证	345	10.1.6 不断进行技术积累.....	361
9.1 美国的 IT 认证考试.....	345	10.1.7 在行业应用中形成竞争优势.....	361
9.1.1 概况.....	345	10.1.8 不断总结, 与时俱进.....	362
9.1.2 ICCP 认证考试简介.....	346	10.2 系统分析的职责分配.....	362
9.1.3 CIO 认证问题.....	347	10.2.1 业务流程分析员.....	362
9.2 漫漫系分路, 伴我进步.....	348	10.2.2 业务设计员.....	362
9.2.1 合理安排好时间.....	350	10.2.3 业务模型复审员.....	363
9.2.2 培养正确的自学方法.....	351	10.2.4 需求复审员.....	363
9.2.3 考试时沉着、冷静、细心.....	351	10.2.5 系统分析员.....	363
9.2.4 可能的话参加辅导.....	352	10.2.6 用例阐释者.....	363
9.3 信息系统项目管理师应试建议.....	352	10.2.7 用户界面设计员.....	363
9.3.1 确立正确的复习应试思想.....	353	10.3 聚为京城增辉, 散可星火燎原.....	364
9.3.2 上午试题的备考建议.....	353	10.4 寂寞的系统分析员.....	365
9.3.3 下午试题一的备考建议.....	354	10.5 一个系统分析员的希望.....	366
		10.6 CSAI 任重道远.....	368

1.1 数据库安全技术

数据库技术从 20 世纪 60 年代中期开始发展,到现在已经成为了一个活跃的学科领域。以数据库为基础的信息系统正成为经济、政务、国防等领域的信息基础设施,数据库中存储的信息的价值也越来越高,因此数据库系统的安全问题也显得越来越重要。在新的网络环境中,数据库系统需要面对更多的安全威胁,针对数据库系统的攻击方式也层出不穷。

1.1.1 数据库安全概述

数据库系统安全控制是指为数据库系统建立的安全保护措施,以保护数据库系统软件和其中的数据不因偶然或恶意的原因而遭到破坏、更改和泄露。目前,数据库系统安全与网络安全、操作系统安全及协议安全一起构成了信息系统安全的 4 个最主要的研究领域。

20 世纪 70 年代初,美国军方率先发起对多级安全数据库管理系统(Multilevel Secure Database Management System, 简称 MLS DBMS)的研究。此后,一系列数据库安全模型被提出。

80 年代,美国国防部根据军用计算机系统的安全需要,制定了《可信计算机系统安全评估标准》(Trusted Computer System Evaluation Criteria, 简称 TCSEC),以及该标准的可信数据库系统的解释(Trusted Database Interpretation, 简称为 TDI),从而形成了最早的信息安全及数据库安全评估体系。TCSEC/TDI 将系统安全性分为 4 组 7 个等级,依次是 D(最小保护)、C1(自主安全保护)、C2(受控存取保护)、B1(标记安全保护)、B2(结构化保护)、B3(安全域)和 A1(验证设计),按系统可靠或可信程度逐渐增高。

90 年代后期,《信息技术安全评价通用准则》(Common Criteria, 简称为 CC)被 ISO 接受为国际标准,确立了现代信息安全标准的框架,这些标准指导了安全数据库系统的研究及其应用系统的开发。

在安全数据库需求及信息安全标准的推动下,国外各大主流数据库厂商相继推出了各自的安全数据库产品,如 Sybase 公司的 Secure SQL Server(最早通过 B1 级安全评估)、Oracle 公司的 Trusted Oracle 7 和 Informix 公司的 Informix-online/Secure 5.0 等。近几年来,Oracle 公司的 Oracle 9i 和 Oracle 10g 从用户认证、访问控制、加密存储和审计策略等方面进一步加强了安全控制功能。

我国从 80 年代开始进行数据库技术的研究和开发,从 90 年代初开始进行安全数据库理论的研究和实际系统的研制。2001 年,中国军方提出了我国最早的数据库安全标准——《军用数据库安全评估准则》。2002 年,公安部发布了公安部行业标准——GA/T 389-2002:《计算机信息系统安全等级保护/数据库管理系统技术要求》。

90 年代以来,华中理工大学(现华中科技大学)、中国人民大学和东北大学等单位对数据库安全技术进行了研究和实践,并开发出了相应的安全数据库软件,如基本达到 B1 级安全要求的

DM3 数据库、COBASE (KingBase) 数据库 2.0 可信版本及 OpenBase Secure 等。

2003 年, 中科院信息安全国家重点实验室基于开放源代码的数据库管理系统 Postgre SQL 开发出安全数据库系统 LOIS。

总体来说, 与国外主流数据库产品相比, 我国的研究成果在安全性和可用性上还有一定的差距。

根据 2004 年底的统计, 几国外数据库管理系统在国内的市场占有率达到 95%, 国产数据库的总市场容量大约为 3.5%, 其他开源的产品大约占 1.5%。国外的数据库产品不提供源程序代码, 也很少有可供公开调用的内核接口, 从而加大了自主安全保护的技术难度。加之发达国家限制 C2 级以上安全级别的信息技术与产品对我国的出口, 所以研究开发数据库安全控制技术具有重要的现实意义, 任重而道远。

1.1.2 数据库系统的安全需求

与其他计算机系统 (如操作系统) 的安全需求类似, 数据库系统的安全需求可以归纳为完整性、保密性和可用性 3 个方面。

1. 完整性

数据库系统的完整性主要包括物理完整性和逻辑完整性。

物理完整性是指保证数据库的数据不受物理故障 (如硬件故障或掉电等) 的影响, 并有可能在灾难性毁坏时重建和恢复数据库。

逻辑完整性是指对数据库逻辑结构的保护包括数据语义与操作完整性, 前者主要指数据存取在逻辑上满足完整性约束; 后者主要指在并发事务中保证数据的逻辑一致性。

2. 保密性

数据库的保密性是指不允许未经授权的用户存取数据。一般要求对用户的身分进行标识与鉴别, 并采取相应的存取控制策略以保证用户仅能访问授权数据, 同一组数据的不同用户可以被赋予不同的存取权限。同时, 还应能够对用户的访问操作进行跟踪和审计。此外, 还应该控制用户通过推理方式从经过授权的已知数据获取未经授权的数据, 造成信息泄露。

3. 可用性

数据库的可用性是指不应拒绝授权用户对数据库的正常操作, 同时保证系统的运行效率并提供用户友好的人机交互。

一般而言, 数据库的保密性和可用性是一对矛盾, 对这一矛盾的分析与解决构成了数据库系统的安全模型和一系列安全机制的主要目标。

1.1.3 数据库系统的安全模型

安全模型也称为“策略表达模型”, 它是一种抽象且独立于软件实现的概念模型, 数据库系统的安全模型是用于精确描述数据库系统的安全需求和安全策略的有效方式。

从 70 年代开始, 一系列数据库安全模型与原型系统得到研究。80 年代末开始, 研究的重点集中于如何在数据库系统中实现多级安全。即如何将传统的关系数据库理论与多级安全模型相结合, 建立多级安全数据库系统。到目前为止, 先后提出的基于多级关系模型的数据库多级安全模型主要有 Bell-La Padula (简称为 BLP)、Biba、SeaView 和 Jajodia Sandhu (简称为 JS) 模型等。

在多级安全模型中, 客体 (各种逻辑数据对象) 被赋予不同的安全标记属性, 或称为“密级” (security level); 主体 (用户或用户进程) 根据访问权限也被分配不同的许可级 (clearance level)。

主体根据一定的安全规则访问客体，以保证系统的安全性和完整性。一般地，多级安全模型还能对系统内的信息流动进行控制。传统模式中关系的定义需要修改以支持多级关系，其中关系的完整性约束及关系操作也需要改进以保证安全性。因此，数据库系统的多级安全模型是以多级关系数据模型为基础的。

与传统关系数据模型类似，多级关系数据模型中的三要素为多级关系、多级关系完整性约束和多级关系操作。此外，为解决实际存储问题，多级关系模型中还包括多级关系的分解与恢复算法。按由大到小的次序，多级访问控制粒度可分为关系级、元组级与属性级。粒度越小，则控制越灵活，相对应的多级关系模型越复杂。

随着研究的深入，人们逐渐认识到，多级安全模型与传统的关系数据库理论（如可串行化理论等）之间存在一定的内在冲突，导致在某些问题上必须在正确性与安全性之间妥协。比如，数据库多级安全模型通过引入多实例来解决数据完整性和推理控制问题。多实例不可避免地会带来数据一致性问题，也会影响系统的运行效率，在不少场合显得弊大于利。有的学者研究了消除多实例的方法，比如通过将所有的主键赋予可能的最低安全级来消除元组多实例的发生，但是这种方法大多限制了系统的可用性和灵活性。如何在满足数据的保密性和完整性的同时兼顾系统的可用性，这一直是数据库安全模型研究需要解决的一个重要问题。

1.1.4 数据库系统安全机制

数据库安全机制是用于实现数据库的各种安全策略的功能集合，正是由这些安全机制来实现安全模型，进而实现保护数据库系统安全的目标。近年来，对用户的认证与鉴别、存取控制、数据库加密及推理控制等安全机制的研究取得了不少新的进展。

1.1.4.1 用户标识与鉴别

用户标识是指用户向系统出示自己的身份证明，最简单的方法是输入用户 ID 和密码。标识机制用于惟一标志进入系统的每个用户的身份，因此必须保证标识的惟一性。鉴别是指系统检查验证用户的身份证明，用于检验用户身份的合法性。标识和鉴别功能保证了只有合法的用户才能存取系统中的资源。

由于数据库用户的安全等级是不同的，因此分配给他们的权限也是不一样的，数据库系统必须建立严格的用户认证机制。身份的标识和鉴别是 DBMS 对访问者授权的前提，并且通过审计机制使 DBMS 保留追究用户行为责任的能力。功能完善的标识与鉴别机制也是访问控制机制有效实施的基础，特别是在一个开放的多用户系统的网络环境中，识别与鉴别用户是构筑 DBMS 安全防线的第 1 个重要环节。

近年来标识与鉴别技术发展迅速，一些实体认证的新技术在数据库系统集成中得到应用。目前，常用的方法有通行字认证、数字证书认证、智能卡认证和个人特征识别等。

通行字也称为“口令”或“密码”，它是一种根据已知事物验证身份的方法，也是一种最广泛研究和使用的身份验证法。在数据库系统中往往对通行字采取一些控制措施，常见的有最小长度限制、次数限定、选择字符、有效期、双通行字和封锁用户系统等。一般还需考虑通行字的分配和管理，以及在计算机中的安全存储。通行字多以加密形式存储，攻击者要得到通行字，必须知道加密算法和密钥。算法可能是公开的，但密钥应该是秘密的。也有的系统存储通行字的单向 Hash 值，攻击者即使得到密文也难以推出通行字的明文。

数字证书是认证中心颁发并进行数字签名的数字凭证，它实现实体身份的鉴别与认证、信息

完整性验证、机密性和不可否认性等安全服务。数字证书可用于证明实体所宣称的身份与其持有的公钥的匹配关系，使得实体的身份与证书中的公钥相互绑定。

智能卡（有源卡、IC 卡或 Smart 卡）作为个人所有物，可以用来验证个人身份，典型智能卡主要由微处理器、存储器、输入输出接口、安全逻辑及运算处理器等组成。在智能卡中引入了认证的概念，认证是智能卡和应用终端之间通过相应的认证过程来相互确认合法性。在卡和接口设备之间只有相互认证之后才能进行数据的读写操作，目的在于防止伪造应用终端及相应的智能卡。

根据被授权用户的个人特征来进行确证是一种可信度更高的验证方法，个人特征识别应用了生物统计学（Biometrics）的研究成果，即利用个人具有惟一性的生理特征来实现。个人特征都具有因人而异和随身携带的特点，不会丢失并且难以伪造，非常适合于个人身份认证。目前已得到应用的个人生理特征包括指纹、语音声纹（voice-print）、DNA、视网膜、虹膜、脸型和手型等。一些学者已开始研究基于用户个人行为方式的身份识别技术，如用户写签名和敲击键盘的方式等。

个人特征一般需要应用多媒体数据存储技术来建立档案，相应地需要基于多媒体数据的压缩、存储和检索等技术作为支撑。目前已有不少基于个人特征识别的身份认证系统成功地投入应用。如美国联邦调查局（FBI）成功地将小波理论应用于压缩和识别指纹图样，从而可以将一个 10 MB 的指纹图样压缩成 500 KB，从而大大减少了数百万指纹档案的存储空间和检索时间。

1.1.4.2 存取控制

访问控制的目的是确保用户对数据库只能进行经过授权的有关操作。在存取控制机制中，一般把被访问的资源称为“客体”，把以用户名义进行资源访问的进程、事务等实体称为“主体”。

传统的存取控制机制有两种，即 DAC（Discretionary Access Control，自主存取控制）和 MAC（Mandatory Access Control，强制存取控制）。在 DAC 机制中，用户对不同的数据对象有不同的存取权限，而且还可以将其拥有的存取权限转授给其他用户。DAC 访问控制完全基于访问者和对象的身份；MAC 机制对于不同类型的信息采取不同层次的安全策略，对不同类型的数据来进行访问授权。在 MAC 机制中，存取权限不可以转授，所有用户必须遵守由数据库管理员建立的安全规则，其中最基本的规则为“向下读取，向上写入”。显然，与 DAC 相比，MAC 机制比较严格。

近年来，RBAC（Role-based Access Control，基于角色的存取控制）得到了广泛的关注。RBAC 在主体和权限之间增加了一个中间桥梁——角色。权限被授予角色，而管理员通过指定用户为特定角色来为用户授权。从而大大简化了授权管理，具有强大的可操作性和可管理性。角色可以根据组织中的不同工作创建，然后根据用户的责任和资格分配角色，用户可以轻松地进行角色转换。而随着新应用和新系统的增加，角色可以分配更多的权限，也可以根据需要撤销相应的权限。

RBAC 核心模型包含了 5 个基本的静态集合，即用户集（users）、角色集（roles）、特权集（perms）（包括对象集（objects）和操作集（operators）），以及一个运行过程中动态维护的集合，即会话集（sessions），如图 1-1 所示。

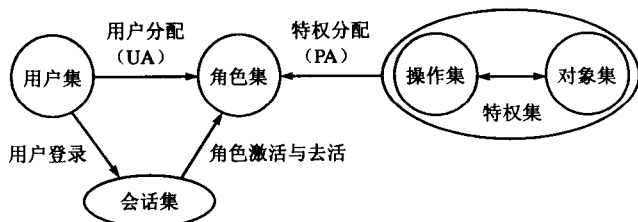


图 1-1 RBAC 核心模型

用户集包括系统中可以执行操作的用户，是主动的实体；对象集是系统中被动的实体，包含系统需要保护的信息；操作集是定义在对象上的一组操作，对象上的一组操作构成了一个特权；角色则是 RBAC 模型的核心，通过用户分配（UA）和特权分配（PA）使用户与特权关联起来。

RBAC 属于策略中立型的存取控制模型，既可以实现自主存取控制策略，又可以实现强制存取控制策略。它可以有效缓解传统安全管理处理瓶颈问题，被认为是一种普遍适用的访问控制模型，尤其适用于大型组织的有效的访问控制机制。

2002 年，Park. J 和 Sundhu. R 首次提出了 UCON（Usage Control，使用控制）的概念。UCON 对传统的存取控制进行了扩展，定义了授权（Authorization）、职责（Obligation）和条件（Condition）3 个决定性因素，同时提出了存取控制的连续性（Continuity）和易变性（Mutability）两个重要属性。UCON 集合了传统的访问控制、可信管理，以及数字权力管理，从而用系统方式提供了一个保护数字资源的统一标准的框架，为下一代存取控制机制提供了新思路。

1.1.4.3 数据库加密

由于数据库在操作系统中以文件形式管理，所以入侵者可以直接利用操作系统的漏洞窃取数据库文件，或者篡改数据库文件内容。另一方面，数据库管理员（DBA）可以任意访问所有数据，往往超出了其职责范围，同样造成安全隐患。因此，数据库的保密问题不仅包括在传输过程中采用加密保护和控制非法访问，还包括对存储的敏感数据进行加密保护，使得即使数据不幸泄露或者丢失，也难以造成泄密。同时，数据库加密可以由用户用自己的密钥加密自己的敏感信息，而不需要了解数据内容的数据库管理员无法进行正常解密，从而可以实现个性化的用户隐私保护。

对数据库加密必然会带来数据存储与索引、密钥分配和管理等一系列问题，同时加密也会显著地降低数据库的访问与运行效率。保密性与可用性之间不可避免地存在冲突，需要妥善解决二者之间的矛盾。

数据库中存储密文数据后，如何进行高效查询成为一个重要的问题。查询语句一般不可以直接运用到密文数据库的查询过程中，一般的方法是首先解密加密数据，然后查询解密数据。但由于要对整个数据库或数据表进行解密操作，因此开销巨大。在实际操作中需要通过有效的查询策略来直接执行密文查询或较小粒度的快速解密。

一般来说，一个好的数据库加密系统应该满足以下几个方面的要求。

- ① 足够的加密强度，保证长时间且大量数据不被破译。
- ② 加密后的数据库存储量没有明显的增加。
- ③ 加解密速度足够快，影响数据操作响应时间尽量短。
- ④ 加解密对数据库的合法用户操作（如数据的增、删、改等）是透明的。
- ⑤ 灵活的密钥管理机制，加解密密钥存储安全，使用方便可靠。

1. 数据库加密的实现机制

数据库加密的实现机制主要研究执行加密部件在数据库系统中所处的层次和位置，通过对比各种体系结构的运行效率、可扩展性和安全性，以求得最佳的系统结构。

按照加密部件与数据库系统的不同关系，数据库加密机制可以从大的方面分为库内加密和库外加密。

（1）库内加密

库内加密在 DBMS 内核层实现加密，加 / 解密过程对用户与应用透明，数据在物理存取之前完成加 / 解密工作。