硕士学位论文

（工程硕士）

移动业务支撑网安全管理系统设计与实现

DESIGN AND IMPLEMENTATION OF SECURITY MANAGEMENT SYSTEM FOR MOBILE SERVICE SUPPORT NETWORK

朱苏楠

哈尔滨工业大学

2018 年 6 月

国内图书分类号：TP311　　学校代码：10213
国际图书分类号：621.3　　密级：公开

工程硕士学位论文

移动业务支撑网安全管理系统设计与实现

硕士研究生：朱苏楠
导　　师：李全龙 副教授
副 导 师：钟　山
申请学位：工程硕士
学　　科：软件工程
所在单位：软件学院
答辩日期：2018 年 6 月
授予学位单位：哈尔滨工业大学

Classified Index: TP311
U.D.C: 621.3

Dissertation for the Master's Degree in Engineering

DESIGN AND IMPLEMENTATION OF SECURITY MANAGEMENT SYSTEM FOR MOBILE SERVICE SUPPORT NETWORK

Candidate: Zhu Sunan
Supervisor: Associate Prof. Li Quanlong
Associate Supervisor: Zhong Shan
Academic Degree Applied for: Master of Engineering
Speciality: Software Engineering
Affiliation: School of Software
Date of Defence: June， 2018
Degree-Conferring-Institution: Harbin Institute of Technology

摘　要

互联网高速发展的同时也给人们带来了层出不穷的安全隐患，并且终端的安全漏洞数量只增不减，如若一旦安全性受到威胁，将会给整个网络的运营带来严重的后果，会给企业、甚至国家带来极大的安全威胁。保证终端的安全性迫在眉睫，如何对终端进行安全管理成为很多企业、单位首要考虑的事情。

近些年来黑龙江省的移动业务飞速增长，移动用户的数目越来越大，与此同时信息安全每况日下，原有的管理措施已不能满足黑龙江移动在权限管理、认证管理、审计管理等方面的安全管理要求。亟需一个对移动业务支撑网的安全管理系统，实现对业务支撑网的管理、认证、授权、审计等安全功能。本文设计并实现了业务支撑网安全管理系统，主要完成以下工作：

首先，分析了业务支撑网安全管理系统的研究背景和意义，包括当前的国内外研究现状以及存在的问题，提出了研究业务支撑网安全管理系统的必要性和紧迫性。其次，完成了安全管理系统的需求分析，主要介绍安全管理系统的功能性需求和非功能性需求，为后续业务网安全管理系统的设计和实现提供了基础。接着，设计安全管理系统，包括安全管理系统总体架构，以及数据库设计、每个功能模块的功能设计等。然后，完成了安全管理系统的开发与实现，提供了各功能的实现结果，接着为安全管理系统的各个功能模块实现了详细的功能测试及性能测试，测试结果符合预期要求。

最后，概括本文研究内容，并明确日后研究中需要优化和改善之处。

关键词：终端安全；业务支撑网；安全管理系统

Abstract

The rapid developing Internet brings the endless security risks and the security vulnerabilities increase. Once the safety is threatened, many serious results will be brought to the Internet, the companies and even the country. It's urgent to guarantee the terminal security. How to manage the terminals safely has been a foremost consideration of companies and departments.

In recent years, the China Mobile business of Heilongjiang province develops rapidly and the number of users becomes bigger and bigger while the information security status becoms worse and worse. The original management measurement can not satisfy the safety management requirement in right management, authentication management and audit management of Heilongjiang Mobile. As a result, a security management system of Mobile service support network is needed, which can realize the management, authentication, authorization and audit function to the service support network. This paper design and realize the service support network security management system. The paper mainly completes the following work:

Firstly, this paper describes the research background and analysises the significance of doing research on the service support network security management system, and the research status of inland and abroad and the existing problems recently, then raises the necessity and urgency of researching the service support network security management system. Secondly, this paper focuses on the functional requirements of each function module and non-functional requirements of the security management system, which is a basis to design and implementate the security management system. Thirdly, the description of the security management system dedign is given. It introduces its general framework, as well as the functional design and database design of each functional module in the security management system. Fourthly, it completes the development and implementation of the service network security management system and many screenshots of functions are shown. And then it completes the functional testing and performance testing of each functional module in the service network security management system. The testing results conform to the expected demand.

Finally, the paper summarizes the research content and specifies what to optimize and improve in future research.

Keywords: terminal security, service support network, security management system

目　录

第 1 章 绪　论

1.1 课题的来源、背景、目的及意义

1.1.1 课题的来源和背景

在互联网飞速发展的时代，各种网络安全问题也随着而来，木马、病毒、恶意攻击等对网上应用带来很多不安全因素，并且终端的安全漏洞数量只增不减，如若一旦安全性受到威胁，将会给整个网络的运营带来严重的后果，在不确定因素的极强毁坏力的作用下，企业以及事业单位在经济财富方面会遭受重创，同时甚至会给国家社会经济带来极大的危害。保证终端的安全性迫在眉睫，如何对终端进行安全管理成为很多公司、单位首要考虑的事情。

近些年来移动公司的业务越来越繁忙，移动用户的数目越来越大，但是安全隐患越来越多，现有的管理系统已经无法满足安全管理的需求，以下是主要存在问题：

（1）各应用系统中的帐号、密码策略和认证授权机制都是独立的，数据库也是分开的，管理员也不一致。但是移动公司定期需要对各个应用系统进行维护，将会面临复杂而繁重的工作量。

（2）对于整个业务支撑网中的各类资源，由于应用系统间互相独立，资源的管理也是各自为政，导致无法按照最小权限原则为用户进行集中的资源分配。然而用户的数量还在不断增加，更是加重了权限管理的任务。

（3）系统中存在共用帐号情况，这会导致帐号管理困难，而且多人使用更容易导致安全漏洞的产生，另外当发生安全事故时，究竟是哪个用户在使用帐号是很难确定的，致使责任认定困难。

（4）用户在若干个系统中拥有若干个帐号，随着多种业务同时进行工作，在不同应用系统中不断切换，因此需要进行频繁地输入帐号密码进行不同系统的认证，操作繁杂，影响了工作效率。同时用户为便于记忆，会设置相同的帐号密码或者选择简单的安全性不高的密码，导致安全漏洞的产生。

（5）由于各个应用系统是独立的，那它们的审计是也是相互独立的。只能在单个应用系统内进行审计工作，缺少日志数据的关联分析，这对审计任务的综合分析带来了困难，致使当有入侵行为时没有办法及时发现，进而无法进行警报以及责任的及时追踪。

介于上述存在的严重问题，迫切需要一个统一的基础安全服务系统为用户和资源提供安全严格的管理。移动业务支撑网安全管理系统的建设能够有效有序地对用户、资源进行统一集中的管理，为移动公司业务的安全运行提供可靠的保障，协助移动公司日常井然有序地运作。

1.1.2 目的及意义

近些年来移动公司的业务越来越繁忙，移动用户的数目越来越大，但是安全隐患越来越多，从前的管理系统已经无法满足安全管理的需求，亟需一个业务支撑网管理系统。该系统建设目的是将中国移动业务支撑网中的帐号管理、认证、授权以及审计整合集中到一起，构建一个可以对整个系统中的用户、资源进行有效集中管理的安全管理系统，称为 4A 安全管理系统。

在 4A 管理系统的帮助下，移动公司可以集中地管理用户及用户所需的资源，且 4A 管理系统具有较好的拓展性，可以很容易地集成新的应用。根据移动公司的实际需求，按照“事先授权，事中监控，事后审计”的原则对事务的整个生存周期进行监控管理进而构建安全管理系统，为各种用户及各类资源提供安全管理服务，不仅可以安全管理内部人员还可以管理外维人员的访问，可以统一管理控制各类系统资源及应用资源，为移动公司的业务系统提供安全管理支撑。

1.2 国内外研究现状分析

随着全球互联网的高速飞快发展，网络中的安全隐患也随之层出不穷，木马、病毒、恶意攻击等对网上应用带来很多不安全因素，并且终端的安全漏洞数量只增不减，如若一旦安全性受到威胁，将会给整个网络的运营带来严重的后果，在不确定因素的极强毁坏力的作用下，企业以及事业单位在经济财富方面会遭受重创。对终端安全性进行保障的方法一般有两个，一个是保证接入信道的安全性，另一个是保证终端的安全性。

为保证终端的安全性，其一是，在从 20 世纪 90 年代初期至今的二十多年间，国内外的学者与研究人员研究了很多确保终端安全接入网络的方法。很多新概念被相继提出，例如入侵检测[1]、攻击检测[2]、联动防御[3]、可信计算[4,5,6]等，专家们提出这些概念的根本出发点都是终端安全，他们认为终端安全是防范的根本，是保证整个信息平台的安全的基础。根据这样的理念，许多被开发的实现信息系统安全的软硬件平台中，都着重研究开发终端安全准入控制技术，并将其作为产品的核心技术和核心构造。其中较为出名的是华为公司的安全渗

透网络 SPN 及思科公司的自防御网络 SDN[7]。随着信息安全问题越发受到公众重视，移动互联网安全市场开始迅速发展，从 Juniper Research 的调查结果来看，全球移动设备安全如查杀毒安全软件、将智能移动设备安全接入等，截止到 2011 年其市场价值总额已达 50 亿美元，同时在安全接入与加密上的费用超过了 6.76 亿美元，增长率超过 50%。

其二是终端安全管理的研究，国内外陆续提出 AAA、4A 的概念，两者所研究内容很相似。其中，AAA 由国外提出，分别取自 Authentication、Authorization 和 Administration 的三个 A，表示认证、授权、管理。4A 的概念是由国内提出，取自 Account Management、Authentication、Authorization 和 Audit 的四个 A，表示帐号管理、认证、授权及审计。认证解决的是“你是谁？”，授权解决的是“你能做什么”，审计解决的是“发生了什么”。很显然，国内的 4A 与国外的 4A 的差别在于第三个 A，国内 4A 突出帐号管理（Account Management），而国外 AAA 强调管理（Administration），包含了帐号管理、资源管理、权限管理在内的更广泛的管理概念。国外的 AAA 产品主要有 Sun 公司的 Identity Manager、IBM 的身份和访问管理整合服务、CA 公司的 eTrust 以及 BMC 公司的 Control-SA[8]等等，这些产品多以身份识别与访问管理的套件出现。国内目前有很多相关的安全产品，如安盟的身份认证令牌产品、绿盟安全审计平台产品等。但这些产品只能完成一两项功能，且彼此互相独立，缺乏关联，没有被统一地合成起来。国内的 4A 产品中，大部分是在各个公司研究领域的基础上改进而来，如北京国富安公司开发的 4A 管理平台是由认证产品改进的，而启明星辰公司开发的 4A 管理平台是由审计产品改进的。还有一些是与国外公司合作开发的，由国外的 IAM 产品改进而来，如天懋公司的 Trustmo-4A。

除了公司开发的产品外，在学术领域还有很多研究成果。在国外，Dan 提出智能化的集认证、授权、管理于一身的安全管理平台，该平台可以自动地将密码密钥、证书和特权与各种各样的设备和环境中的安全应用程序集成使用[9]。Chang 等提出一种云计算环境的身份验证和授权插件模型，使云客户在部署应用程序时依然保持对企业信息的安全控制管理[10]。Kubovy 等提出了一种确保身份验证、授权和资源服务器之间的安全通信的方法，还介绍了中央认证和授权系统（CAAS），一种实现和使用令牌加密的 OAuth2.0 框架[11]。针对将企业业务平台与不同的认证机制集成在一起时存在重复认证和授权、授权管理困难等问题，Li 等提出了一种在标准接口中使用认证代理和授权代理来传递认证和授权结果的方法，在单点登录的设计与实现中进行了运用 [12]。随着企业从集中式迁移到分布式计算环境，安全策略的管理，特别是授权策略，正变得越来越

困难，Varadhara 等研究并设计了安全分布式授权服务框架解决了分布式授权问题[13]。Lenz 等为欧洲跨越国家电子身份管理平台提出一种新颖的跨界授权方法，可以帮助完成进行跨境身份认证和授权管理[14]。Tumin 等认为若将用户和资源均看成个体的话，授权关系是纷繁复杂的，所以该文献提出用户组和资源组的概念，用于减少现有关系的数量，从而简化授权管理任务[15]。针对数据库的访问控制，Jonscher 等描述了一个基于角色的授权方案，该方案可以避免隐式访问权限的选择，进而可以对数据库进行安全的访问控制[16]。Zhao 等提出了一种基于三层结构的数字文档管理方案，该方案采用对称加密、组合密钥和硬件加密技术实现加密、数字签名、认证和授权等功能，保证了数字文档的安全性。另外基于上述技术实现了数字文档管理系统，该系统可以很容易地集成到现有的办公自动化系统中，提高了管理水平、工作效率以及促进了资源共享[17]。

在国内，王立强研究并改进了天津移动 4A 管理平台，综合考虑接入资源的应急切换、金库认证应急切换和统一认证管理的应急切换三种模式，开发了 4A 应急管理平台，提升了对发生故障时的应急处理能力，但是没有涉及授权、认证、审计管理等方面的处理 [18]。赵瑞星设计实现 4A 平台，对帐号、IT 资源以及权限集中管控，解决了河南移动在帐号管理、权限管理上存在的问题 [19]。王明强为实现 4A 管理平台的应急处理能力，综合考虑资源、金库以及认证的应急切换，再多重机制的保障下使得平台的应急处理能力得到了大幅度的改善[20]。郭敏针对 4A 管控平台存在内部人员的高权限帐号被滥用的风险，设计并实现了平台的金库管理系统[21]。杨诚炜设计实现了既方便了业务人员进行设备的管理和操作的、又保证业务支撑网的安全的 4A 管理平台，特别是对于业务工作人员的不安全操作能够起到很好的监管作用，防范因不正规操作而导致的安全事件发生[22]。

审计在安全管理系统中扮演着的重要角色，其对于发现系统中存在的安全隐患或者安全漏洞起着至关重要的作用。随着移动业务量的不断上升，现有的一些审计策略已经很难满足需求，越来越多的审计策略被提出来对日志进行分析。徐开勇等人对传统的 Apriori 算法进行了改进，并将其运用在日志审计中，对用户行为进行关联分析，从而发现异常将其进行记录并警报[23]。针对 Web 应用安全日志审计系统，段娟对其进行了详细的研究与设计，她将整个系统分成了日志采集、处理分析和警告三个部分来实现，并提出了一种基于强 Apriori 的免疫遗传算法从日志中提取规则，这提高了构建日志规则的准确性[24]。王玉婉设计与实现了一个针对移动互联网行为进行审计的系统，其采用了半监督学习训练方法对日志数据进行训练，然后采用选择性集成学习方法提高模型的泛

化能力，使用了这两种方法相结合来提高审计系统的业务分析能力[25]。在本文中，针对用户的行为采用隐马尔可夫链进行建模，从而发现用户平常的操作行为模式，来检测用户的异常操作，发现审计中的疑点。

近些年来移动业务越来越繁忙，移动用户的数目越来越大，但是安全隐患越来越多，从前的管理系统已经无法满足安全管理的需求，亟需一个业务支撑网管理系统。中国移动是我国特大型电信运营商之一，建设 4A 框架，不仅可以安全管理内部人员还可以管理外维人员的访问，也可以统一管控各类系统资源及应用资源，从而提升业务支撑网的安全管理能力，是一个非常重要的课题。

1.3 本文主要研究内容和结构

本文主要研究业务支撑网安全管理系统的设计与实现。建设业务支撑网安全管理系统。本文主要研究业务支撑网安全管理系统的五大功能模块：统一门户、帐号管理、认证管理、授权管理以及审计管理五个功能模块，具体内容如下：

统一门户的研究内容是为安全系统的登录提供统一的入口，在用户认证成功后，对系统资源进行集中展示，并提供单点登录等功能，方便用户操作。

帐号管理主要完成对 4A 系统中的用户、应用资源、系统资源进行集中的主、从帐号管理，包括帐号的增加、修改、删除等全生命周期管理操作，禁止所有用户在非帐号管理模块对两种资源创建帐号。

认证管理主要是设计并且实现了对系统中帐号和资源的认证，并且进行了系统资源和应用资源单点登录测试的设计与实现，使得用户能够通过统一门户界面进行审计管理、授权管理等系统的认证。

授权管理主要是设计并实现了系统中的角色和权限管理，以及在系统内的委托授权功能，使得系统用户能够在各自的权限范围内进行相应的操作。

审计管理是从日志数据的采集、标准化和分析来进行。设计了基于关键字和均值、基于用户行为模式的审计策略来对系统日志数据进行审计。

本论文分为五章，具体安排内容如下：

第 1 章是绪论，本章主要介绍业务支撑网安全管理系统的课题来源、背景、目的及意义，还有国内外研究现状分析，提出了研究业务支撑网安全管理系统的必要性和紧迫性。

第 2 章是安全管理系统的需求分析，主要介绍安全管理系统的功能性和非功能性需求，为后续的设计和实现提供基础。

第 3 章是安全管理系统的设计，给出系统总体架构、数据库设计和各个功

能模块的具体设计等。

第 4 章是安全管理系统的实现，本章完成了安全管理系统的开发与实现，提供了各功能的实现截图。

第 5 章是安全管理系统的相关功能性测试，测试覆盖系统中五个功能模块的操作分支的测试用例，并进行测试用例的实际测试。

最后总结，概括本文研究内容，并明确日后研究中需要优化和改善之处。

1.4 本章小结

本章重点说明本课题的研究背景和意义，详述了现今移动公司的业务支撑网出现的问题，提出研究移动业务支撑网安全管理系统的必要性及迫切性。此外介绍了国内外研究现状、本文主要研究内容和结构等。

第2章 安全管理系统需求分析

本章完成了对业务支撑网安全管理系统的需求分析，主要包括功能需求、非功能性需求。对于不同的功能需求，分别给出用例图。针对非功能需求，主要描述性能需求和兼容性需求等。

2.1 系统功能需求分析

移动公司的业务种类繁多，管理各部门、设备、系统等的工作纷繁复杂，管理中对安全性有严格的要求，所以亟需统一的安全管理系统，统一地管理整个公司安全有序的运营。本文设计并实现 4A 安全管理系统，该系统包括五大功能模块：统一门户功能模块、帐号管理功能模块、认证管理功能模块、授权管理功能模块、审计中心功能模块，针对每一功能模块，实现如下需求分析内容：

2.1.1 统一门户需求分析

4A 系统规定统一门户是用户在业务支撑网对资源访问的唯一入口，如果要访问资源，那么用户不可能绕过 4A 统一门户。用户成功登录后，4A 系统将向用户集中展示授权给用户的各个资源，并且用户可以通过单点登录功能直接实现资源的登录。4A 统一门户的功能要点如下所述：

（1）可以进行个人信息补全、展现帐号的权限等，还应提供主帐号密码重置功能，适用于用户主动修改主帐号密码或者密码到期更换密码的情景；

（2）在登录界面上，当主帐号输入正确的帐号密码登录成功后，可以显示本次及上次登录时间；界面应集成针对用户的个性化服务、公告信息、帮助信息等；支持个人界面锁屏，当用户登录 4A 系统后长时间不操作 4A 系统页面可自动进行锁屏，也支持用户自主的手动锁屏。

（3）可以对应用资源、系统资源进行排序展示，展示的顺序可以按照资源编号、资源种类等排列，也可按照用户自定义的顺序排列，对资源进行展示可以便于用户快定位查找相应资源。

（4）为用户提供一个个人私有的安全文件夹，对文件夹中的文件，用户可以对其进行上传、下载和分发等。

（5）支持查看待办工单列表，并且对于待办工单中涉及的资源或模块支持

直接的单点登录操作。

（6）Push 信息视窗功能，在 Push 信息视窗中用户可以查看其个人在外部系统中的工作汇总、待办任务、重要提醒等。

（7）4A 门户应支持用户自主进行主页显示设置及个人界面锁屏等；

图 2-1 展示的是统一门户的用例图。

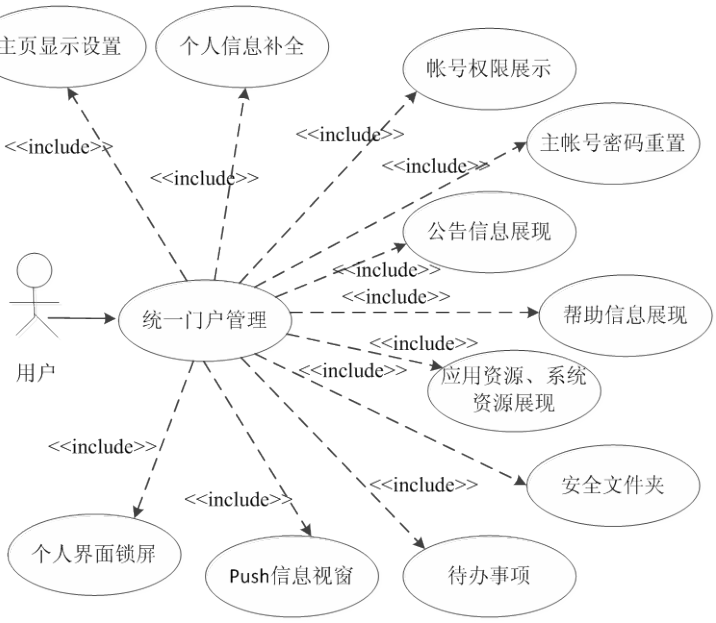


图 2-1 统一门户用例图

2.1.2 帐号管理需求分析

帐号管理涉及的帐号包括业务支撑网资源中的全部帐号，分为主帐号（自然人）和从帐号（资源）。帐号管理模块的功能主要包括主、从帐号管理和密码策略管理。

首先，主帐号管理应该实现以下功能：

（1）主帐号生命周期管理：对主帐号的创建、修改、删除、加/解锁等。

（2）主帐号属性管理：首先管理主帐号的基本属性，如个人信息（性别、年龄等）、主帐号名称、创建时间等；还涉及主帐号的扩展属性，如邮箱、电话、证件号码等；主帐号状态：包括正常、锁定、删除三种状态；还有主帐号的密码策略和认证策略；另外还有主帐号类型：应对主帐号按照工作岗位进行分类，如系统管理员、安全审计员、营业员等；最后包括主帐号标记：可以使用标记方法对主帐号进行按需的标记管理。

（3）主帐号状态管理：主帐号至少应具有正常、锁定、逻辑删除三种状态，其中，正常：是指允许该主帐号正常登录 4A 系统并访问各类资源；锁定：是指短时间禁止该帐号登录 4A 系统，可以通过解锁恢复正常状态，通常用于反映用户多次登录失败后锁定、发现违规操作锁定等，锁定状态分为管理员加锁和系统加锁，其中管理员加锁应只允许管理员进行解锁，系统加锁可以允许用户通过提交必要的身份认证信息（如短信验证码、身份证号码、预留验证问题、证书、令牌等）恢复正常状态或者由管理员进行解锁；逻辑删除：是指永久禁止该帐号登录 4A 系统，不允许恢复正常状态，通常用于反映该帐号对应的用户已离职，主帐号不允许物理删除，以便后期审计。

（4）主帐号命名管理：主帐号的命名不允许仅仅使用数字或其他编码，不允许用 BOSS 工号做主帐号；建议为用户姓名全拼，如果相同，用追加数字以保证用户名的唯一性，也可以用组织机构代码或其他标识位+人员姓名拼音等方式命名。

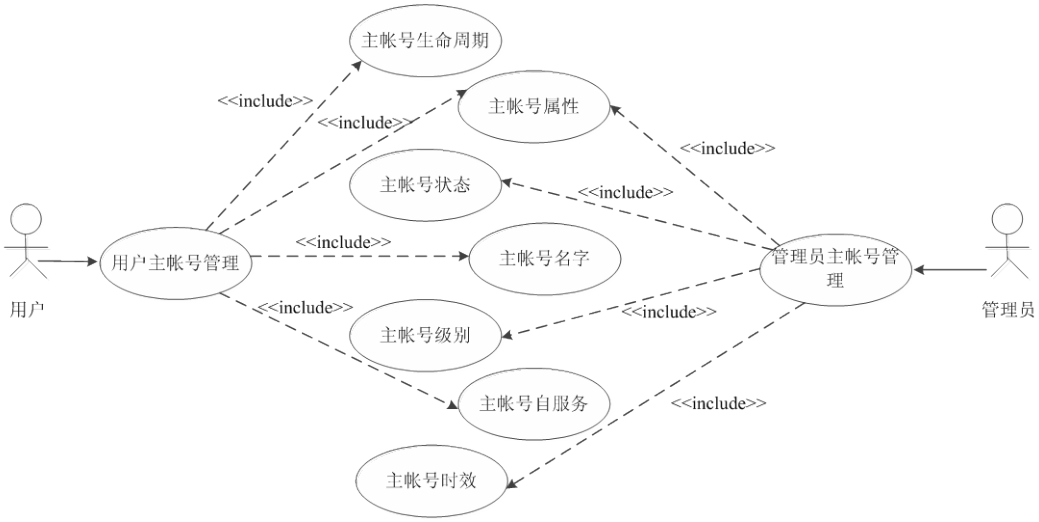


图 2-2 主帐号管理用例图

（5）主帐号分级管理：不同级别的管理员可管理的主帐号范围是不同的，如系统总管理员可以管理所有的主帐号，但是下属级别的管理员可管理的主帐号则是有限的。

（6）主帐号自助服务：用户可以自主修改自身主帐号的有关属性，无须经管理员许可，如修改性别、年龄等，也可以进行密码的修改，用户修改密码时，输入的新密码必须符合系统安全策略才可生效。严禁自然人通过自服务修改个人强认证信息（如：手机号码）、所属组织结构、主帐号角色及权限等。

（7）主帐号时效管理：应支持对长期未登录 4A 系统的主帐号的管理员人

工加锁或系统自动锁定，以防止闲置主帐号被用于攻击行为或违法操作。具备设置主帐号长期不登录的自动锁定时间阈值，如三个月。

图 2-2 展示了主帐号管理用例图。

其次，与主帐号管理类似，从帐号管理应该包括以下几个功能：（1）从帐号生命周期管理：创建、修改、删除；（2）从帐号的收集及导入：系统可以从从帐号数据库收集并向 4A 系统中导入从帐号；（3）从帐号推送及同步：4A 系统可以定期将系统中的从帐号同步地存储到对应的资源帐号库中，保证从帐号的一致性；（4）从帐号状态管理：管理从帐号的正常、锁定、删除三种状态；（5）从帐号分级管理：不同级别的资源管理员可管理的从帐号范围是不同的，如资源总管理员可以管理所有的从帐号，但是下属级别的资源管理员可管理的从帐号则是受限的；（6）从帐号自服务管理：用户可以自己管理自身拥有的从帐号，如修改从帐号属性等。

图 2-3 展示了从帐号管理用例图。

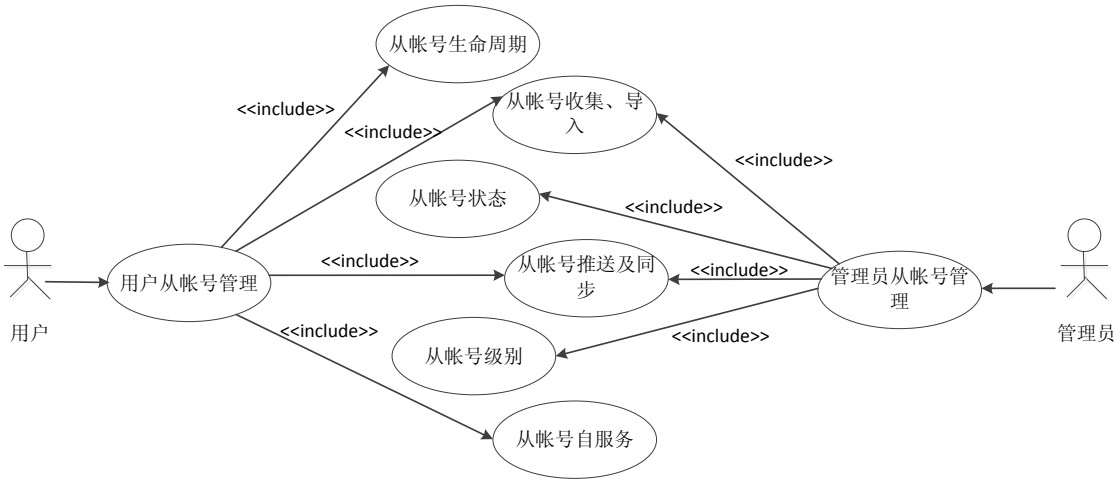


图 2-3 从帐号管理用例图

接着，在 4A 系统中，涉及到大量地密码验证工作，而且在不同的应用场景中，所涉及到的安全级别或者是加密的方式都会有不同的要求，因此会采用不同的密码策略。例如对于主帐号，系统会对其密码进行定期核查，在密码即将过期的时候，会对用户发送密码即将过期的消息，提示用户在近几天内对密码进行修改。密码策略管理应该实现以下功能：管理主从帐号的密码安全设置、组成规则及校验策略等；主帐号密码的有效期验证、提醒、管理员激活等功能，并支持分级管理；针对从帐号密码，系统需定期依据密码策略进行安全性检查，若检查不合格，则系统可以自动修改从帐号密码；帐号密码的收集、存放，为达到安全性要求，存放和传输过程都应加密。

2.1.3 认证管理需求分析

认证管理主要研究资源的认证，也就是如何对资源进行统一的安全认证服务，进而集中控制认证，保障访问资源的安全性。认证管理包括认证策略管理和从帐号单点登录认证服务。为了保证系统的安全性，不同的应用场景中应使用不同的认证策略，因此要对这些认证策略进行统一的管理。认证策略管理就是实现对认证策略的配置、查看、添加、删除等功能。认证策略主要涉及主帐号认证时的认证策略。对主帐号的认证，即对自然人认证，要求需要使用静态密码认证以及至少一种强认证策略认证。其中强认证策略包括 PKI/CA 认证[26]、令牌认证[27]、短信认证[28]和生物认证[29]等

从帐号单点登录认证服务是对从帐号的认证服务，是在主帐号认证之后执行的。4A 系统在对从帐号完成认证后才可为从帐号提供单点登录方式进行登录。从帐号的认证是在单点登录接口完成的，分为系统资源认证和应用资源认证。系统资源认证，4A 系统对于被管系统资源实现单点登录统一认证服务，对于纳入金库场景管理范围的系统资源需要进行金库认证；应用资源认证，4A 系统对于被管应用资源实现单点登录统一认证服务，对于已经接入 4A 系统且具有互访需求的应用资源，也应通过 4A 进行集中认证。

2.1.4 授权管理需求分析

授权管理是指各管理员在4A系统上赋予自然人权限的过程，用户可以在权限内进行相应的操作与访问。授权管理包括角色和权限管理以及委托授权管理。

在角色和权限管理中管理员会将各类权限关联到具体的角色，每个角色都拥有不同的权限组合，然后再将不同的角色分配给每个帐号，进而实现对用户的完整授权过程，该过程的模型如图2-4所示。

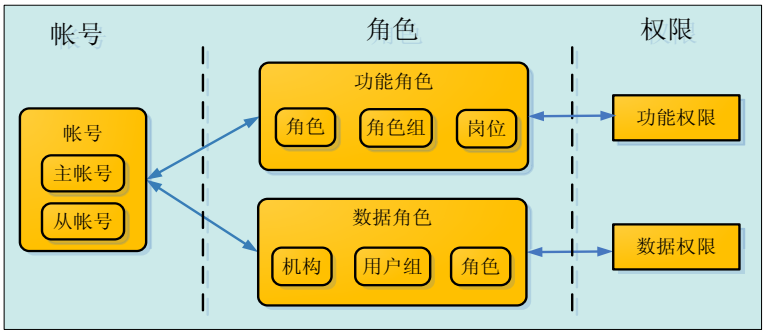


图 2-4 4A 系统授权管理模型

首先，可以将从帐号赋给主帐号，也就是将从帐号分配给主帐号进而建立

两者之间的关联。其次，可以将角色赋给帐号，一个帐号可以扮演多个角色。角色是授权模型的主体，帐号关联的角色决定了帐号最终的权限范围。在4A系统中，角色主要分为两大类：功能角色和数据角色，在接入管理的各类资源中角色的具体体现可以为角色、角色组、岗位、机构或用户组等。角色级授权需要实现角色的展示、创建、变更和删除功能，并支持应用角色的分级管理。最后，可以将权限赋给角色，每个角色都有对资源不同的处理权限。权限代表着系统中模块或对象，权限分为功能权限和数据权限。

图2-5给出了授权管理的E-R图。

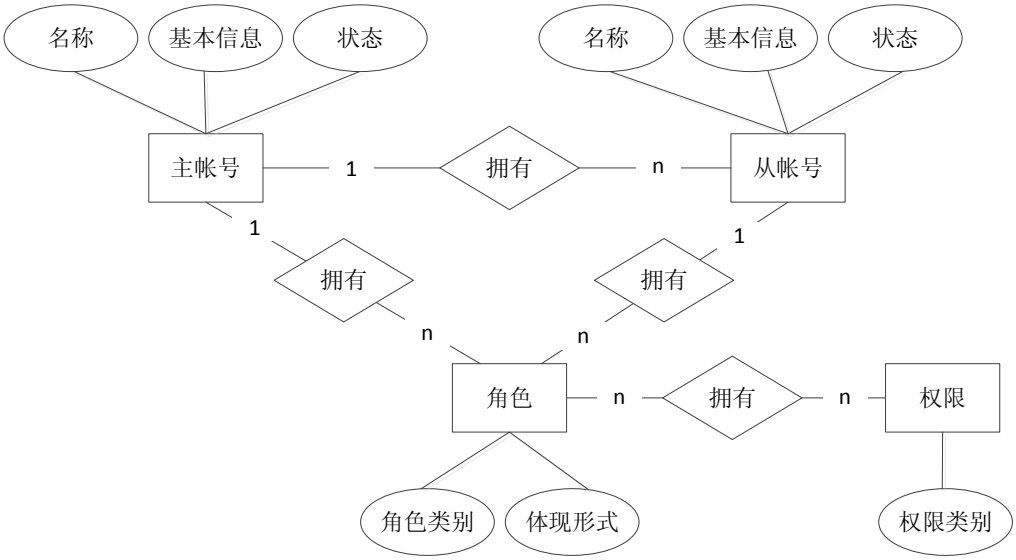


图2-5 授权管理E-R图

2.1.5 审计管理需求分析

审计管理模块的主要功能点包括审计策略中心、数据标准化、中间数据处理、数据采集、用户行为分析等，具体如下：

（1）审计策略中心：主要实现策略的创建、修改、删除、查询等功能。策略管理范围包括标准化类策略、中间处理类策略和业务分析类策略。

（2）数据标准化：首先，包括数据合法性校验，验证原始数据内容是否合法；接着是日志完整性校验，验证原始日志字段完整性；然后是日志字段映射，将原始日志解析提取的字段映射为标准化字段；最后是日志补全，将原始日志映射后的字段按照5W1H模型进行补全。

（3）中间数据处理：包括日志筛选、业务场景分析和均值统计。其中日志筛选是基于日志筛选策略从标准化日志中按照操作信息进行日志筛选；业务场景分析是基于业务场景分析策略从日志筛选结果或标准化日志中分析出异常行

为，提取出专题日志；均值统计分析是基于均值统计分析策略，对标准化日志进行统计计算，得出业务场景阀值。

（4）数据采集：主要是对主机、数据库、网络设备、应用系统等用户操作日志进行收集和存储。安全系统数据的采集范围包括 4A 系统帐号、授权管理日志；4A 系统认证、登录日志；4A 系统自管理日志等。

（5）用户行为分析：对用户在一段时间内的行为日志，进行数据分析（归并、分拣、聚类）并构建分析模型，构建条件基于行为发生 IP 地址段、行为发生时间范围、行为发生时间周期、行为结果等。

图 2-6 展示了审计管理模块的用例图。

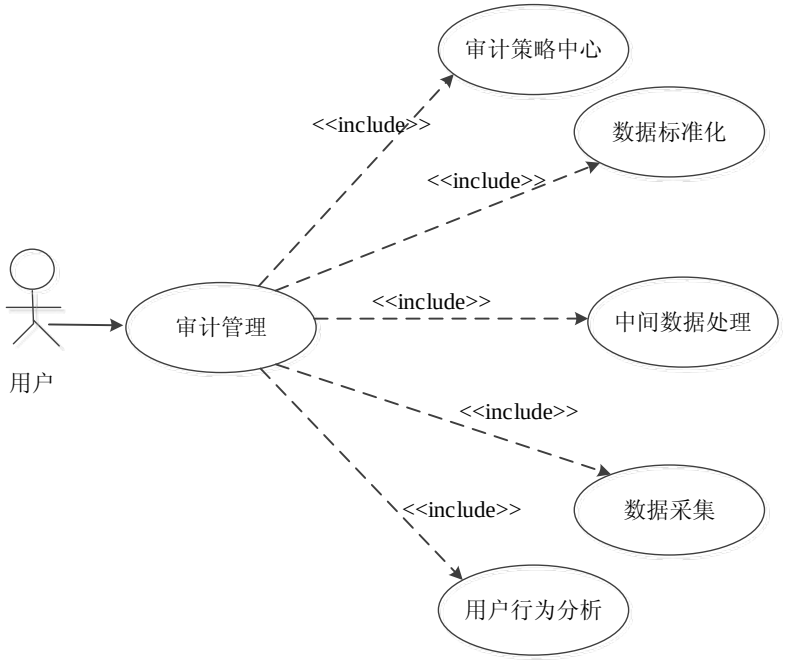


图 2-6 审计管理用例图

2.2 系统非功能性需求

2.2.1 性能需求

在性能需求方面，首先在并发上要求系统可最大同时并发 8000 用户，其次系统承载能力上，系统能够承载现网所有用户的正常操作，1.5 小时内能够加载 1.2 万用户同时在线进行登录操作。同时对操作系统级别以及数据库级别的测试指标如下：

操作系统级别的测试指标：

1）系统 CPU 利用率：不超过 70%（最大负载情况下）；

2）用户 CPU 利用率：不超过 80%（最大负载情况下）；

3）内存占用情况：不超过 80%（最大负载情况下）；

数据库级别的测试指标：

1）数据库的并发连接数能够满足用户需求；

2）数据库死锁情况：在大并发数情况下，数据库不出现死锁情况；

3）数据库服务器 I/O 情况；

2.2.2 兼容性需求分析

首先，4A 系统应该适应较为常用的 Windows 操作系统，并且支持较为常用的数据库系统，还应该支持多种主流的浏览器，要求兼容 IE7 以上版本的浏览器。

2.3 系统可行性分析

可行性分析是要分析在目前可达的环境下，是否可以按照需求分析中的完成系统的开发。本文可行性研究从以下两个方面来进行：

（1）技术可行性

技术可行性是判断设计的系统是否可以利用目前存在的技术进行实现。4A 安全系统主要完成统一门户、帐号管理、认证管理、授权管理以及审计管理功能，这些功能没有涉及到过分复杂的算法。即使有些功能点的操作比较繁琐，但是可以将其划分为细小的步骤，然后选择合适的编程语言按部就班地进行实现。数据存储方面，通过使用数据库系统可以满足系统数据存储的要求。

（2）操作可行性

使用系统的用户来源单一，用户仅包括移动公司的工作人员，随着系统的应用，会定期对公司人员的用户体验、问题反馈等进行收集统计，不断改进和优化系统，让系统更加便于用户使用。

2.4 本章小结

本章主要完成了对 4A 安全管理系统的需求分析，包括每个功能模块的功能性需求分析以及系统的非功能性需求分析（性能需求分析、兼容性需求分析等），为后续 4A 安全管理系统的设计和实现提供需求基础，另外还包括系统的可行性分析。

第3章 安全管理系统设计

基于第二章中对安全管理系统的需求分析，本章先从总体上对系统功能架构以及数据库进行设计，再分别对系统中的各功能模块进行详细的设计。

3.1 系统功能架构

根据业务需求分析，对安全管理系统的框架进行设计如图 3-1 所示。将系统设计成表现层、业务层、数据层、接口层以及外部安全组件五个部分。表现层主要对业务层的执行结果进行集中展示；业务层主要按照业务逻辑对数据层提供的数据进行操作；数据层主要实现对系统内数据库中的数据进行管理；接口层主要是提供业务层和数据层提供接口；外部安全组件主要是对业务层的功能进行补充实现，如动态令牌认证、短信口令认证等。

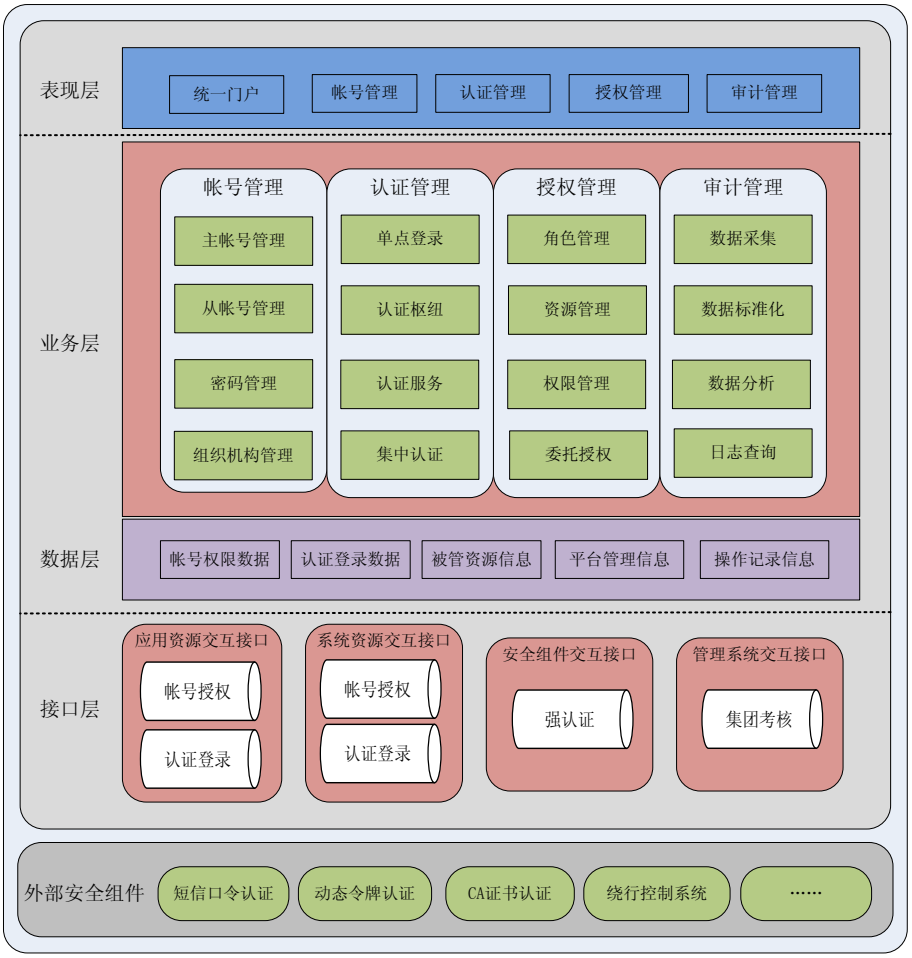


图 3-1 业务支撑网安全管理系统体系框架图

在本文中主要对业务支撑网安全管理系统中关键的基础子功能进行设计与实现，主要包括了统一门户以及帐号、认证、授权和审计五个功能模块，其结构如图 3-2 所示。

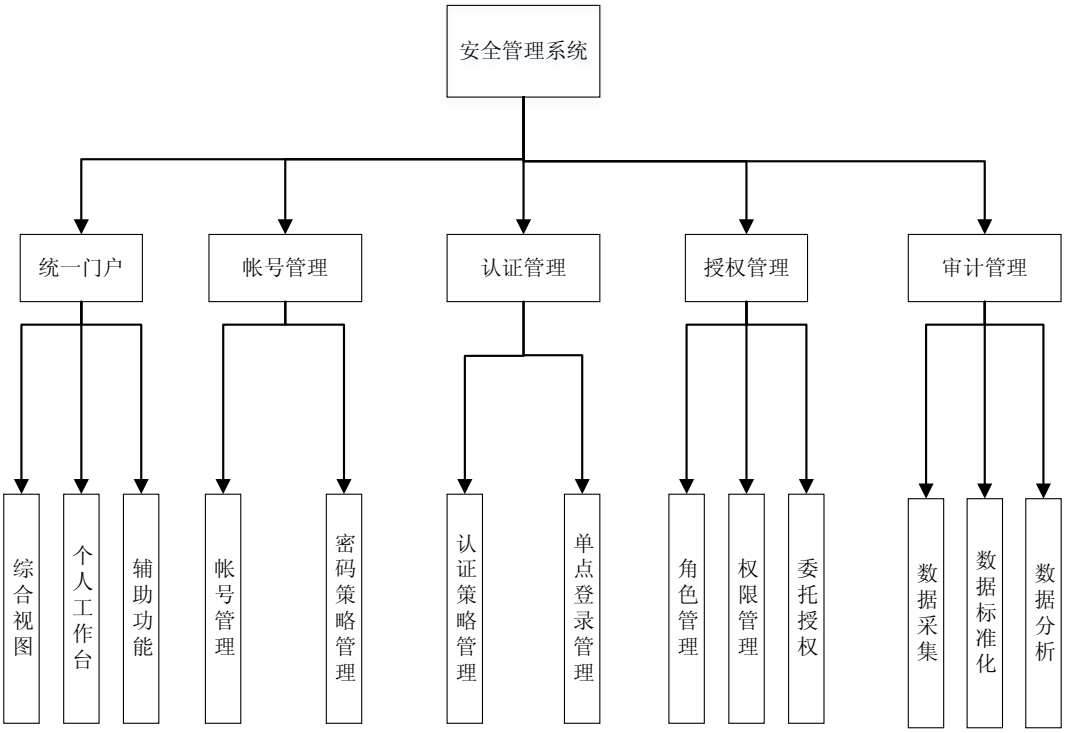


图 3-2 安全管理系统总体功能结构图

统一门户将整个安全系统的资源集中在一个页面上进行集中布局和展示。在用户进行系统登录成功后，能够将拥有操作权限的资源展示给用户，方便用户进行操作，并且在门户页面可以进行单点登录，快速进行资源的访问，而且系统内提供的消息、公告、提示等也能够在门户页面进行展示。

帐号、认证和授权管理主要是实现对系统内的用户、资源以及他们之间的权限和访问进行管理。帐号管理主要包括了对系统内的主、从帐号进行管理，对其属性进行维护 。4A 认证管理在系统中承担着对帐号或者资源的访问等操作的认证，确保访问以及资源使用合法。授权管理主要是实现对系统内用户的权限范围进行控制，规定了用户能够进行访问的范围。

审计管理主要包括了对系统内日志数据的采集、处理和分析。日志采集能够对用户的访问记录、关键操作、业务操作等进行收集和存储。通过对日志数据进行标准化后，按照不同的审计策略，可以采用不同的算法对日志数据进行分析，从而发现系统内存在的审计疑点，而发现系统内存在的业务漏洞，确保系统内的安全，并且能够为责任追踪提供证据。

3.2 数据库设计

安全管理系统的数据库整体设计如图 3-3 所示。接下来会具体介绍安全管理系统中涉及数据库的功能模块的数据库设计，分别是帐号管理模块数据库设计、认证管理模块数据库设计、授权管理模块数据库设计以及审计管理模块数据库设计。

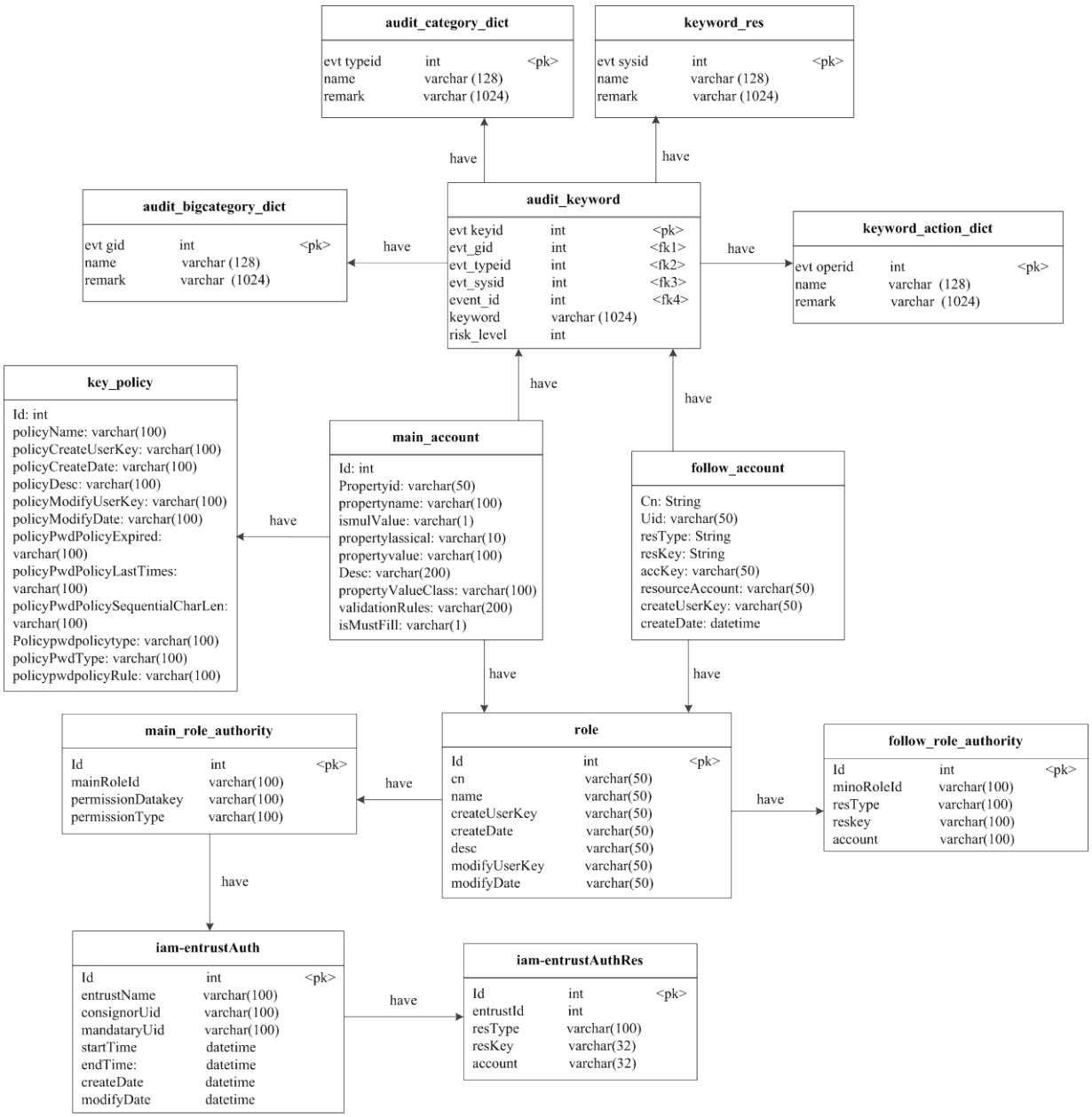


图 3-3 系统数据库整体设计图

3.2.1 帐号管理模块数据库设计

4A 帐号管理模块包含帐号管理、密码策略管理两个功能模块，其中帐号管理包括了主帐号和从帐号管理，涉及到主从帐号的新增、删除、修改以及查询等操作。为 4A 系统内所有涉及到的帐号提供有效的管理。密码策略管理模块是对主帐号和从帐号所采用的密码策略进行管理，因为不同的帐号类型所采取的密码策略存在差异。

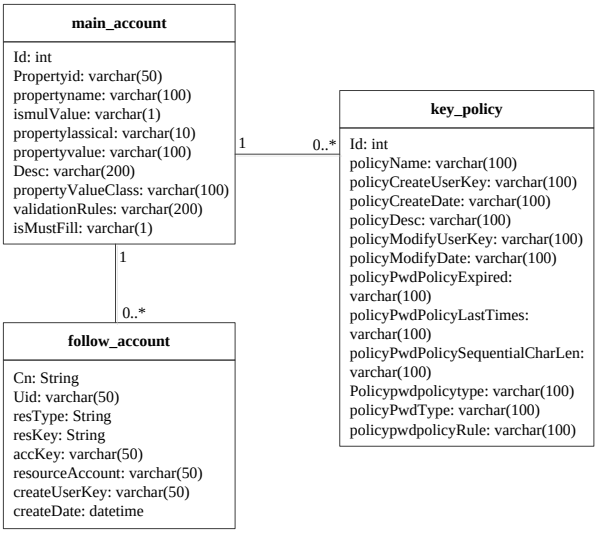


图 3-4 帐号管理模块的数据库设计

帐号管理模块的数据库设计如图 3-4 所示，其中 main_account 表是主帐号属性表，follow_account 表是从帐号属性表，key_policy 是密码策略表。一个主帐号可以拥有多个从帐号，且每个主帐号都要有多种密码策略，分别适用于不同的应用场景。接下来分别说明上述三个数据表的详细设计。

首先，主帐号属性表。主帐号属性管理的目的是能够对主帐号属性自由扩展，满足用户管理不断变化的需求。主帐号的相关属性主要包括有基本信息、扩展属性、帐号状态、密码策略、认证策略、帐号类型和帐号标记等属性。其中每种属性都可以取多个值，例如基本属性中包括了用户名、密码、Email、电话等信息。为了实现对与主帐号相关的属性的增、删、改、查操作，表 3-1 列出了数据库中添加主帐号属性的表结构。在数据库中进行存储时，将所有的属性都分成自然属性和社会属性两类，自然属性包括了帐号对应人的姓名、年龄等信息，而社会属性包括了帐号在所担任的职务、帐号类型等信息。

表 3-1 主帐号属性表

字段名称	字段描述	类型	长度	备注
Id	主键	int	8	自增 Id
Propertyid	属性 id	varchar	50	属性 id
propertyname	属性名称	varchar	100	属性名称
ismulValue	是否多值	varchar	1	是否多值（0 代表是，1 代表否）
propertylassical	属性分类	varchar	10	属性分类（目前主要分为自然属性，社会属性）
propertyvalue	属性值	varchar	100	属性值（目前主要分为单选框，多选框，下拉框）
Desc	描述	varchar	200	描述
propertyValueClass	属性值类型	varchar	100	属性值类型
validationRules	校验规则	varchar	200	校验规则
isMustFill	是否为必填项	varchar	1	是否为必填项

表 3-2 从帐号信息属性表

属性名称	要求	类型	多值	长度	备注
Cn	必选	String	N	50	系统生成的 cn 串
Uid	必选	varchar	N	50	用户的 uid
resType	必选	varchar	N	50	资源类型 资源类型分为： Unix:Unix 类型 Windows:win 类型 netDevice:网络设备 netUnit：网元 database：数据库 application:应用系统
resKey	必选	varchar	N	50	资源的 cn
accKey	必选	varchar	N	50	从帐号 key
resourceAccount	必选	varchar	N	50	资源从帐号名称
createUserKey	必选	varchar	N	50	创建者
createDate	必选	datetime	N	50	创建时间

接着，从帐号属性表。从帐号是指自然人访问业务支撑网某个资源的身份标识，按照从帐号所属的资源类型，可分为应用资源帐号和系统资源（含虚拟资源）帐号。按照从帐号的用途，包含系统帐号、管理帐号、普通帐号、程序帐号、自助终端帐号、未知帐号。类似于从帐号属性表的设计，安全管理系统从帐号属性表的设计如表 3-2 所示。

最后，介绍密码策略表的设计。在 4A 系统中，涉及到大量地密码验证工作，而且在不同的应用场景中，所涉及到的安全级别或者是加密的方式都会有不同的要求，因此会采用不同的密码策略。例如对于主帐号，系统会对其密码进行定期核查，在密码即将过期的时候，会对用户发送密码即将过期的消息，提示用户在近几天内对密码进行修改。为了更好的对系统中所使用的密码策略进行管理，设计了表 3-3 来存储系统中所使用的密码策略。

表 3-3 密码策略表

属性名称	要求	类型	长度	备注
Id	必须	Integer		主键 自增
policyName	必须	varchar	100	名称
policyCreateUserKey	必须	varchar	100	创建者
policyCreateDate	必须	varchar	100	创建日期
policyDesc	可选	varchar	100	描述
policyModifyUserKey	可选	varchar	100	修改者
policyModifyDate	可选	varchar	100	修改日期
policyPwdPolicyExpired	可选	varchar	100	有效期
policyPwdPolicyLastTimes	可选	varchar	100	强制密码历史次数
policyPwdPolicySequentialCharLen	可选	varchar	100	连续字符长度
Policypwdpolicytype	必添	varchar	100	密码策略类型，user（用户），device(设备)。
policyPwdType	必须	varchar	100	指定是模糊策略还是精确策略。模糊策略：1，精确策略：0
policypwdpolicyRule	可选	varchar	100	密码的设定规则

3.2.2 认证管理模块数据库设计

在安全管理系统中，为了保证系统的安全性，在不同的应用场景中，会存在着不同的认证策略。为了使得认证策略得到更好的管理，设计了认证策略表

3-4 来对认其进行存储。对认证策略的管理主要包括了对认证策略的新增、删除、修改和查找操作。根据不同的密码策略，会涉及到不同的认证策略。在进行认证策略的添加时，主要涉及到两个操作，第一个是检测添加的策略是否合法，例如名字是否跟已有的策略名重复，如果重复将不能进行添加。第二就是执行将数据插入到策略表中进行存储，更新数据库表。认证策略模块的认证策略表的设计如表 3-4 所示。

表 3-4 认证策略表

属性名称	要求	类型	长度	备注
id	必须	Integer	10	主键 自增
policyName	必须	varchar	100	名称
policyIsUsePwd	必须	varchar	1	是否使用静态密码:0 为不使用，1 为使用
policyLevel	必须	varchar	50	策略级别
policyCreateUserKey	必须	varchar	100	创建者
policyCreateDate	必须	datetime	100	创建日期
policyDesc	可选	varchar	100	描述
policyModifyUserKey	可选	varchar	100	修改者
policyModifyDate	可选	datetime	100	修改日期
Policyisusevpntreasury model	可选	Varchar	100	是否启用 VPN 金库认证,0 为不启用,1 为开启

3.2.3 授权管理模块数据库设计

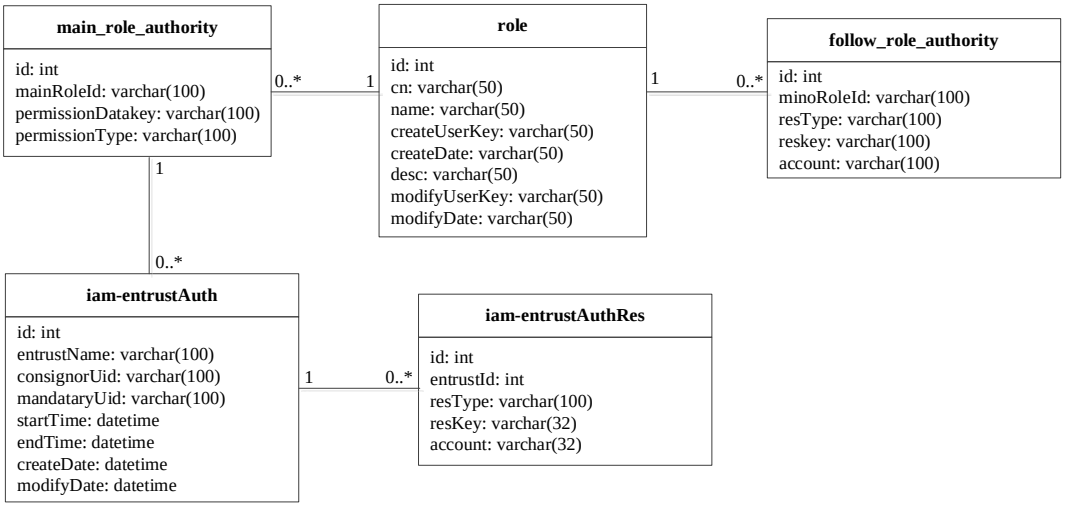


图 3-5 授权管理模块的数据库设计

授权管理模块的数据库设计如图 3-5 所示，role 是帐号角色基本属性表，如果该帐号是主帐号则会为其分配主帐号角色对应的权限，关联 main_role_authority 表即主帐号角色与权限关系表，如果该帐号是从帐号则会为其分配从帐号角色对应的权限，关联 follow_role_authority 表即从帐号角色与权限关系表。另外，主帐号可以对其拥有的从帐号进行委托授权，iam_entrustAuth 表是委托授权表，一次的委托授权可以包含多个资源的委托授权，iam_entrustAuthRe 表是资源授权与委托关系表。接下来会给出每个表具体设计。

首先，帐号角色基本属性表的设计。在进行角色创建时，不管是主帐号角色还是从帐号角色对象都应该具备的基本属性如表 3-5 所示。根据实际情况，可以对各角色的属性进行相应的扩展。在系统中，对主帐号角色的扩展属性包括了用户的组织的主键、用户组主键、资源组主键、资源组类型等，而从帐号角色的扩展属性包括了委托者与被委托者之间的关系、记录该从帐号角色被哪个用户组引用、各类型主机资源主键集合等。

表 3-5 帐号角色基本属性表

属性名称	要求	类型	多值	长度	备注
id	必须	Integer			主键 自增
cn	必选	varchar	N	50	标识符，自增编号例如：1001
name	必选	varchar	N	50	名称,存储角色名称
createUserKey	必须	varchar	N	50	创建者 (存储用户 uid)
createDate	必须	datetime	N	50	创建日期(存储格式为 YYYY-MM-DD HH:MM:SS)
desc	可选	varchar	N	200	描述
modifyUserKey	可选	varchar	N	50	修改者 (存储用户 uid)
modifyDate	可选	datetime	N	50	修改日期(存储格式为 YYYY-MM-DD HH:MM:SS)

接着，主帐号角色与权限关系表的设计以及从帐号角色与权限关系表的设计。在系统中，角色和权限的关系是关联在一起的，不管是什么级别的用户或者什么类型的帐号类型，都一定有其自己的权限，只是大和小、宽和窄的区别。在系统中角色和权限的关系表可以分为主帐号角色与权限关系表以及从帐号角色与权限关系表，主帐号角色与权限关系表、从帐号角色与权限关系表的表结构分别如表 3-6、表 3-7 所示。

表 3-6 主帐号角色与权限关系表

属性名称	要求	类型	长度	备注
id	必须	Integer		主键 自增
mainRoleId	必须	varchar	100	主帐号角色 ID
permissionDatakey	可选	varchar	100	权限值
permissionType	可选	varchar	100	权限类型 组织机构：Organization 功能：function 资源组：resGroup 用户组：userGroup

表 3-7 从帐号角色与权限关系表

属性名称	要求	类型	长度	备注
id	必须	Integer		主键 自增
minoRoleId	必须	varchar	100	从帐号角色 ID
resType	可选	varchar	100	资源类型
reskey	可选	varchar	100	资源 key
account	可选	varchar	100	从帐号

表 3-8 委托授权表

委托授权表：iam-entrustAuth

对应对象：EntrustAuthPojo 委托授权实体

属性名称	要求	类型	长度	备注
id	必须	Integer		委托授权 ID 主键 自增
entrustName	必须	varchar	100	委托授权名称
consignorUid	必须	varchar	100	委托人 UID
mandataryUid	必须	varchar	100	被委托人 UID
startTime	必须	datetime	100	开始时间 格式：yyyy-MM-dd HH:MM:SS
endTime	必须	datetime	100	结束时间 格式：yyyy-MM-dd HH:MM:SS
createDate	必须	datetime	100	创建日期 格式：yyyy-MM-dd HH:MM:SS
modifyDate	必须	datetime	100	修改日期 格式：yyyy-MM-dd HH:MM:SS

然后，委托授权表的设计以及资源授权与委托关系表的设计。在委托授权管理中用户可以将自己的从帐号委托给其他用户，并可以规定该用户对从帐号

的使用期限，到期后 4A 系统会帮助用户自动收回从帐号，用户也可以在使用期限到期前主动收回。在系统中主要进行的操作包括了增加委托授权、删除委托授权、修改委托授权以及查询委托授权操作。委托授权表、资源授权与委托关系两个表的表结构分别如表 3-8 和 3-9 所示。

表 3-9 资源授权与委托关系表

资源授权与委托关系表：iam-entrustAuthRes 对应对象：EntrustAuthResPojo　资源授权与委托关系实体				
属性名称	要求	类型	长度	备注
id	必选	Integer		关联 ID 主键 自增
entrustId	必选	Integer	100	外键：委托授权的 KEY
resType	必选	varchar	100	Unix 主机："unix"; windows 主机： "windows"; 网络设备："netDevice"; 网元："netunit"; 应用系统："application";数据库："database";
resKey	必选	varchar	32	资源 KEY
account	必选	varchar	32	从帐号 KEY

3.2.4 审计管理模块数据库设计

在审计管理模块的日志数据分析功能中，对采集的日志数据进行标准化后，为了找出日志存在的审计疑点，需按照审计策略对日志进行分析。本文采用基于关键字分析和均值统计分析的审计策略以及基于用户行为模式的审计策略。

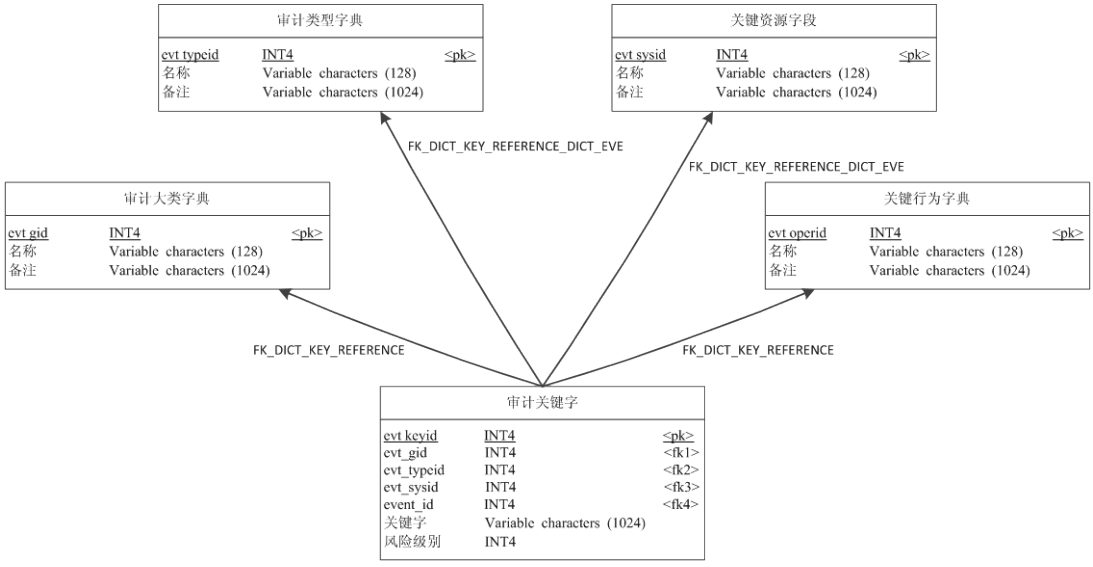


图 3-6 关键字筛选数据库设计

关键字分析时根据策略要素对标准化日志或者中间数据进行匹配和比较的过程，以发现异常和违规行为，并通过预警策略进行预警提示。关键字分析的数据库设计结构如图 3-6 所示。其中关键字分析策略就是在关键字策略的基础上加上 5 个 W(who、when、where、what、why)+how，这里的 how 就是关键字策略。

3.3 统一门户模块设计

安全管理系统的 Web 门户功能模块包括综合视图、个人工作台、辅助功能三个主要的功能，其功能结构图如图 3-7 所示。

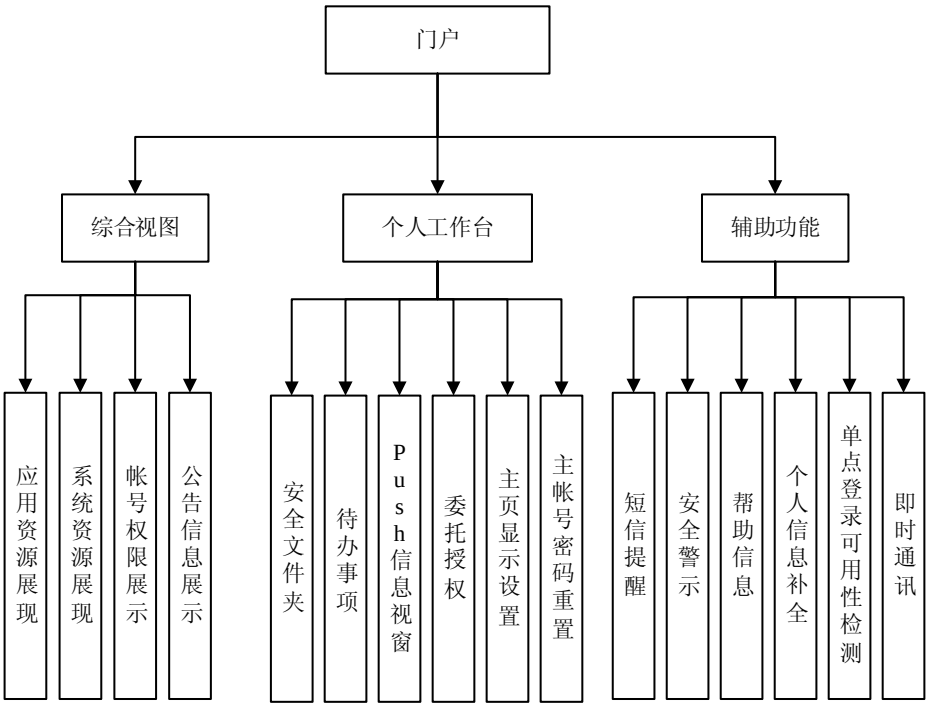


图 3-7 系统统一门户结构图

综合视图：应用资源展现是为了方便用户进行操作，在用户完成登录操作后，系统将应用资源集中展示，选择想要进入的应用系统，进行单点登录。系统资源展现是在用户认证成功后，能够在页面上看到权限内的系统资源，并且点击相应资源时可以实现单点登录。公告栏主要的是展示系统内部的通知、公告、新闻等信息，并且能够进行下载操作。为实现多个帐号相同时间并发登录门户，需要实现各服务器间的负载均衡，在网络层要实现 IP 负载均衡，在协议层采用 HTTP 重定向协议并实现 DNS 地址解析负载均衡。

个人工作台：安全文件夹是给用户提供的一个专属文件夹，能够对一些敏

感数据和文件进行相应的操作。待办事项是系统的个人工作台向用户即将要处理的业务进行提示。Push 信息视窗完成的是系统个人工作台为用户提供来自于外部系统的 Push 信息视窗展示，以便于用户直接在 4A 个人工作台查看其在外部系统门户中的工作汇总、待办任务、重要提醒。委托授权是指用户把自己的从帐号授权给其他用户使用，并设定使用周期，到期后 4A 系统自动回收，用户也可以在到期前主动回收。主页显示设置使用户可以根据自己的工作习惯对页面的内容进行调整。主帐号密码修改功能适用于用户知道主帐号的旧密码，用户自主修改密码或者系统提示用户主帐号密码过期的场景，用户可以在个人工作台中进行主帐号密码修改，系统在验证用户主帐号旧密码正确以及新密码符合密码策略要求之后，提示用户修改密码成功。

辅助功能：短信提醒功能是指 4A 系统应在主帐号登录成功、实体权限变更完成或有待办任务等情况时进行短信提醒，以减少帐号被冒用、帐号状态异常变更及工单处理不及时等问题。安全警示功能是指系统在用户登录界面或者登陆后的界面进行操作时，会给出安全提示，对于某些关键操作，给出安全警告。帮助信息功能是给用户提供系统操作指南，提供一些常用的软件工具或者应用文档的下载。在线问答功能是为系统内部的用户提供一种相互交流的途径，方便用户和管理员或者维护人员之间的沟通。单点登录可用性探测功能是指 4A 门户应提供一种对资源（系统资源、应用资源）的可用性探测功能，便于个人用户自行完成单点登录可用性探测。即时通讯功能是指用户登录 4A 门户后可以在即时通讯功能中选择用户或群组进行工作交流。

3.4 帐号管理模块设计

4A 体系框架中最重要的是 4A 帐号管理模块，4A 帐号管理模块是整个 4A 体系的管理枢纽，本文涉及到帐号管理中的帐号管理、密码策略管理两个功能模块，其中帐号管理包括了主帐号和从帐号管理，涉及到主从帐号的新增、删除、修改以及查询等操作。为 4A 系统内所有涉及到的帐号提供有效的管理。密码策略管理模块是对主帐号和从帐号所采用的密码策略进行管理，因为不同的帐号类型所采取的密码策略存在差异。一个主帐号可以拥有多个从帐号，且每个主帐号都要有多种密码策略，分别适用于不同的应用场景。接下来具体介绍帐号管理和密码策略管理这两个功能的设计。

3.4.1 帐号管理设计

在安全管理系统中，每个帐号在创建的同时，都具有多个不同类型的属性。

主帐号属性管理的目的是能够对主帐号属性自由扩展，满足用户管理不断变化的需求。主帐号的相关属性主要包括有基本信息、扩展属性、帐号状态、密码策略、认证策略、帐号类型和帐号标记等属性。

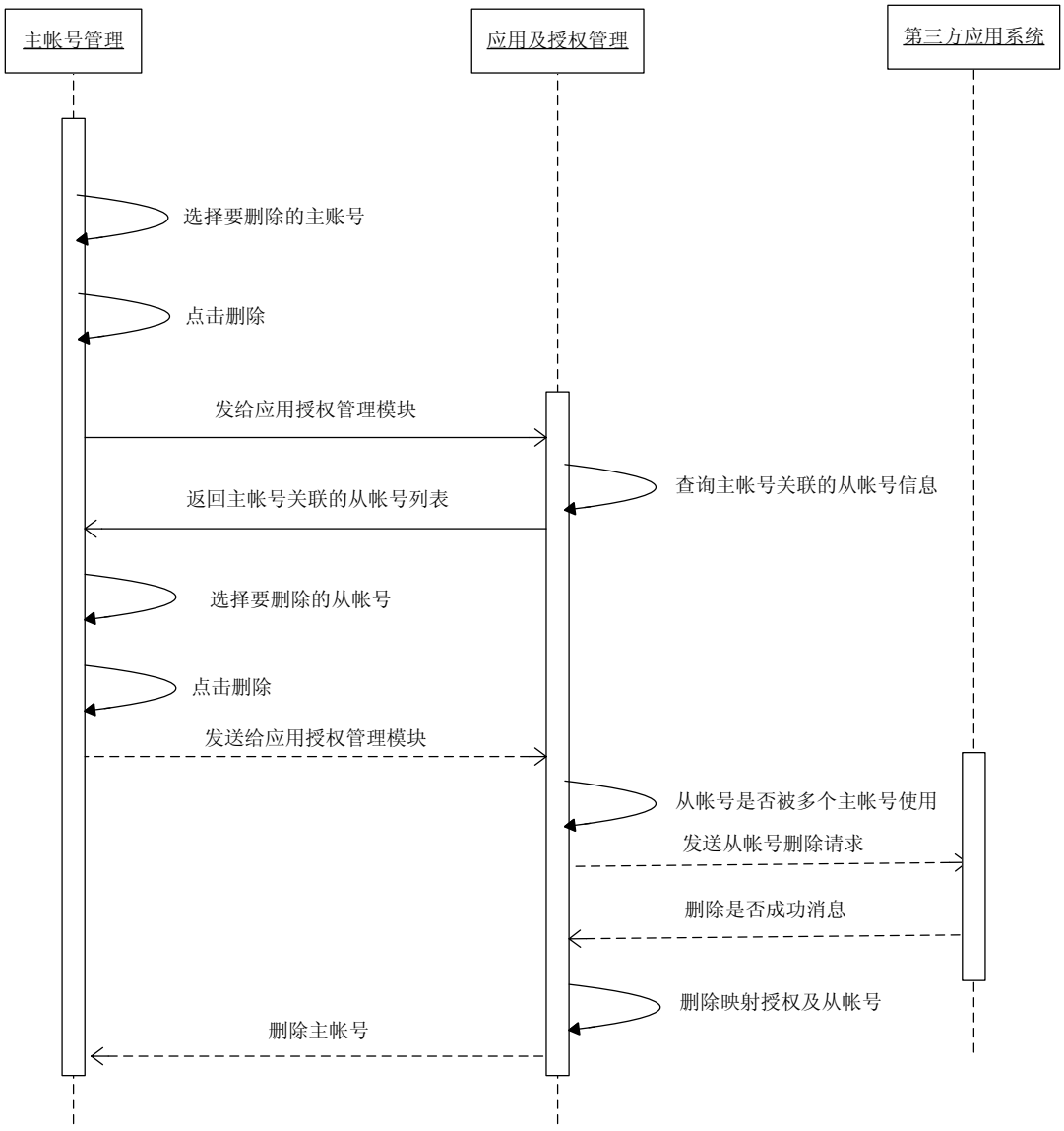


图 3-8 删除主帐号时功能调用序列图

从帐号是指自然人访问业务支撑网某个资源的身份标识，按照从帐号所属的资源类型，可分为应用资源帐号和系统资源（含虚拟资源）帐号。按照从帐号的用途，包含系统帐号、管理帐号、普通帐号、程序帐号、自助终端帐号、未知帐号，下面具体解释这几种帐号。

（1）系统帐号：资源本身自带的非管理权限帐号，如主机系统的 bin、daemon 等，此类帐号必须定义责任人，但不允许自然人使用系统帐号登录对应资源；4A 系统应支持将虚拟资源从帐号进行统一管理；

（2）管理帐号：具有系统管理权限的帐号，分为具有全部管理权限的超级管理帐号（也即特权帐号）和拥有部分管理权限的普通管理帐号。特权帐号必须绑定责任人主帐号；

（3）普通帐号：进行日常业务操作和运维的资源帐号；

（4）程序帐号：指分配给应用程序使用的资源帐号，如数据库连接帐号、模拟拨测帐号、BOMC 监控帐号、4A 同步帐号、SMP 采控帐号等，程序帐号必须绑定责任人主帐号。

（5）自助终端帐号：自助终端帐号是营业厅管理人员登录自助终端渠道使用的应用系统从帐号，该类帐号应绑定到营业厅管理人员。

（6）未知帐号或未知类型帐号：从设备上同步到 4A 系统后待设定类型的帐号，未知帐号必须先设定类型后方可进行管理操作和登录使用。

在系统中进行主从帐号的管理时，当用户出现离职等状况下，其主帐号必须进行逻辑删除，在删除主帐号同时的可选择性删除已授权的应用从帐号;同时需要注意，若 4A 系统所管理的应用系统接入方式为同步时需要删除第三方应用系统中的帐号。删除时各功能的调用关系图如图 3-8 所示。在进行从帐号删除时，需要检测该从帐号是否还被其他主帐号使用，如果还在被其他主帐号使用，那么就不能进行删除操作。进行主帐号删除时的类图如图 3-9 所示，其中 UserAction 类主要负责主帐号的查询和删除操作。ApplicationAccountAction 类主要是负责与主帐号相关联的从帐号的删除。

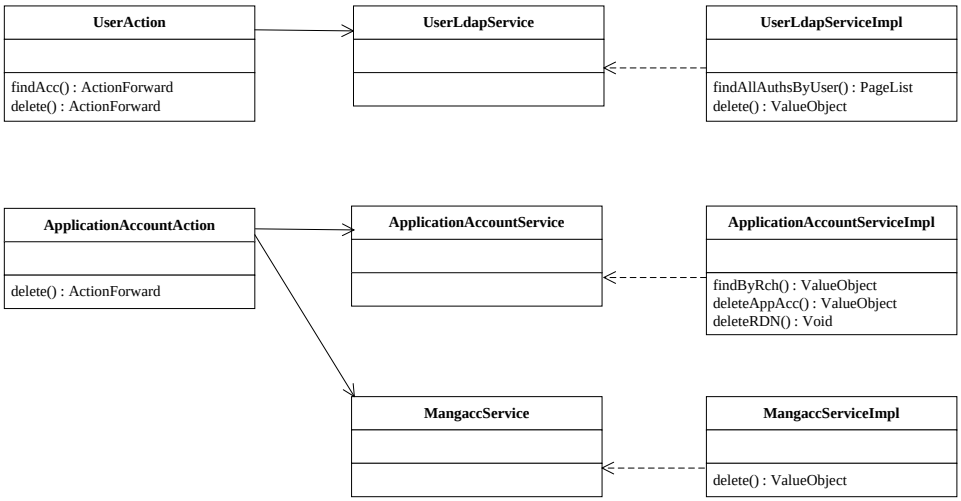


图 3-9 删除主帐号时类图

3.4.2 密码策略管理设计

在 4A 系统中，涉及到大量地密码验证工作，而且在不同的应用场景中，所涉及到的安全级别或者是加密的方式都会有不同的要求，因此会采用不同的密码策略。例如对于主帐号，系统会对其密码进行定期核查，在密码即将过期的时候，会对用户发送密码即将过期的消息，提示用户在近几天内对密码进行修改。

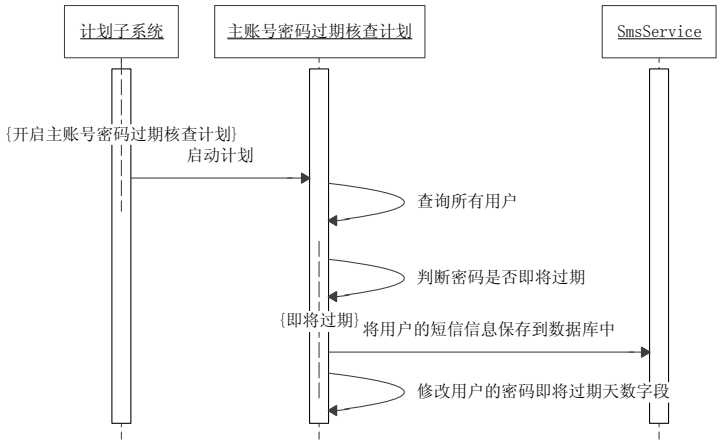


图 3-10 主帐号密码过期提醒

为了对系统中的密码策略进行说明，在这里本文以系统中一种最常使用的主帐号密码过期核查计划为例子进行阐述，该计划主要对系统中各帐号所涉及的密码过期策略进行服务。主帐号密码过期核查计划主要服务于 portal 用户登录时的密码过期验证和 portal 的主帐号密码过期提醒功能，通过系统定期的执行任务来检查主帐号的密码是否即将过期，如果即将过期会把用户密码即将过期的短信与用户 ID 和用户电话号码保存到数据库中，在系统设定的时间内通过短信向用户统一进行发送。该计划的执行的时序图如图 3-10 所示。

（1）当计划子系统启动的时候该计划自动启动。

（2）计划启动以后在每晚 12 点查询所有用户，先判断用户的密码即将过期天数字段字段是不是非空或者非 0，如果是非空或者非 0 就对用户进行检查，检查的时候先判断该用户是否绑定了密码策略，如果绑定了密码策略则根据密码策略的密码有效期和用户的密码修改时间进行判断密码是否即将过期。如果没有绑定密码策略则系统默认密码有限期为 90 天,如果用户的密码修改时间为空，则根据用户创建时间来进行判断。

（3）如果用户在 5 天后密码即将过期，则检查用户是否开启了密码过期提醒的服务,如果开启了则将用户的用户 ID，手机号码，短信信息保存到数据库中，每天早上 7 点给用户发送密码即将过期提醒短信。

（4）发送完短信后，将还有几天过期的天数保存在即将过期天数字段中。

在进行主帐号密码过期提醒时的类图如图 3-11 所示。在 UserPWDTimeCheckDao 类中有四个方法，其中 loadUsersConfig 方法返回的是当前系统中所有可用用户的集合，checkUserPWDTime 方法检查用户密码是否过期，getAllUserPWDPolicy 方法获取所有用户的密码策略，返回 Map 类型的值，其中 Key 为密码策略 ID，value 为密码策略的实体，modifyUser 方法用来修改用户信息。ShortMessage 类用来进行短信的提醒的发送。

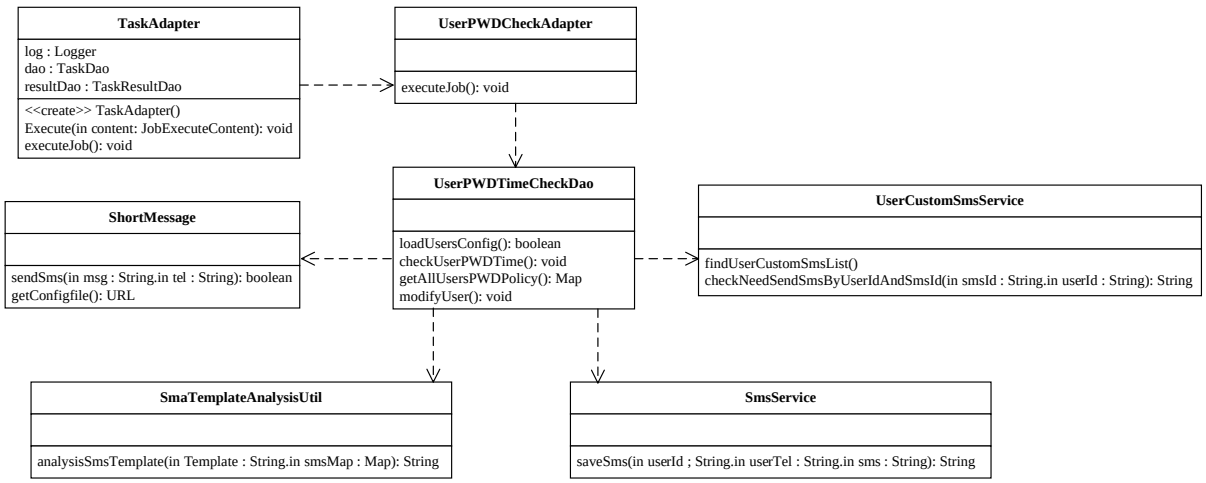


图 3-11 主帐号密码过期提醒类图

3.5 认证管理模块设计

3.5.1 认证策略管理设计

在安全管理系统中，为了保证系统的安全性，在不同的应用场景中，会存在着不同的认证策略。对认证策略的管理主要包括了对认证策略的新增、删除、修改和查找操作。根据不同的密码策略，会涉及到不同的认证策略。在进行认证策略的添加时，主要涉及到两个操作，第一个是检测添加的策略是否合法，例如名字是否跟已有的策略名重复，如果重复将不能进行添加。第二就是执行将数据插入到策略表中进行存储，更新数据库表。

3.5.2 单点登录管理设计

单点登录是指定用户登陆到 portal 页面后，可以在 portal 页面上看到，该用户被允许登录的相应应用系统，包括 C/S、B/S 系统，针对 B/S 架构的无法共用证书的应用系统引入 HttpClient，采用分步认证方法来实现单点登录，C/S 架构的应用系统可以加入代理登录中间件来进行代理登录[30]。每个系统对应一个或多个可登陆该系统的从帐号，用户可以选择以哪一个帐号来登陆该应用系统。

单点登录应用系统类图如图 3-12 所示，系统中的代码结构主要涉及到两个类，分别是 AppFillAction 类和 AppFillServiceImpl 类。针对不同的登录情形，其有不同的登录方法。

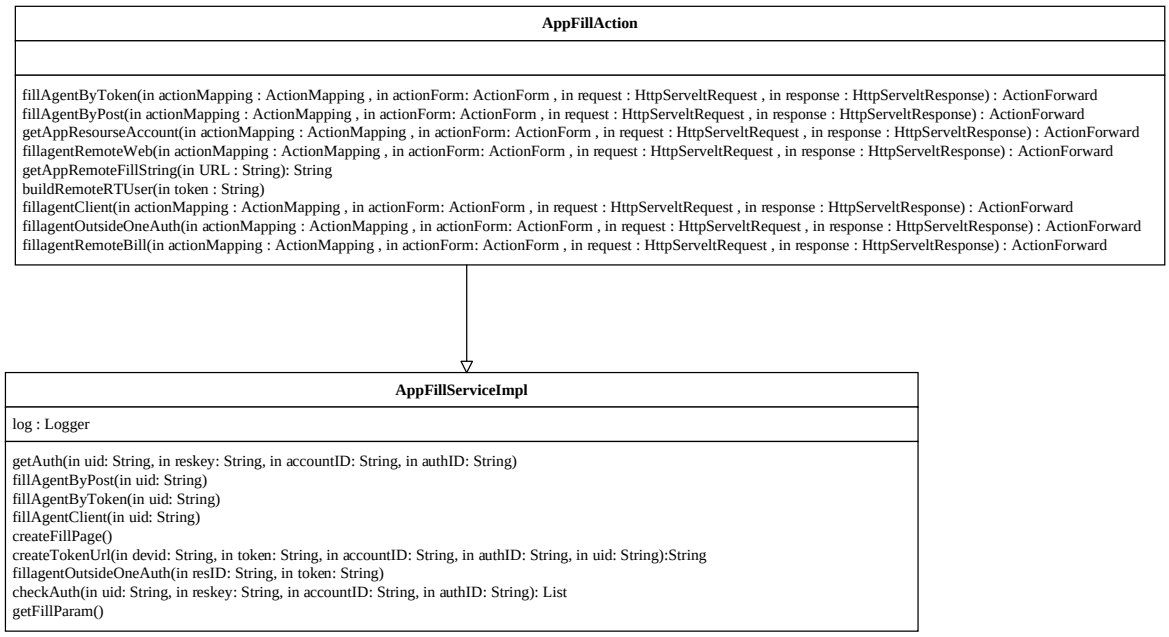


图 3-12 单点登录应用系统类图

代码的时序图如图 3-13 所示，其体现了在三种不同场景下，系统中代码的调用执行情况。首先，本地模拟代填调用 fillagentByPost()，对设备 ID、从帐号名称和当前用户查询授权，判断从帐号密码是否过期，获得代填结果 POJO，封装代填串，调用代填客户端，成功时返回登录成功，失败时返回详细信息。另外，应用系统票据登陆时，判断从帐号是否过期，获得代填结果，并向应用侧设置票据信息，获取客户端实例，将票据信息发送给代填组件，验证票据接口有效性，并返回结果。然后，CS 远程客户端代填时，判断从帐号是否过期，

获得代填结果，读取客户端信息。获取代填客户端实例，构建代填参数，拼装代填串，封装代填结果。调用代填组件进行代填，成功返回结果，失败时返回详细信息。

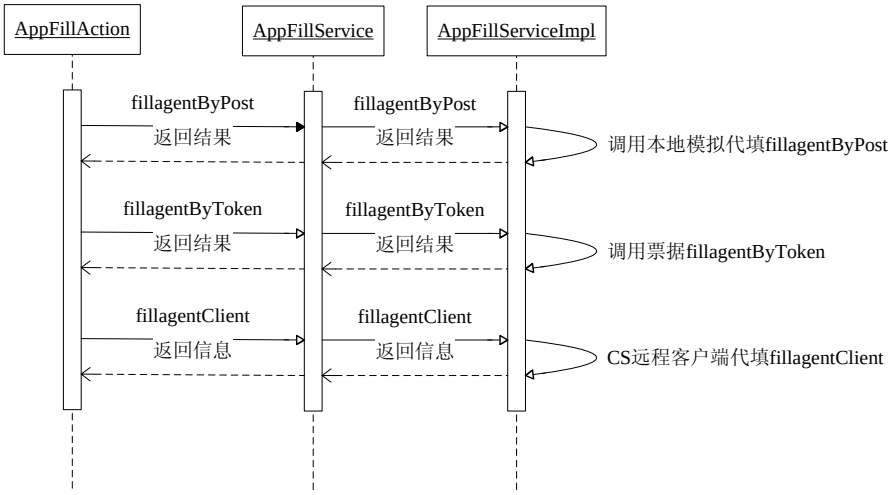


图 3-13 单点登录代码调用执行情况

在单点登录过程中进行探测时，分别对应用资源和系统资源进行可用性探测。对应用资源进行探测的时序图如图 3-14 所示，对系统资源进行探测的时序图如图 3-15 所示。

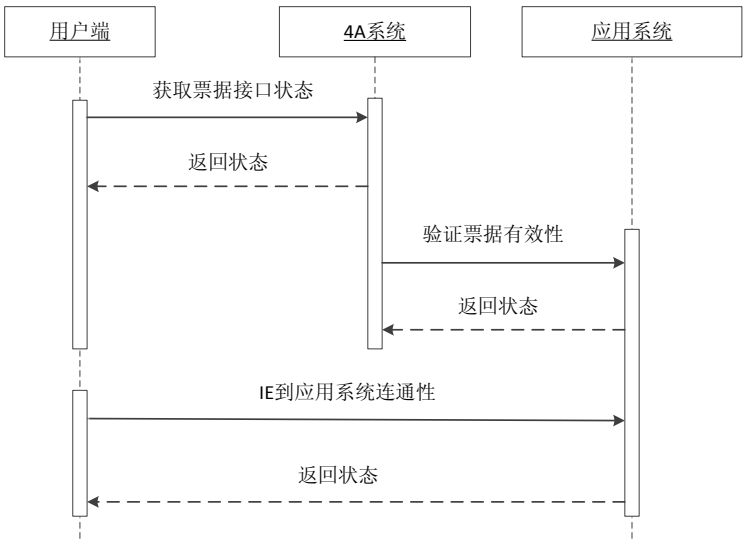


图 3-14 单点登录应用资源探测

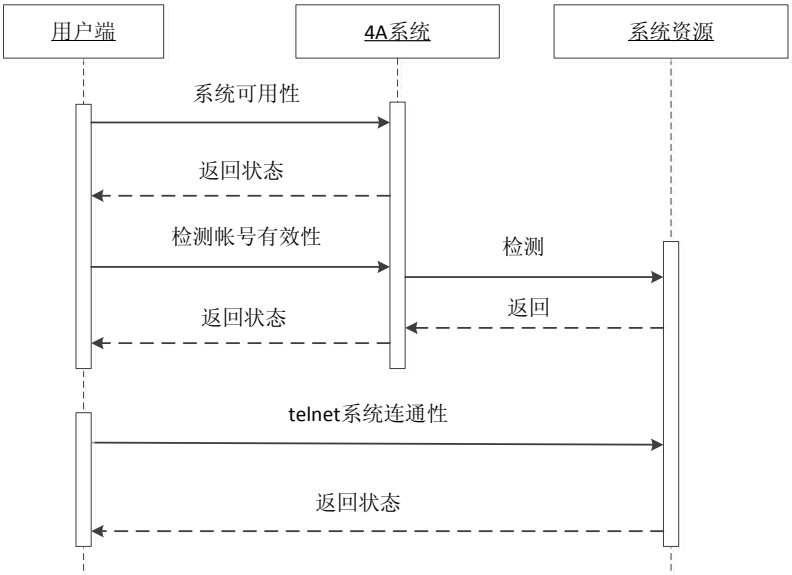


图 3-15 单点登录系统资源探测

3.6 授权管理模块设计

在系统授权管理功能中，角色定义为资源中若干访问权限的集合，包括功能角色和数据角色。在系统内角色和权限属于多对多的关系，角色可以拥有多个权限，而权限也可以被赋予多个角色，并且每个用户可以拥有不同的角色。不同的应用资源，由不同维度的权限集合进行表现，包括了角色、角色组、组织机构、用户组、岗位等。在 4A 管理系统上必须支持对角色的功能管理，包括角色的查询、创建、变更、删除和稽核等功能。

在对系统中的角色进行设置时，需要满足的要求是：角色名称在系统中不允许相同；一个角色至少拥有一个或以上的权限；当角色被赋予用户或者岗位时，不允许直接删除；系统内置两个角色，分别是普通用户角色、管理员角色。普通用户角色具有登录 PORTAL 权限，登录 PORTAL 权限是指用户可以通过应用系统与 Portal Server 通信，进而进行认证的权限[31]。管理员角色具有登录 PORTAL 权限和登录后台的管理权限；管理员只能管理其权限的范围内的角色。

3.6.1 角色和权限管理设计

角色是用户和资源之间的桥梁，可以实现用户和访问权限之间的逻辑分离，由此对角色的管理尤为重要。基于角色的访问控制模型(Role-based Access Control，RBAC)，以角色为中介，可以使用户和权限的变化互不影响，进而提高权限管理的效率[32]。在安全系统中设置的管理员角色分为以下几种，具体包括了系统管理员、管控系统管理员、主帐号管理员、审计管理员、接入资源管

理员等，每种管理员角色对应的系统管理权限如表 3-10 所示。

表 3-10 各角色所有权限表

管理员角色	权限
系统管理员	管理系统的超级管理员，拥有管理系统的所有权限
管控系统管理员	管控系统管理员负责授权管控系统一级主帐号管理员、一级审计管理员和一级接入资源管理员，以及对系统进行日常维护。
主帐号管理员	主帐号管理员负责在其授权范围内的主帐号生命周期管理以及各主帐号相关属性的管理，能够按照组织关系在其授权范围进一步创建并授权下一级的主帐号管理员。
审计管理员	审计管理员能够使用系统的审计管理功能模块，负责管理和审计管控系统自身日志以及接入资源产生的相关日志。
接入资源管理员	接入资源管理员负责管理接入管控系统的所有资源以及相关的功能模块，负责对普通用户进行授权使其能够访问接入资源。

管理主要是对资源中的功能权限和数据权限进行管理。规定了在系统中，哪些或者哪种类型的帐号能够进行操作的功能项或者能够访问到的数据范围。在对系统中的权限进行划分时，要确保系统的安全，以免有越权等操作的发生。在系统中，角色和权限的关系是关联在一起的，不管是什么级别的用户或者什么类型的帐号类型，都一定有其自己的权限，只是大和小、宽和窄的区别。

在本系统中，能够对角色的权限进行增、删、改、查等操作，能够对系统中的主帐号、从帐号授予权限，以及对应用资源、系统资源进行相应的权限管理。

3.6.2 委托授权管理设计

在委托授权管理中用户可以将自己的从帐号委托给其他用户，并可以规定该用户对从帐号的使用期限，到期后 4A 系统会帮助用户自动收回从帐号，用户也可以在使用期限到期前主动收回。在系统中主要进行的操作包括了增加委托授权、删除委托授权、修改委托授权以及查询委托授权操作。本功能涉及委托授权表、资源授权与委托关系两个表，数据库设计一节会给出两个表的具体设计。

在进行委托授权管理时需要注意的约束限制为：增加委托授权的操作时，一次只能设置一个主帐号，开始时间必须大于当前时间，一个委托人不能对同一个被委托人增加两个授权实体，而且要保证委托人与被委托人不能是同一个用户。删除委托授权时需要关联删除委托授权中设置的资源授权委托，对于系

统中的过期委托授权，也应该进行删除。修改委托授权时，不能修改被委托人名称，开始时间必须要大于当前时间。进行委托授权查询，能够显示用户所设置的委托授权基本信息，点击某个委托授权时，能够查看所配置的资源授权委托。

3.7 审计管理模块设计

审计管理可以简化的包括数据采集，数据处理，数据分析三个阶段的功能。数据采集就是对系统中所有的日志数据进行收集，将原始的日志数据导入数据库中，建立原始访问日志数据表[33]；数据处理对采集的日志数据按照对应的标准化策略进行标准化，然后按照规则对数据进行筛选匹配等操作[34]，得到中间数据；数据分析是根据处理后的数据，按照系统定好的相应策略，例如均值统计分析策略[35]等，对数据进行匹配分析，根据分析的结果来发现系统中的哪些操作存在着审计疑点。下面我们将分别来对这三个阶段进行阐述。

3.7.1 数据采集设计

安全审计数据采集主要是对主机、数据库、网络设备、应用系统等用户操作日志进行收集和存储。审计的采集范围包括了 4A 系统帐号、授权管理日志，4A 系统认证、登录日志，自管理日志，数据运营状态等。被管理资源的审计信息采集范围主要包括了应用资源的关键操作与敏感数据操作日志，操作系统、数据库的关键操作与敏感数据操作日志，网络及安全设备的关键操作日志等。

在表 3-11 中列出了对帐号管理、授权管理、认证管理以及与网络相关日志对数据采集的最低要求。在采集完成之后，能够在系统中进行日志查询操作。

在安全管理系统中包含了三种类型的采集引擎，分别是基于主机日志的采集引擎（HBA）、基于网络行为的采集引擎（NBA）、基于网关操作的采集引擎（GBA）三种类型。HBA 主要负责采集资源主机上产生的日志数据采集，并且对日志相关的人员信息、资源信息进行补全。NBA 对采集到的数据进行重组和分析，提取操作者（操作来源）、目标及其（设备、主机、应用）、操作途径、操作的命令内容即结果。最后反映的是具体什么人从什么地方对什么数据进行了操作。并通过关联和聚合审计下来的操作行为，得到更高级的安全事件。GBA 采集引擎是基于网关的操作审计，用户访问后台主机时先通过 GBA 主机，然后从 GBA 主机访问后台主机。

表3-11 数据采集最低要求

操作类型	操作子类	操作细项	采集对象	审计级别	采集时间
帐号管理	主帐号管理	主帐号创建	4A 系统	重要	准实时
		主帐号删除		重要	准实时
		主帐号修改		重要	准实时
		主帐号加/解锁		重要	准实时
		主帐号导入/导出		非常重要	准实时
		主帐号密码重置		重要	准实时
	从帐号管理	从帐号增加	主机、数据库、应用、4A 系统	重要	准实时
		从帐号删除	主机、数据库、应用、4A 系统	重要	准实时
		从帐号修改	主机、数据库、应用、4A 系统	重要	准实时
授权管理	主从帐号关系管理	主从帐号操作授权关系管理	4A 系统	非常重要	准实时
	主帐号角色或主帐号用户组管理	角色/用户组增加	4A 系统	一般	准实时或定时
		角色/用户组删除	4A 系统	一般	准实时或定时
		角色/用户组修改	4A 系统	一般	准实时或定时
	主帐号角色/权限关系管理	角色/权限关系管理	4A 系统	重要	准实时或定时
认证登录	帐号认证	认证成功	4A 系统	一般	准实时
		认证失败	4A 系统	一般	准实时
	单点登录	单点登录成功	4A 系统	一般	准实时
		单点登录失败	4A 系统	一般	准实时
关键操作	网络关键操作	系统网络参数变更	网络	一般	准实时或定时
		系统安全参数变更	主机	一般	准实时或定时

3.7.2 数据标准化设计

（1）日志合法性校验

数据合法性校验策略是用于验证原始数据内容是否合法的规则。采集到的日志不合法（即：不符合采集日志的格式标准、字段内容不符合相应的格式要求）将备案存储，供参考审核使用。例如：校验主帐号名称不能含有‘?’、‘*’、‘&’等特殊符号的策略。当不合法的判断方式主要是依据字段内容，涉及的字段包括：帐号、日期、源 IP、目的 IP。对采集到的不合法的日志即时发出预警。

（2）日志完整性检验

日志完整性校验策略是用于验证原始日志字段完整性的规则，支持对不同采集数据源的【主帐号、从帐号、资源名称、资源模块（应用资源）】等字段完整性检查策略配置。完整性校验策略对不同的审计资源（CRM、BOMC 等）配置不同的校验策略。

不完整的判断方式主要是依据字段的缺失情况，涉及的字段包括：主帐号/归属责任人主帐号、从帐号、日期、源 IP、目的 IP、操作内容。对采集到的不完整的日志即时发出预警。

（3）日志字段映射策略

日志字段映射策略是将原始日志解析提取的字段映射为标准化字段的规则。日志字段映射策略应支持对不同采集数据源的字段映射策略配置。日志字段映射策略支持对不同的审计资源（CRM、BOMC、BASS 等）的不同日志类型配置不同的映射策略。例如在某应用系统的日志映射如下如表 3-12 所示：

表 3-12 某应用系统日志映射举例

原始日志	映射规则	审计系统标准化字段
2015-01-13 00:02:47 smu_feam[2780] Info:[0413725] Receiving----Operator:hwhlr9820, SOCKETID: 592, IP: 135. 10. 26. 133, MML Command: MODLCK: ISDN="8615180803704",IC=FALSE,OC=FALSE;	(\d{4}\-\d{2}\-\d{2}\s*\d+\:\d+\:\d+)\s*(?:\S*)\s*(?:Info:)\s*(?:\S*)\s*(?:\S*)\s*\s*(?:\S*)\s*(\S*)\s*(?:Operator：)\s*(\S*)\,\s*(?:\S*)\s*(?:\d*)\,\s*(?:IP:)\s*(\d+\.\d+\.\d+\.\d+)\,\s*(?:MML\s*Command:)\s*(.*)	logtime,result,account,sip,operate

字段映射组件根据映射规则将上述原始日志映射为审计系统标准化字段。

（4）日志补全策略

日志补全策略是将原始日志映射后的字段按照 5W1H 模型[36]进行补全的规则。日志补全要求，如下表 3-13 所示：

表3-13 审计信息内容补全要求

分类	补全项
审计主体信息	自然人姓名、主帐号、从帐号、主帐号角色、主帐号类型、主帐号状态、从帐号类型、主帐号归属组织等
审计客体信息	归属的资源组、归属业务系统、IP 地址、资源类型（主机、数据库、网络设备、安全设备、应用系统）、资源责任人、资源名称等
审计动作信息	操作编号、日志来源、操作类型、操作子类、操作细项、审计级别（一般/重要/非常重要）等

3.7.3 日志数据分析设计

通过对采集的日志数据进行标准化之后，为了找出日志存在的审计疑点，需要按照审计策略对日志进行分析。在这里本文采用基于关键字分析和均值统计分析的审计策略以及基于用户行为模式的审计策略。

3.7.3.1 基于关键字和均值统计的审计分析

关键字分析时根据策略要素对标准化日志或者中间数据进行匹配和比较的过程，以发现异常和违规行为，并通过预警策略进行预警提示。关键字分析的过程图如图 3-16 所示。关键字可以从数据字典、审计字典里面进行获取。当然也可以通过对日志和策略进行分词处理后，对其中的关键字进行排序，选出一些新的但常用的词作为关键字。最简单的关键字策略包括了对日志数据中关键字短缺失的检查以及日志字段是否可以匹配。

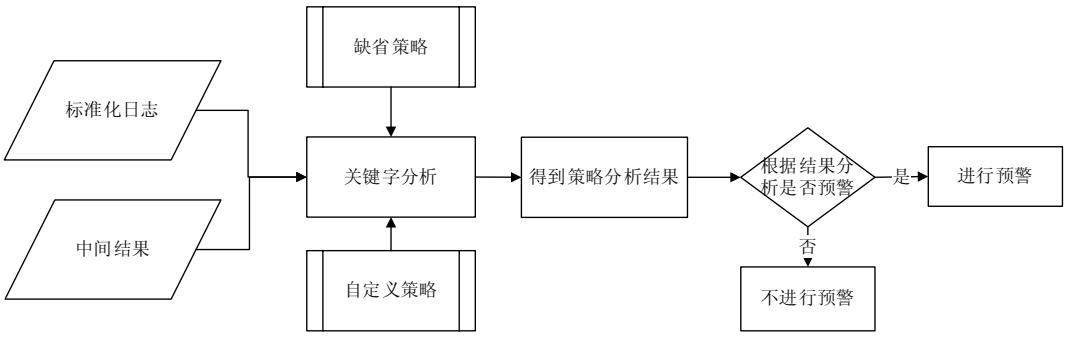


图 3-16 关键字分析过程图

在系统中，关键字分析策略就是在关键字策略的基础上加上 5 个 W(who、when、where、what、why)+how，这里的 how 就是关键字策略。加上 5 个 W 意味着在关键操作的基础上加上了操作的描述场景，当这样的操作场景出现时，

意味着这类的操作是用户最关心的事件。因此关键字分析策略是基于关键字策略进行的。下面举例说明审计分析中的关键字如表 3-14 所示。

表 3-14 审计分析关键字表

5W1H 对象	关键字分类方法	举例
Who	按主帐号角色	（非）帐号管理员、系统管理员、应用管理员、营业员、客服坐席、渠道、大客户经理、其它...
	按从帐号类别	（非）系统帐号、管理帐号、普通帐号、程序帐号、未知帐号、孤立帐号...
When	按时间周期	日、周、(非)工作时间段、按小时段...
	按是否工作日	工作日、节假日...
Where	按 IP 网段	（非）运维网段、互联网段、VPN 网段、办公网段、市场部所在网段、其他特定 IP 地址段...
	按地域	（非）XX 城市、XX 区、XX 县...
How	按操作类型	帐号管理、授权管理、认证登录、敏感数据操作...
	按照操作子类	角色用户组管理、从帐号/角色(用户组)关系管理 角色/权限关系管理、从帐号/权限关系管理
What	按被操作的应用资源类型	经营分析系统、运营管理系统...
	按被操作的系统资源类型	XX 主机、XX 数据库、XX 网络设备...
Why	按是否有凭据	有凭据(公文、工单、介绍信等)、无凭据...

统计分析策略是根据用户所关心的操作场景，在此基础上设定该场景事件或者多个场景事件发生的频次，设定改统计分析策略的阈值。在不同的事件类型上，设定的阈值也会不一样，常用的阈值计算规则是均值计算方法，基于标准化日志进行统计，计算出相应的均值，作为阀值数据供报表和上层统计分析策略使用。进行均值统计分析的时序图如图 3-17 所示。

关联分析基于 5W1H 模型中的属性、自定义的模型元素和异构事件进行分析规则配置，通过组合判断多个异构事件判断操作行为性质，发掘隐藏的相关性，发现可能存在的违规行为。关联分析关注审计客体和审计动作，以 What 和 How 为主要关联对象，发现审计主体存在的异常、违规行为。在系统内进行关联分析的序列图如图 3-18 所示，在该过程中主要涉及到的操作序列为：

（1） 分析线程从数据源获取待分析的日志数据

（2） 根据日志数据类型，从策略库中获取与之相匹配的策略类型。

（3） 根据策略，对数据进行关联分析，并将分析结果存入数据库中。

（4） 根据告警配置与分析结果比较，若超出了设定阈值，输出告警信息。

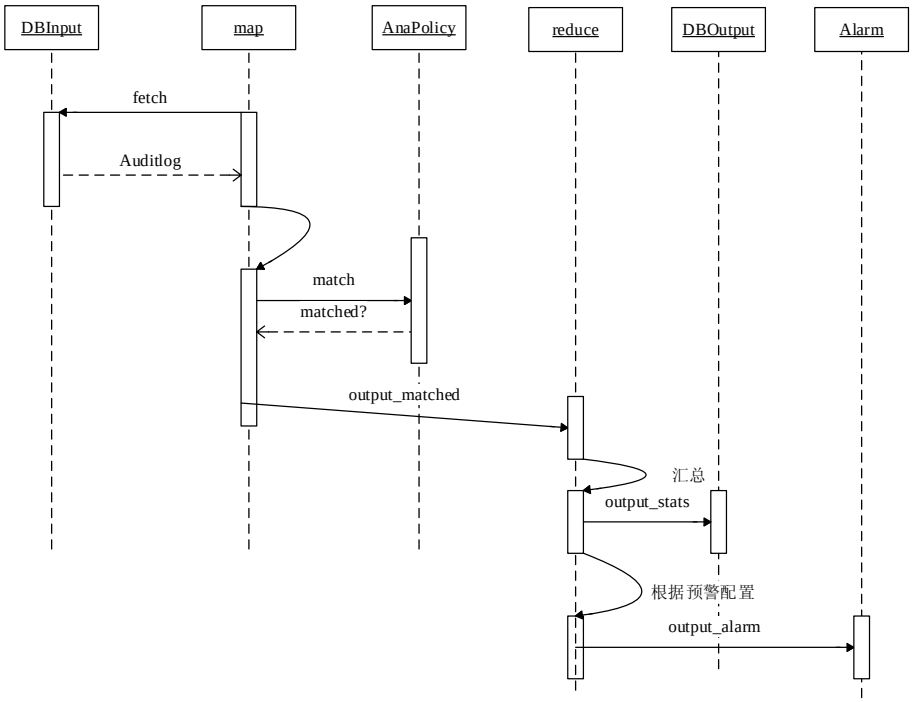


图 3-17 均值统计分析序列图

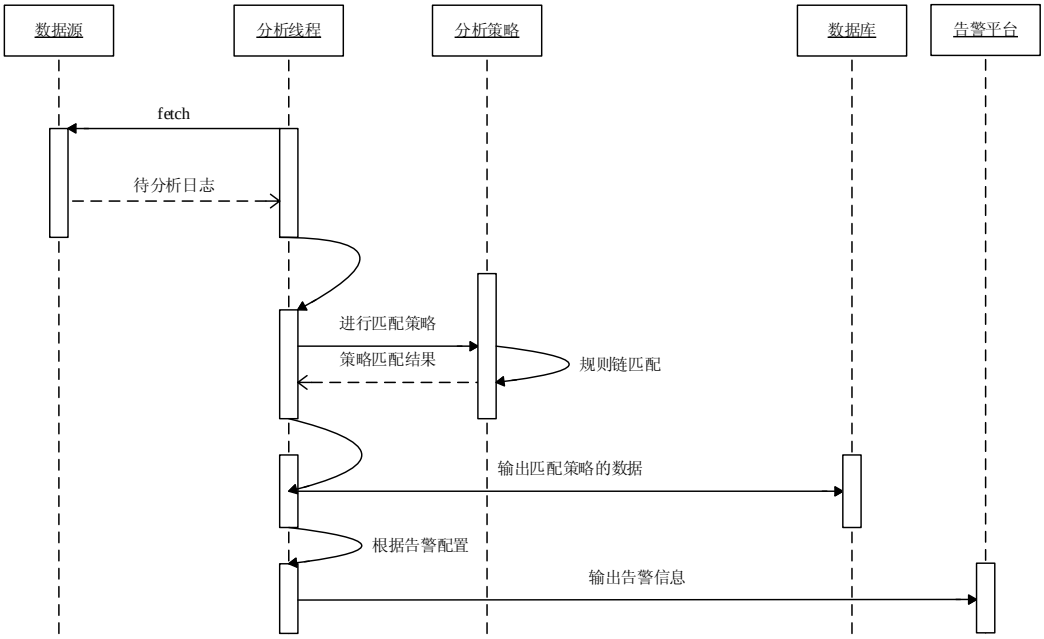


图 3-18 关联分析序列图

3.7.3.2 基于用户行为模式的审计分析

为了实时监测用户的行为并对其异常行为（异于整体用户的日常正常行为或者异于用户自身日常正常行为的行为）进行及时的警报，本小节将对用户的日常行为进行归纳并得出其正常行为模式，然后根据该行为模式发现其异常行为并警报。

主要是根据用户日常操作的网域/IP 段活动范围以及操作的业务深度，即访问的业务 URL 的维度和频度来归纳用户的日常行为模式[37]，从业务的角度进行总结出每个用户的日常行为规则，从而对用户的操作进行安全性分析和判断。分析原理如图 3-19 所示。其中，通过马尔可夫链来刻画用户的行为模式，因为应用系统用户业务轨迹和操作行为之间相互影响，符合马尔可夫模型的映射隐含关系[38]。为了描述用户业务轨迹和操作行为，本文采用用户时序的目的 IP 地址和操作命令两个属性进行描述。生成马尔可夫链即用户行为模式的具体步骤是，针对某用户，先对该用户经过简单安全规则识别的安全行为日志按照不同<目的 IP 地址，操作命令>二元组进行日志数量的统计；然后根据时间上的前后关系，统计从某源<目的 IP 地址，操作命令>二元组到某目的<目的 IP 地址，操作命令>二元组的日志数量，用该数量除以该源<目的 IP 地址，操作命令>二元组上所有日志数量即该路径上的转移概率；对每一对可能的二元组对进行上述转移概率的计算，最后形成该用户的马尔可夫链，也就是该用户的行为模式。针对所有用户，也按照上述步骤生成整体用户的马尔可夫链，即整体用户的行为模式。

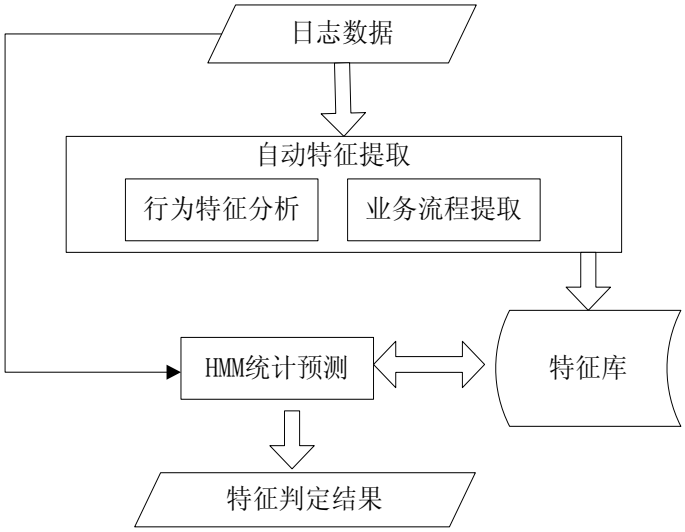


图 3-19 基于用户行为模式的审计分析原理图

举个例子，生成的马尔可夫链如图 3-20 所示。马尔科夫链中的每个状态都是<目的 IP 地址，操作命令>二元组，状态间的转移概率即对应二元组对之间的转移概率，$P_{i,j}$ 是从<目的 IP 地址 i，操作命令 i>二元组到<目的 IP 地址 j，操作命令 j>二元组的转移概率。

对于某用户的某次登录，为了识别用户此次的行为是否异常，也就是是否不符合整体用户行为模式或是不符合用户自身独有的行为模式。在识别用户行为是否异常前，需要进行前期的处理：采集此次登录用户生成的操作日志并进行标准化，在经过简单安全规则识别之后，对用户此次所有操作按照时间顺序生成<目的 IP 地址，操作命令>格式的行为序列。

为判断用户行为是否异常，首先，要判断用户行为是否符合整体用户行为模式。根据统计学规律大多数用户是符合整体用户行为模式的，只有少数人的行为模式是相对独特的，本文假设针对某用户的某行为序列，整体用户执行该行为序列的概率符合正态分布 $N(\mu,\sigma^2)$，均值 μ 是用整体用户马尔可夫链计算的行为转移概率，方差 σ^2 是这样估计的：找出有上述行为序列的十位用户，按其各自的马尔可夫链计算转移概率，这些转移概率的方差即是正态分布方差。当该用户用自身马尔科夫链计算出的转移概率远离均值，脱离 99%的置信区间（μ-3σ，μ+3σ）时，本文认为用户的行为偏离了整体用户的行为模式需要对其进行警报。

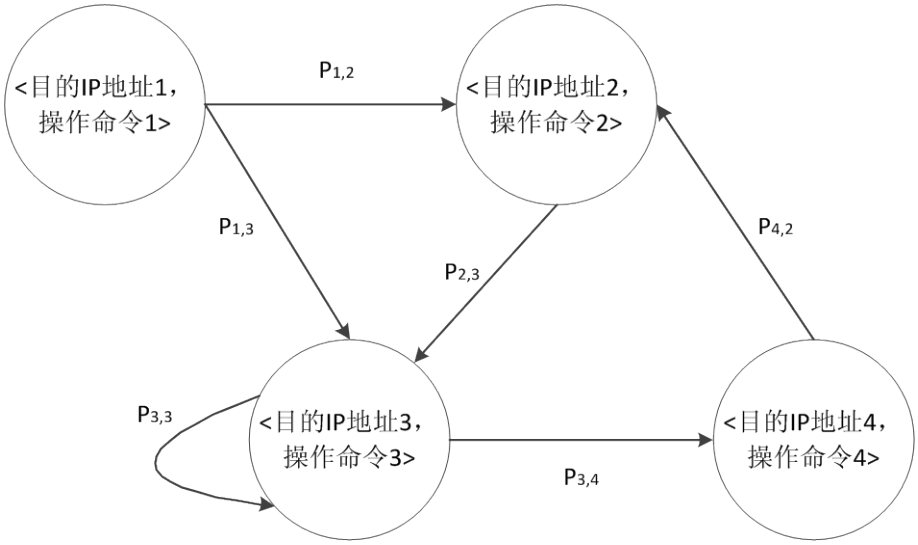


图 3-20 用户马尔可夫链举例

其次，判断用户的行为是否不符合用户自身独有的行为模式，如果用户做了很多以前很少进行的操作，那么可以认为用户的行为是异常的。本文规定如

果某用户执行了多次在其马尔可夫链中转移概率排在后 20%的操作，执行的次数占本次行为的操作总次数的 50%以上，则认为用户行为是否不符合其以往的行为模式，需要进行警报。

3.8 本章小结

本章介绍了安全管理系统的系统功能架构，完成了详细的数据库设计，还主要对安全管理系统中的各功能模块进行了详细的设计，包括对各功能点的详细描述，明确了各功能点的操作过程，为后续的功能实现部分做了充分的准备。

第4章 安全管理系统实现

根据系统设计的结果，对安全管理系统中的功能进行编码实现。本章对各功能模块中的重要部分进行实现效果展示。

4.1 统一门户模块的实现

经过页面设计和编码实现，登录系统后，统一门户界面如图 4-1 所示，图中各区域展示信息包括：

图 4-1 统一门户界面

（1）系统的名称以及中国移动的 LOGO，表明该系统归移动所有。

（2）系统中常用的业务菜单，包括了资源管理、个人中心、管理中心、审计门户等。

（3）登录信息：显示用户登录名，以及系统当前的登录人数和上次登录时间等信息。

（4）系统公告主要显示系统中的通知、公告等消息。

（5）信息小贴士中主要包括了密码过期、个人积分等信息。用户可以对自己所关心的信息进行添加。

（6）常用资源中展示了用户经常使用的一些系统资源，方便用户进行操作和迅速访问，提供了用户自己添加内容的功能。

4.2 帐号管理模块实现

4.2.1 帐号管理实现

在帐号管理模块中，本文主要通过主帐号的属性管理，从帐号的自服务管

理，以及在删除主帐号时删除从帐号为例子来表明该模块的实现情况。主帐号属性管理包括对属性的查询，增加，修改和删除等操作。下面以对主属性的删除为例对帐号属性管理在系统上的实现情况进行阐述。

在系统内进行属性添加的流程图如图 4-2 所示。在实现过程中，将添加的属性与数据库中已有的属性进行比对，如果发现该属性已经存在，那么将返回添加页面，并且给出提示添加失败的原因。

在系统内进行属性删除的流程图如图 4-3 所示。在实现过程中，除了实现参数的传递，还需要对该属性的使用情况进行判断，只能删除那些没有被使用的属性。

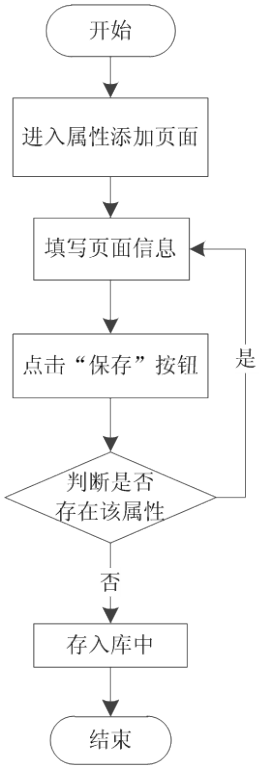


图 4-2 增加属性流程

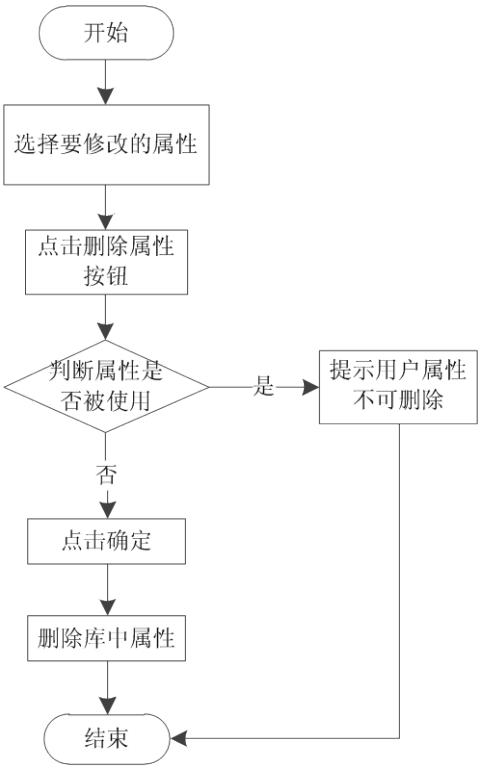
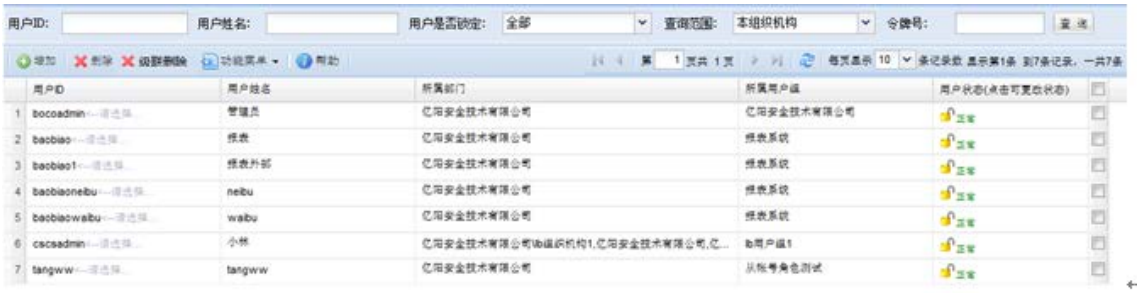


图 4-3 删除属性流程



4-4 主帐号查询选择界面

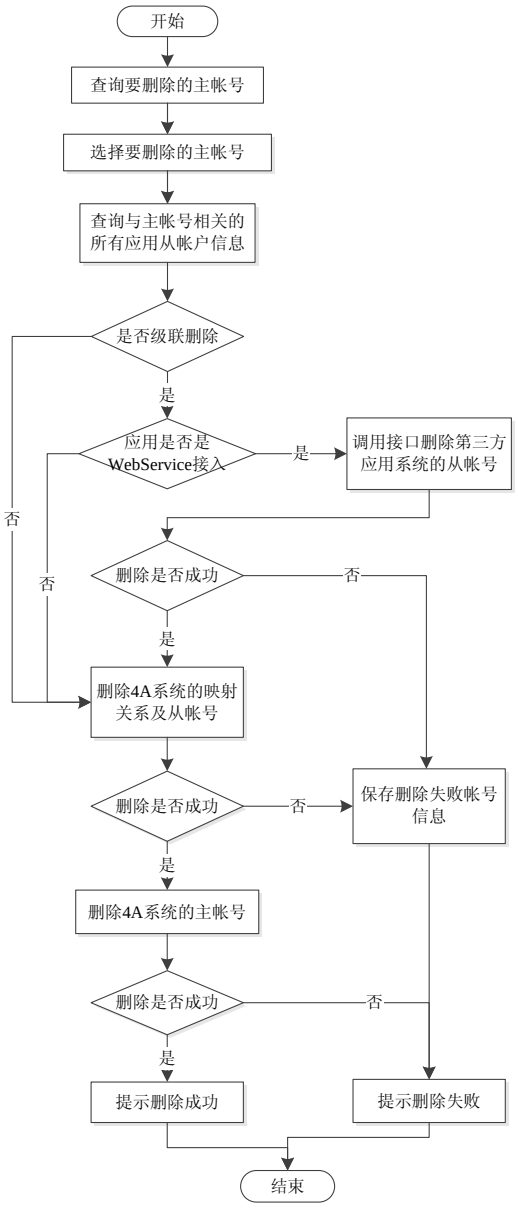


图 4-5 主帐号删除流程图

4A 系统主帐号需要删除时，若此主帐号关联相应的应用系统从帐号，系统中删除此主帐号的映射授权关系和从帐号。主帐号的查询界面如图 4-4 所示。能够实现对主帐号的查询功能，可以根据多个条件进行组合查询，能够实现批量删除操作。其操作流程如下：

（1）选择需要删除的主帐号，可以多选。

（2）选择级联删除时会删除应用系统从帐号及授权关系。

（3）点击删除主帐号后，选择需要删除的关联的应用从帐号。

（4）选择需要删除的应用从帐号。

（5）查询从帐号列表时，需要屏蔽一个从帐号对应多个主帐号的数据，但是在处理时，会默认解除授权关系。

（6）删除从帐号时，需要验证是否需要调用接口删除第三方应用帐号。

在系统内进行主帐号删除的实现流程图如图 4-5 所示。

在进行主帐号删除时，主要涉及到主帐号的查询，根据主帐号查询与其相关的从帐号信息，然后根据是否级联删除，如果选择是，在确定应用有没有接入 WebService 后，调用接口删除第三方应用系统从帐号，如果选择否，那么删除 4A 系统的映射关系以及帐号。在进行删除时，需要判断删除操作是否合法，如果不合法，操作失败后需要保存删除失败的帐号信息。

4.2.2 密码策略管理功能实现

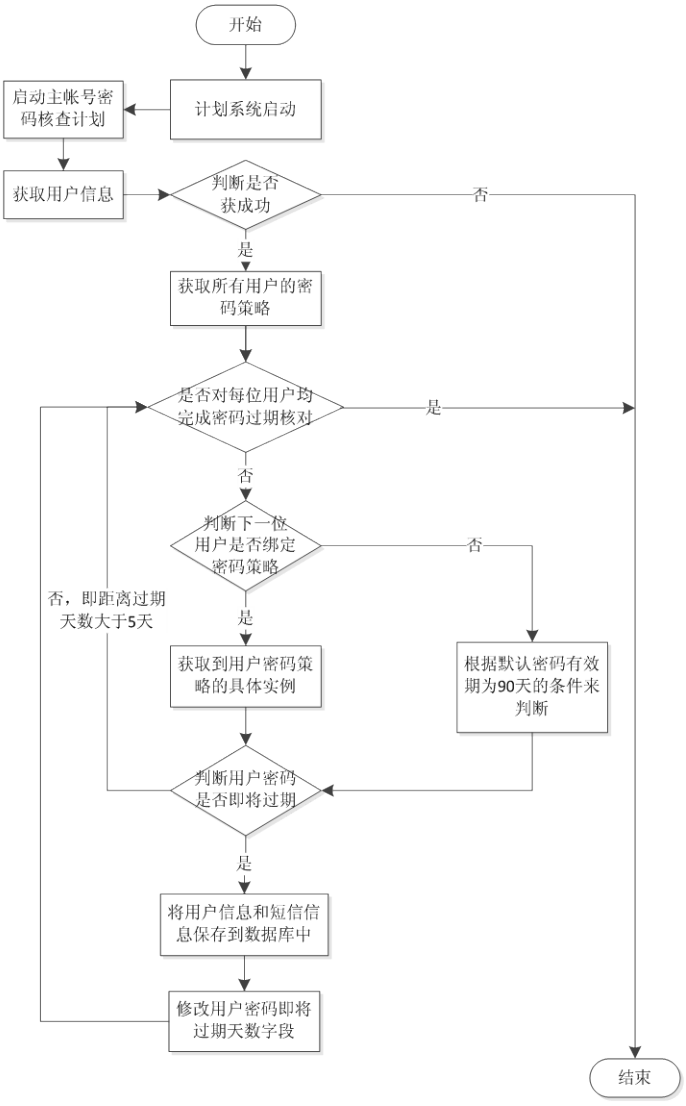


图 4-6 密码过期提醒实现流程

在密码策略管理中，为了防止密码过期情况的发生，最核心的部分是对密码过期情况进行检查，对密码信息及时更新。进行密码过期策提醒的流程图如图 4-6 所示。为了实现该功能，在系统实现的过程中使用的函数方法名以及相应的函数功能如下：

（1） loadUsersConfig 函数：该方法返回当前系统中所可用用户的集合。

（2） checkUserPWDTime 函数：该方法检查用户密码是否即将过期。

（3） getAllUsersPWDPolicy 函数：获取所有用户的密码策略。

（4） modifyUser 函数：对数据库中帐号密码即将过期天数段进行修改。

在密码过期提醒功能实现过程中，根据帐号的密码策略来对密码过期情况进行检查，获取密码还有多长时间过期，并对数据库中的用户密码即将过期天数进行修改，当即将过期天数小于等于 5 天时通过发短信的方式提醒用户修改密码。

4.3 认证管理模块实现

4.3.1 认证策略管理实现

认证策略管理主要是对安全系统中的认证策略进行增、删、改、查操作。在图 4-7 展示了对认证策略进行添加的页面，要注意的是在填写认证策略名称时不能与已有策略同名。

图 4-7 增加认证策略

4.3.2 单点登录可用性探测实现

单点登录可用性探测主要包括应用资源连通性检测和系统资源连通性检测，单点登录应用资源的的流程如图 4-8 所示。

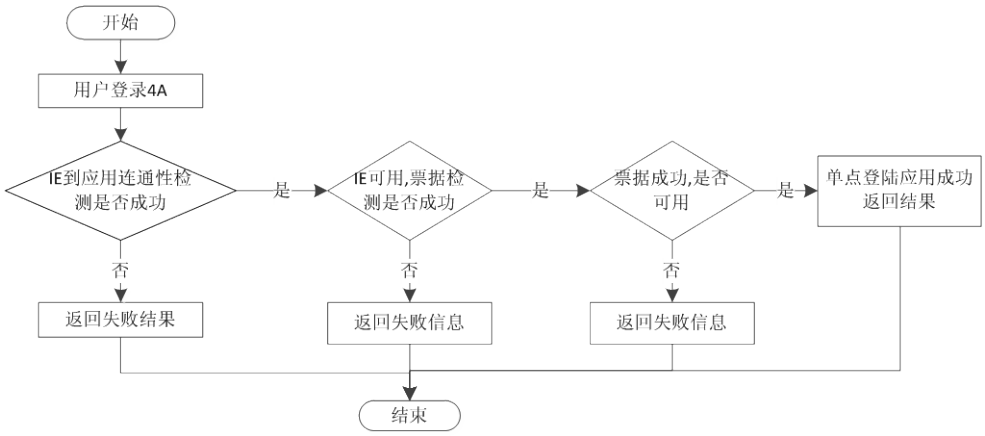


图 4-8 单点登录应用资源流程图

该过程可描述为：

（1）用户登陆 4A 点击应用系统检测按钮。

（2）通过 ie 访问应用资源，并返回结果。

（3）IE 到系统资源连通性检测成功时进行票据检测，如果连通性检测失败返回失败原因。

（4）票据检测成功后进行应用单点登陆操作，并返回相应信息。

单点登录系统资源的流程图如图 4-9 所示。

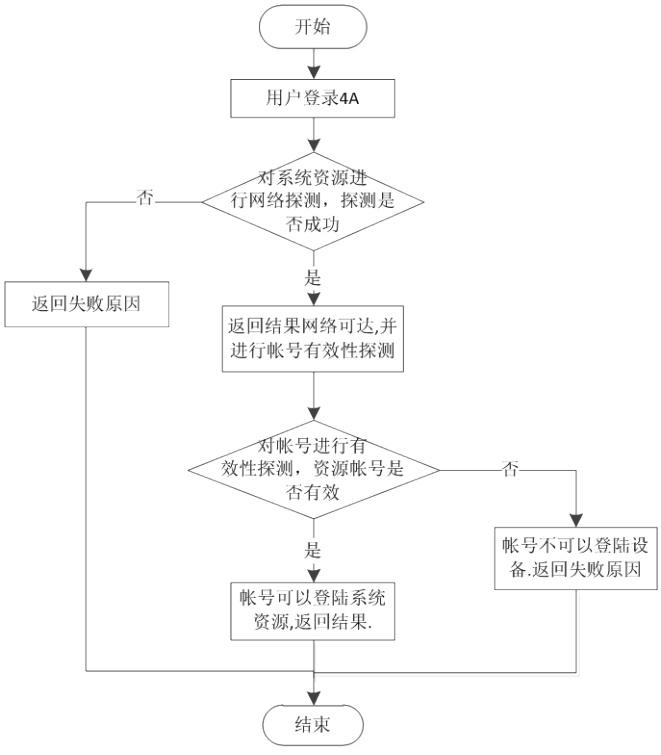


图 4-9 单点登录系统资源流程图

实现该过程的流程描述为：

（1）用户登陆 4A，点击系统资源检测按钮，首先对网络进行检测。

（2）如果网络可达进行帐号有效性检测，否则返回失败原因。

（3）帐号有效性检测，如果帐号可以登陆设备，返回成功信息，否则返回失败原因。

4.4 授权管理模块实现

4.4.1 角色和权限管理实现

实现根据条件查询从帐号和主帐号的关系，操作界面如图 4-10 所示，其中：

（1）点击后左侧显示“主帐号角色”、“从帐号角色”、“映射授权”

（2）点击“映射授权”菜单上的“＋”，下面展现出当前主帐号所管理的资源组树，右侧展现映射授权主界面

（3）如果左侧没有点击资源树，则右侧显示该主帐号管理资源范围内的所有授权信息。

（4）如果左侧点击了资源树，则右侧显示该资源组下所有设备的授权信息，同时，要将该资源组的名称显示在条件列表里。

（5）右侧查询表单内输入的信息要在下面的条件列表里展现，点击 x 可以删除该条件，并且在删除事件触发时，重新查询列表。

（6）当输入主帐号查询条件后，将部门输入清空，并 disabled 掉。

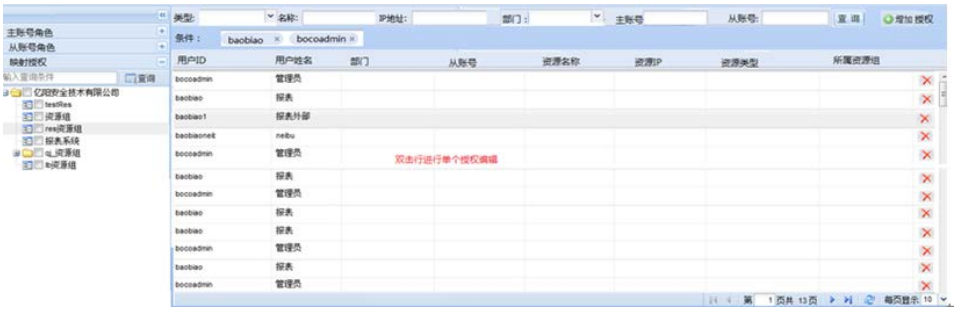


图 4-10 查询操作界面

进行映射授权查询的流程如图 4-11 所示。

在系统内进行映射授权的过程中，需要对多种情况进行判断，只有当符合查询的条件时，才能够进行查询。其中用到的判断条件首先是否输入资源名称、IP，如果没有再判断是否输入主帐号部门作为查询条件，最后判断是否输入主从帐号位查询条件。在不同的查询条件下，输出符合查询条件的结果。如果没有查询条件输入，不执行查询操作。

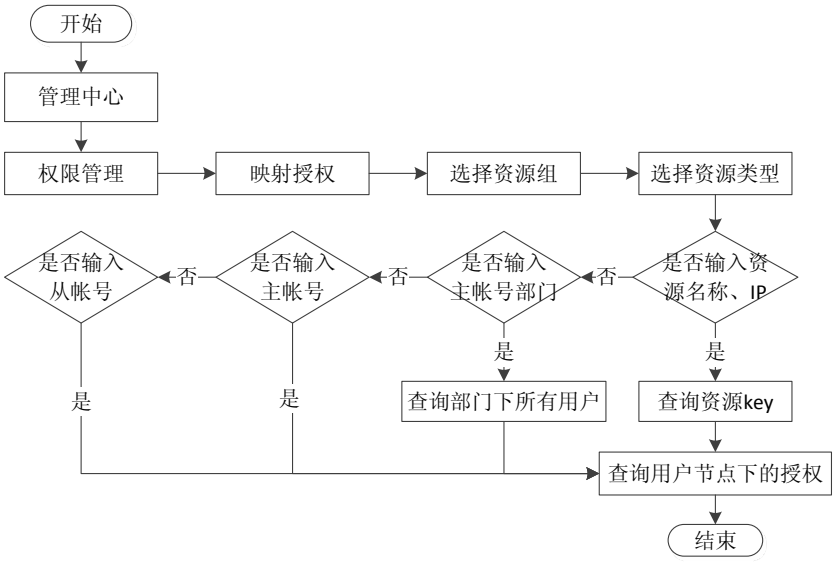


图 4-11 映射授权查询流程图

添加主帐号和从帐号之间的映射授权，旨在建立主帐号和从帐号之间的关联。在系统中进行操作的流程为：进入管理中心，选择权限管理中的映射管理，添加主、从帐号的映射关系，并添加授权，填写授权属性。

在系统上进行操作时，操作效果图所示。在图 4-12 中，选择或者输入要进行权限映射的主从帐号，在图 4-13 中进行权限选择并进入下一步，在图 4-14 中可以发现如授权成功，则执行结果为成功，失败要输出失败原因。

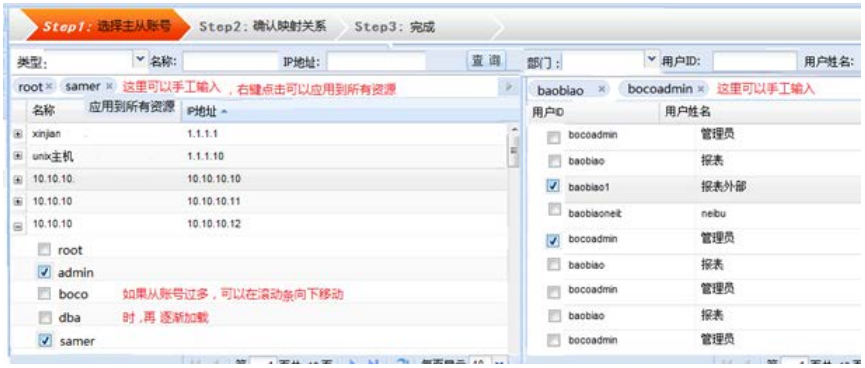


图 4-12 选择主从帐号

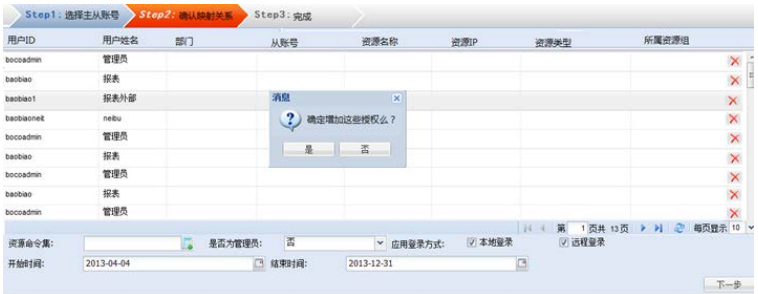


图 4-13 确认映射关系

图 4-14 授权结果图

4.4.2 委托授权管理实现

对系统内的委托授权进行管理时，增加委托授权的流程图如图 4-15 所示。在判断被委托人是否有效时，依据委托人与被委托不能为系统中同一用户，委托人不能对同一个被委托人增加多个委托授权实体为判断条件。

在系统内进行委托授权资源列表查询时查询流程图如图 4-16 所示，当委托人登录 portal 后，在资源管理界面，如果此用户有委托授权，则增加委托授权标签页，在委托授权标签页内，实现对委托资源的维护；根据委托人所委托的授权资源，展现资源列表（调用委托授权资源列表接口），在列表中需显示委托人主帐号信息；点击连接方式后，查询资源所委托的从帐号列表（调用委托授权资源从帐号查询接口），点击从帐号登录；在单点登录过程中需要传递委托人信息，客户端特殊参数处理需要使用此委托人信息；委托授权标签页暂不支持快速登录和设置常用登录方式，从帐号密码自学习；委托授权标签页，可根据资源 IP，资源类型等常用搜索条件，可不含有资源组搜索条件。

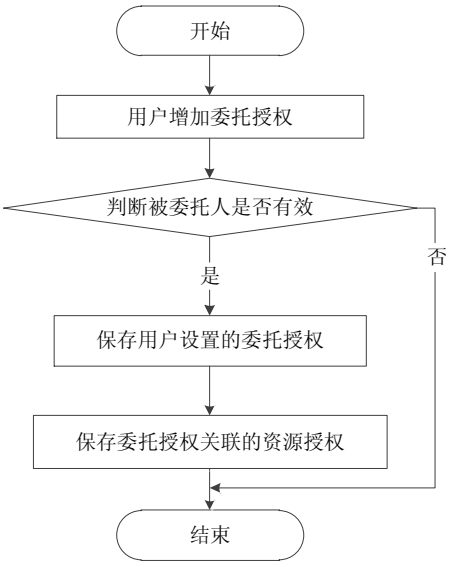


图 4-15 增加委托授权流程

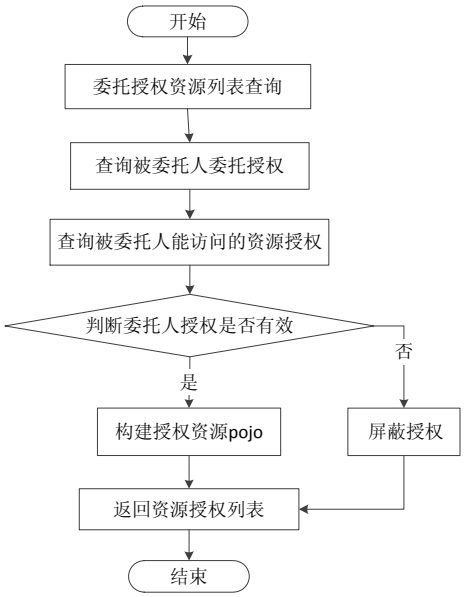


图 4-16 委托授权资源列表查询流程

执行该过程中的限制和约束条件有：（1）在进行委托授权当被委托人登录时，查询被委托人是否拥有委托授权，如果有委托授权，则显示委托授权资源标签页；（2）如果没有委托授权，则不能显示委托授权资源标签页；被委托人可以被多个委托人所委托授权，需要列表中显示委托人名称，端口和常用 资源不显示；（3）系统需要根据委托授权中资源信息，核查委托人的主帐号的授权资源是否有效（一对一授权，从帐号角色授权），只能显示能授权有效的资源；相同的资源需要合并，并按照要求设置必要的属性；（4）对于委托时效过期的委托授权，不能显示委托授权资源。

4.5 审计管理模块关键技术实现

4.5.1 审计策略中心实现

在审计管理模块中，审计策略中心是整个模块的核心。主要包括策略创建、策略的修改、策略删除、策略查询等功能。策略管理范围包括标准化类策略、中间处理类策略和业务分析类策略。策略中心的实现图如图 4-17 所示。

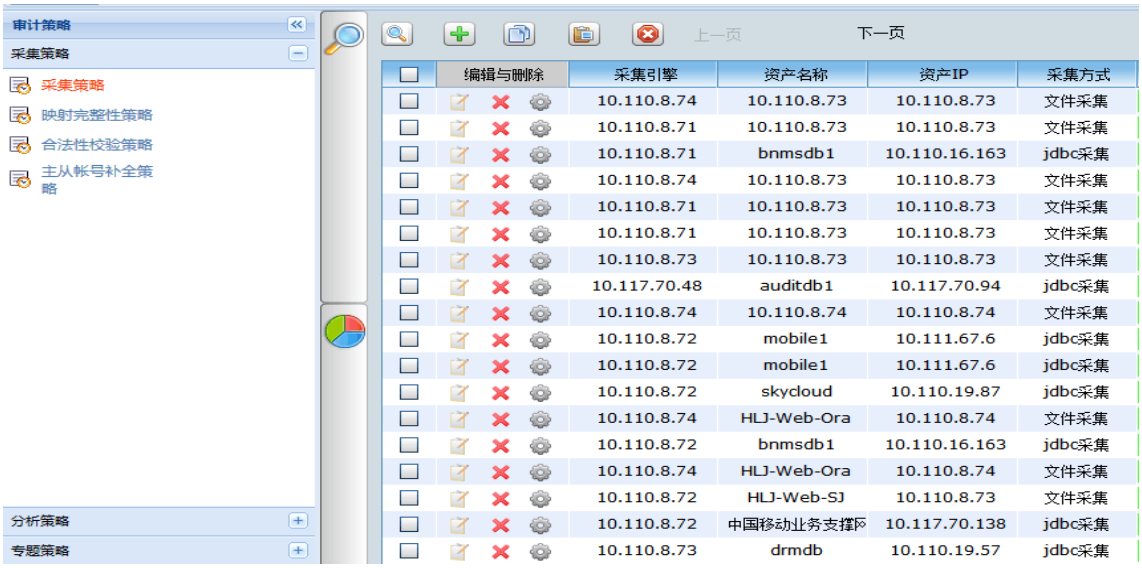


图 4-17 审计策略中心界面

在系统内策略中心页面内操作的流程图如图 4-18 所示，用户登录后通过管理页面进入策略中心，选择要做的操作进行操作。需要下发策略就进入策略下发模块的页面；需要进行内容的编辑就进入相应的策略查看页，通过策略查看页上的功能按钮完成相应的操作，操作完成后退出登录。

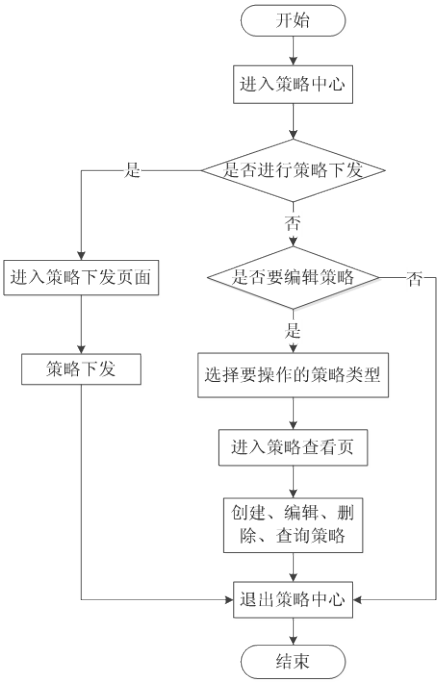


图4-18 策略中心操作的流程图

4.5.2 基于关键字和均值统计的审计分析实现

在关联分析的审计实现里面，涵盖了关键字分析、统计分析。进行关联分析时，可以对关键字与关键字、关键字与统计、统计与关键字、统计与统计四中关联关系进行分析。

其中，关键字分析实现，主要是构建审计关键字词典，然后根据关键字与日志内容进行匹配。

统计分析是对历史的数据进行统计分析，计算出策略的均值。其实现流程图如图 4-19 所示。首先是从审计策略管理中心获取审计策略，然后从日志数据里面选取表，对表里面的每条日志记录进行分析，由于日志数据量较大，因此为了提高分析数据分析的速度，采用了多线程的方式对日志数据进行分析，最后将分析的结果进行汇总，并且将均值存入到均值分析策略表中，为后续的分析做准备。

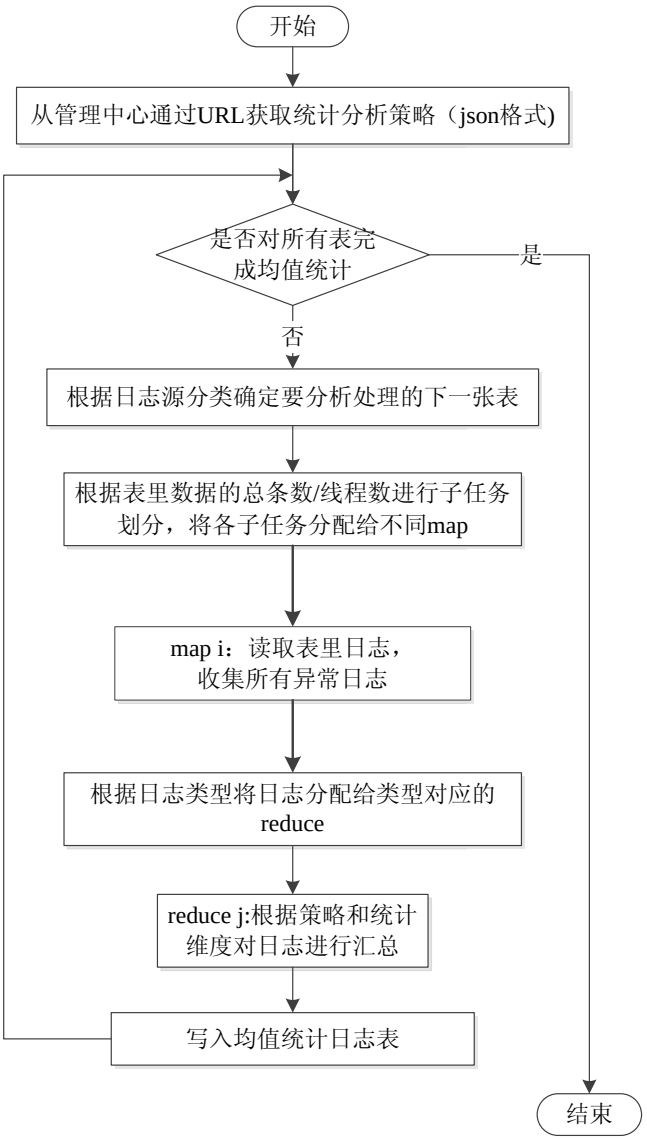


图 4-19 均值计算流程图

关联分析是从多个方面来对日志进行分析，对多个异构事件进行组合。在系统中，关联分析分为前台服务和后台服务。前台主要是对关联分析的策略进行管理，包括对关联分析的增加、修改和删除。后台主要是根据前台制定的策略对日志数据进行分析。后台的实现流程图如图 4-20 所示，使用的编程语言为 JAVA。该过程中，最主要操作是通过日志数据与关联分析策略库中的每条策略进行匹配，来发现与该条日志数据相关的审计策略，最后将结果写入关联分析结果表，并通过结果进行分析判断是否存在审计疑点或者违规操作。

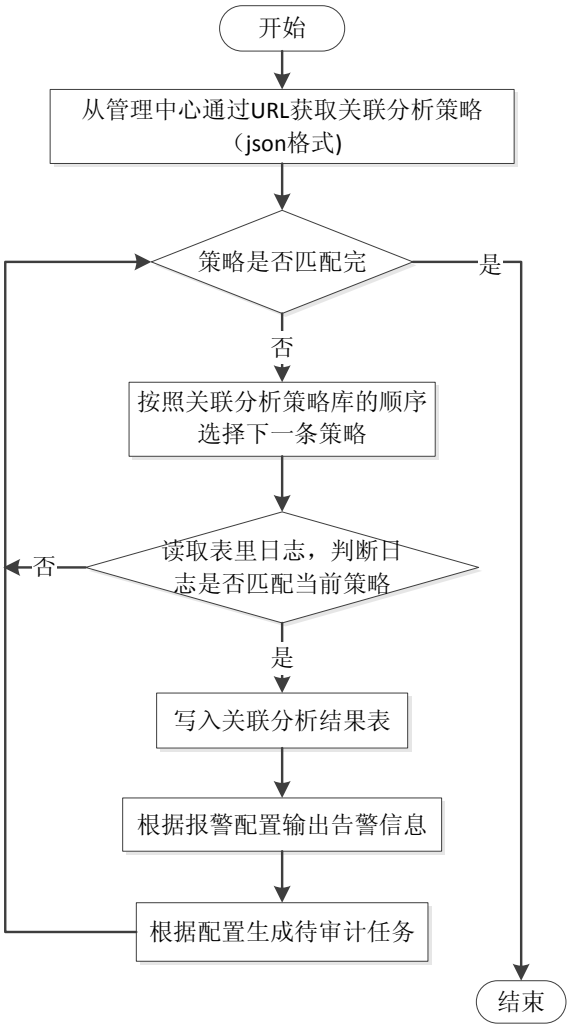


图 4-20 关联分析流程图

4.5.3 基于用户行为模式的审计分析实现

由于应用系统用户业务轨迹和操作行为之间相互影响，符合马尔可夫模型的映射隐含关系，所以通过马尔可夫链来刻画用户的行为模式。为了描述用户业务轨迹和操作行为，本文采用用户时序的目的 IP 地址和操作命令两个属性进行描述。

基于用户行为模式的审计分析的具体流程如图 4-21 所示。为判断用户行为是否异常，首先，要判断用户行为是否符合整体用户行为模式。当该用户用自身马尔科夫链计算出的转移概率远离正态分布均值，脱离 99%的置信区间时，本文认为用户的行为偏离了整体用户的行为模式需要对其进行警报。其次，判断用户的行为是否不符合用户自身独有的行为模式，如果用户执行的其马尔可夫链中转移概率排在后 20%的操作的数目占本次行为的操作总次数的

50%以上，则认为用户行为是否不符合其以往的行为模式，需要进行警报。

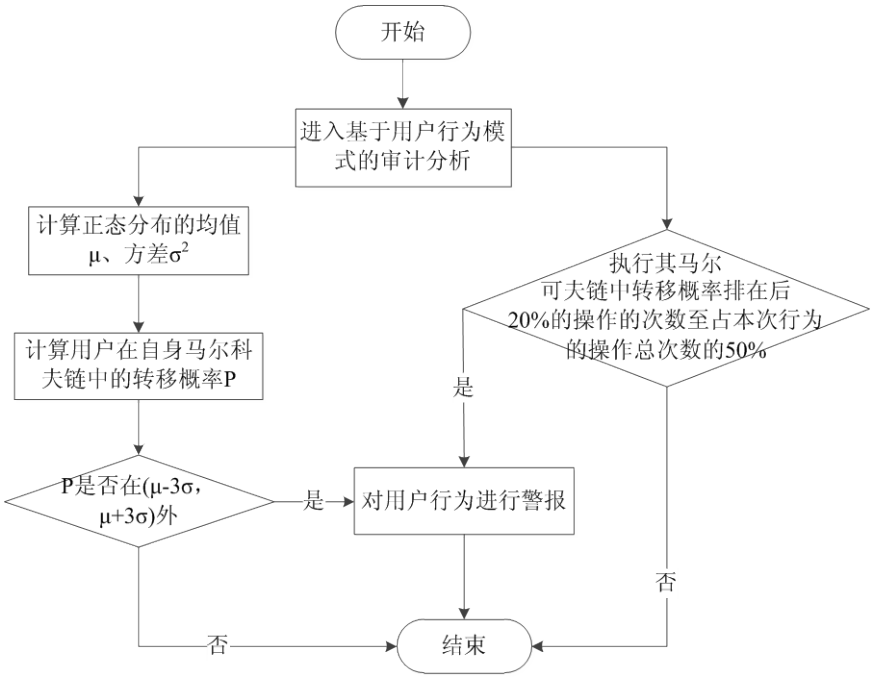


图 4-21 基于用户行为模式的审计分析流程图

在 4A 系统的真实审计日志中，随机抽取了 2017 年 1 月到 4 月期间的系统内部用户操作日志数据，对这些用户进行该段时间内的用户行为模式分析，检测出的异常行为的可视化结果如图 4-22 所示。

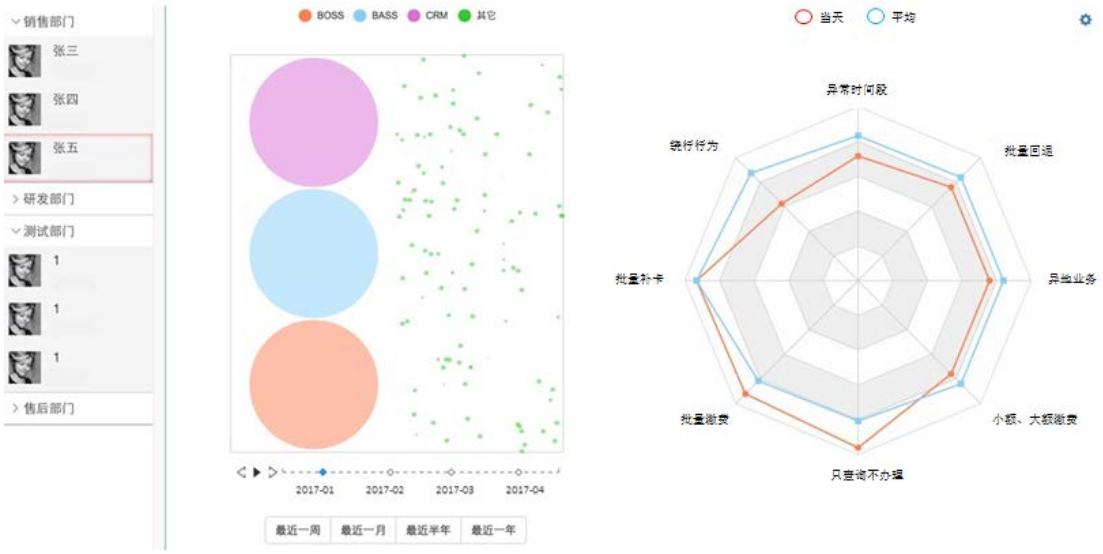


图 4-22 2017 年 1 月到 4 月用户异常行为的可视化结果

4.6 本章小结

在本章中，主要是以系统中部分功能的实现情况为例对系统的实现情况进行了展示，并且从实现流程、代码结构、操作方式等方面对实现的情况进行了重点说明。完成的主要工作是基于功能的设计，进行了代码实现。

第5章 安全管理系统测试和性能分析

本章主要完成业务网安全管理系统的测试工作。本章首先介绍了系统测试环境和测试工具，接着进行功能测试，在该部分针对每个功能模块都设计了测试用例，然后进行性能测试。

5.1 测试工具和环境

5.1.1 测试工具

TestLink[39]是开源的专业管理测试用例和 bug 的工具，它可以管理测试用例的整个生命周期，之后还可以统计分析测试结果。而且，很多 bug 跟踪系统可以和 TestLink 建立关联关系，如 Bugzilla[40]、mantis[41]等。

性能测试的主要目的是确定用户在访问系统时，系统是否可以在规定时间内作出回应，并且如果有很多用户同时访问系统时系统是否还能稳定地运行[42]。本研究使用 Loadrunner 11 作为模拟压力的测试软件，使用 nmonanalyser 作为性能报告生成工具，使用 nmon 作为性能监控工具。

5.1.2 测试环境

系统的测试的硬件环境如表 5-1 所示，软件环境如表 5-2 所示。

表 5-1 测试的硬件环境

设备名称	数量	型号	备注
数据库服务器	1	虚拟机	双 4 核 CPU，内存 16G
应用服务器（tongweb）	13	虚拟机	每台虚拟机双 4 核 CPU，内存 16G。
A10	2	负载均衡	A10 设备
压力测试机	1	Intel(R)Xenon(R)CPU E5-2620 2.00GHZ	2 路 6C 超线程，内存 48G
	2	Intel(R)Xenon(R)CPU E5-2620 2.00GHZ	2 路 6C 超线程，内存 48G
	3	Intel(R)Xenon(R)CPU E5-2620 2.00GHZ	2 路 6C 超线程，内存 48G
	4	Intel(R)Xenon(R)CPU E5-2620 2.00GHZ	2 路 6C 超线程，内存 48G

表 5-2 测试的软件环境

软件名称	版本号	备注
Windows	Window2008	压力测试机
Centos	5.6	应用服务器
Centos	5.6	数据库服务器
Tongweb	5	Web 中间件
Oracle	11	数据库
LDAP	7	帐号、授权存储

5.2 系统功能测试

功能测试是为了验证程序是否能够满足系统需求，并能够正常执行返回期望的结果。接下来将分别对 4A 安全系统的五大功能模块进行相应的功能测试。

5.2.1 统一门户模块功能测试

统一门户模块主要测试这三个功能：综合视图、个人工作台、辅助功能，它们的测试如下所述。

（1） 综合视图

综合视图包括应用资源展现、系统资源展现、帐号权限展示以及公告信息展示。综合视图的具体用例见表 5-3。

表 5-3 综合视图测试用例表

用例描述	期望输出	测试结论
输入主帐号及登录密码，点击登录	提示登录成功	正常
用户登录成功后，选择其被授权的应用资源进行展示	展示应用资源的名称、图标等	正常
用户登录成功后，选择其被授权的系统资源进行展示	展示系统资源的名称、图标等，并支持查询	正常
点击查看个人主帐号的权限全景视图	展示全景视图，即主帐号在哪些资源有从帐号及对应权限操作权限	正常
点击公告栏	展示文字、图片及附件等公告信息	
在公告栏中的附件上点击下载	下载附件	正常

（2） 个人工作台

个人工作台包括六个子功能：安全文件夹、待办事项、Push 信息视窗、委托授权、主页显示设置和主帐号密码重置。

其中，安全文件夹需要测试是否可以为用户提供一个个人私有的安全文件

夹，用户可以上传、下载和分发文件等。

待办事项需要测试是否可以向用户提供待办事项提示服务并且用户可以对事项进行相应的处理。

Push 信息视窗需要测试是否可以为用户提供来自于外部系统的 Push 信息视窗展示，以便于用户直接在 4A 个人工作台查看其在外部系统门户中的工作汇总、待办任务、重要提醒。

主页显示设置需要测试用户是否可以设置登录主界面，提高用户使用效率。主帐号登录后可以在主界面上显示个人本次及上次登录时间。

主帐号密码重置需要测试用户是否可以自主修改密码或者系统提示用户主帐号密码过期时用户重置密码的场景。用户可以在个人工作台中进行主帐号密码修改，用户需输入旧密码及要更改的新密码。4A 系统在验证用户主帐号旧密码正确以及新密码符合密码策略要求之后，应提示用户修改密码成功。

个人工作台具体用例见表 5-4。

表5-4 个人工作台测试用例表

用例描述	期望输出	测试结论
查看用户的私有安全文件夹，上传文件到文件夹，接着对文件夹中的文件进行下载和分发等	文件依次上传、下载和分发成功	正常
输入某待办事项，如资源接入、给帐号授权等	系统向用户提供待办事项提示及相应处理功能	正常
点击 Push 信息视窗展示	为用户提供 Push 信息视窗展示，视窗中包含用户在外部系统门户中的工作汇总、待办任务、重要提醒	正常
设置登录主界面，将进入系统后第一界面设置为公告栏展示或应用资源菜单功能	设置成功，且主帐号登录后可以在主界面上显示个人本次及上次登录时间	正常
输入新的密码信息，进行自主修改密码	4A 系统在验证用户主帐号旧密码正确以及新密码符合密码策略要求之后，提示用户修改密码成功	正常
输入新的密码信息，当系统提示用户主帐号密码过期时	4A 系统在验证用户主帐号旧密码正确以及新密码符合密码策略要求之后，提示用户修改密码成功	正常

（3） **辅助功能**

辅助功能包括个人界面锁屏、短信提醒、安全警示、帮助信息、在线问答、

单点登录可用性探测和即时通讯。

个人界面锁屏需要测试用户是否可以手动锁屏，或登录 4A 系统后长时间不操作或者离开工位的情况下，是否可以对 4A 系统页面进行锁定。

短信提醒需要测试 4A 系统在主帐号登录成功、实体权限变更完成或有待办任务等情况时是否有短信提醒，以减少帐号被冒用、帐号状态异常变更及工单处理不及时等问题。

安全警示需要测试 4A 系统应在用户登录界面或登录后的界面是否可以展现必要的安全警示内容，用于提醒用户按管理要求执行操作。

表 5-5 辅助功能测试用例表

用例描述	期望输出	测试结论
用户点击 4A 门户界面上的锁屏按钮	门户页面被锁定	正常
用户登录 4A 系统后长时间不操作	系统根据设置好的默认锁屏时间进行自动锁屏，门户页面被锁定	正常
在门户界面锁定情况下，输入认证信息	用户重新回到操作页面	正常
分别做下列操作：主帐号登录成功、实体权限变更、有待办任务	有短信提醒	正常
用户登录 4A 系统	在用户登录界面或登录后的界面展现必要的安全警示内容：关键操作会被记录并审计、法律法规条例、违法责任等	正常
在门户界面上点击帮助	提供操作员需要的资料下载或帮助手册等	正常
用户向 4A 系统提交问题	系统管理员收到问题，对问题进行解答后返回，用户收到答案	正常
用户登录后选择可用性探测功能	显示资源的可用性情况	正常
用户登录后选择即时通讯功能，并选择要交流的用户或群组	可以进行即时交流	正常

帮助信息需要测试用户点击帮助时 4A 系统是否会提供操作员需要的资料下载或帮助手册等。提供操作员需要的各类资料，如工具软件、客户端工具的下载，以及使用手册等。

在线问答需要测试在用户是否可以向 4A 系统提交问题，然后系统管理员或 4A 维护人员是否可以对提交的问题进行解答并返回答案给用户。

单点登录可用性探测需要测试 4A 门户是否可提供一种对资源（系统资源、

应用资源）的可用性探测功能，便于个人用户自行完成单点登录可用性探测。

即时通讯需要测试用户登录 4A 门户后是否可以在即时通讯功能中选择用户或群组进行工作交流。

辅助功能具体测试用例见表 5-5。

5.2.2 帐号管理模块功能测试

帐号管理包括主、从帐号管理以及密码策略管理。主帐号管理需要测试是否可以对主帐号的相关属性息进行管理，属性包括基本信息、扩展属性、帐号状态、密码策略、认证策略、帐号类型和帐号标记等。从帐号管理需要测试用户是否可以对其拥有的从帐号的相关属性息进行管理，属性包括基本信息、扩展属性、帐号状态、帐号类型和帐号标记等。密码策略管理需要测试是否可以对所有不同应用场景下的密码策略进行存储，并可以按照密码策略对密码进行定期核查，在密码即将过期的时候，会对用户发送密码即将过期的提示消息。

帐号管理模块具体测试用例见表 5-6。

表 5-6 帐号管理模块测试用例表

用例描述	期望输出	测试结论
点击帐号管理中的主帐号管理，对主帐号进行增、删、改	转到主帐号管理界面，主帐号进行增、删、改成功	正常
点击帐号管理中的主帐号管理，对主帐号属性进行编辑	转到主帐号管理界面，属性管理编辑成功	正常
点击帐号管理中的从帐号管理，对从帐号进行增、删、改	转到从帐号管理界面，主帐号进行增、删、改成功	正常
点击帐号管理中的从帐号管理，对从帐号属性进行编辑	转到从帐号管理界面，用户可以对从帐号的各属性进行管理	正常
设置用户密码即将过期	系统提示密码即将过期的消息	
点击帐号管理中的密码策略管理	展示所有应用场景下的密码策略	正常

5.2.3 认证管理模块功能测试

4A 认证管理包含两部分：认证策略管理和单点登录管理。

认证策略管理可以对不同的应用场景中的不同认证策略进行新增、删除、修改和查找操作。在单点登录管理中，首先对用户拥有的从帐号（系统资源和应用资源）进行可用性进行探测。在确定可用性后，用户可以选择可用的从帐号进行登录。

认证管理模块测试用例见表 5-7。

表 5-7 认证管理测试用例表

用例描述	期望输出	测试结论
用户登录主帐号，选择认证管理中的认证策略管理，对策略进行新增、删除、修改和查找操作	策略新增、删除、修改和查找成功	正常
选择认证管理中的单点登录管理	返回从帐号的可用性探测结果	正常
在单点登录管理中，点击具有可用性的从帐号进行登录	从帐号登录成功	正常

5.2.4 授权管理模块功能测试

表5-8 授权管理测试用例表

用例描述	期望输出	测试结论
选择授权管理中的角色和权限管理，选择查看角色	展示帐号的所有角色	正常
选择角色和权限管理，选择角色创建，填入角色属性，点击创建	角色创建成功	正常
选择角色和权限管理，选择角色修改，填入要修改的角色属性	角色变更成功	正常
选择角色和权限管理，选择角色删除，删除帐号的某角色	角色删除成功	正常
选择角色和权限管理，设置帐号或角色的权限	设置成功	正常
选择角色和权限管理，删除帐号或角色的某项权限	删除成功	正常
选择授权管理中的角色和权限管理，选择权限查看	显示帐号或角色的所有权限信息	正常
选择授权管理中的委托授权管理，输入从帐号的委托用户，并设定从帐号使用期限，到期前不主动收回	到期后 4A 系统自动收回	正常
选择委托授权管理，输入从帐号的委托用户，并设定从帐号使用期限，到期前用户主动收回	从帐号到期前主动收回	正常
选择授权管理中的委托授权管理，查看委托授权	显示用户的所有委托授权信息	正常
选择授权管理中的委托授权管理，删除某个委托授权	删除成功	正常
选择授权管理中的委托授权管理，修改某个委托授权，如修改使用周期	修改成功	正常

授权管理包括角色和权限管理和委托授权管理。首先，角色和权限管理需要测试是否可以对帐号的角色、角色的权限进行增、删、改、查等操作。在委托授权管理中用户可以将自己的从帐号委托给其他用户，并可以规定该用户对从帐号的使用期限，到期后 4A 系统会帮助用户自动收回从帐号，用户也可以在使用期限到期前主动收回，用户可以增加委托授权、删除委托授权、修改委托授权以及查询委托授权等。

表 5-8 给出了授权管理模块的所有测试用例。

5.2.5 审计管理模块功能测试

审计管理模块包括审计策略中心、数据采集、数据标准化、日志数据分析等功能。

审计策略中心需要测试是否可以完成策略创建、策略修改、策略删除、策略查询等功能。

数据采集需要测试是否可以对用户操作日志进行收集和存储。安全系统数据的采集范围包括 4A 系统帐号、授权管理日志；4A 系统认证、登录日志；4A 系统自管理日志等。

表 5-9 审计管理测试用例表

用例描述	期望输出	测试结论
选择审计管理中的审计策略中心，进行策略创建	策略创建成功	正常
选择审计管理中的审计策略中心，选定某策略并进行修改	策略修改成功	正常
选择审计管理中的审计策略中心，删除某策略	策略删除成功	正常
进行一些操作，如登录、授权等，检查是否生成了相应的操作日志	生成了相应的操作日志	正常
当原始数据不合法时，给出校验不合法的结果	校验不合法	正常
当原始日志字段不完整时，提示用户日志缺乏完整性	提示用户日志缺乏完整性	正常
对原始日志解析提取的字段映射为标准化字段，并按照 5W1H 模型进行补全	日志的字段全是标准化字段	正常

表 5-9（续表）

用例描述	期望输出	测试结论
选择中间数据处理中的日志筛选，输入操作信息进行日志筛选	筛选出相关日志	正常
让某用户做一些违规操作或是频繁做一些日常少有的操作	返回检测出的异常行为并进行警报	正常
选择均值统计分析，基于均值统计分析策略，对标准化日志进行统计计算，得出业务场景阀值	返回业务场景阀值	正常

数据标准化需要测试是否可以完成数据合法性校验，验证原始数据内容是否合法；接着是日志完整性校验，验证原始日志字段完整性；然后是日志字段映射，将原始日志解析提取的字段映射为标准化字段；最后是日志补全，将原始日志映射后的字段按照 5W1H 模型进行补全。

日志数据分析需要测试是否可以基于关键字和均值统计或基于用户的行为模式发现异常、违规行为，并进行警报。其中，均值统计分析可以基于均值统计分析策略，对标准化日志进行统计计算，得出业务场景阀值

审计管理功能模块的测试用例如表 5-9 所示。

5.3 系统性能测试

分别进行以下三种场景的性能测试。测试场景 1： 4000 用户瞬时并发；测试场景 2：8000 用户瞬时并发；测试场景 3：承载最大 12000 在线用户。

测试结果如表 5-10 所示。其中，当瞬时并发 4000 用户时，系统的平均操作响应时间为 1.076 秒，当瞬时当瞬时并发 8000 用户时，系统的平均操作响应时间为 1.221 秒。在并发测试过程中，tongweb 没有报错现象，所有操作全部通过，符合预期结果。在负载方面，能够加载 1.2 万用户同时并发处理，持续加载 1 小时，tongweb 应用、oracle 数据库、A10 负载均衡、Ldap 等系统服务器内存、CPU、I/O 资源使用较为平稳，不会出现较大波动。以上三种测试场景的测试结果均符合预期结果。

但是压力测试存在以下限制：由于为生产情况测试，此次测试脚本为模式 1.2 万使用人员登录模拟，记录从提交用户名/服务密码到认证结果返回的请求响应时间，为减少压力测试对生产数据的影响无法模拟增、删、改、查等日常操作。因此测试数据与现实日常情况可能存在误差。

表 5-10 系统性能测试数据

功能	并发/负载	并发压力	响应时间（秒）	A10	Tongweb		Oracle	LDAP
登录以及静态密码验证	并发	4000	1.076	CPU：7% 内存：37%	29	CPU：17%、内存：78%	CPU：31% 内存：94%	CPU：1% 内存：22%
					31	CPU：12%、内存：72%		
					33	CPU：17%、内存：68%		
					34	CPU：15%、内存：95%		
					35	CPU：18%、内存：88%		
					36	CPU：22%、内存：78%		
					37	CPU：20%、内存：93%		
					38	CPU：18%、内存：83%		
					39	CPU：18%、内存：96%		
					103	CPU：21%、内存：89%		
					104	CPU：22%、内存：72%		
					105	CPU：20%、内存：78%		
					106	CPU：19%、内存：96%		
		8000	1.221	CPU：15% 内存：37%	29	CPU：16%、内存：79%	CPU：44% 内存：98%	CPU：1.2% 内存：22%
					31	CPU：11%、内存：72%		
					33	CPU：18%、内存：69%		
					34	CPU：17%、内存：95%		
					35	CPU：19%、内存：90%		
					36	CPU：24%、内存：79%		
					37	CPU：25%、内存：94%		
					38	CPU：19%、内存：84%		
					39	CPU：19%、内存：96%		
					103	CPU：22%、内存：90%		
					104	CPU：23%、内存：73%		
					105	CPU：21%、内存：78%		
					106	CPU：20%、内存：97%		
	负载	12000 负载测试	39.56s	Cpu13% 内存38%	29	CPU：22%、内存：62.5%	CPU：45% 内存：78%	CPU：1.3% 内存：15%
					31	CPU：13%、内存：62.5%		
					33	CPU：23%、内存：62.5%		
					34	CPU：21%、内存：62.5%		
					35	CPU：20%、内存：62.5%		
					36	CPU：21%、内存：62.5%		

表 5-10（续表）

功能	并发/负载	并发压力	响应时间（秒）	A10	Tongweb	Oracle	LDAP
				37	CPU：26%、内存：62.5%		
				38	CPU：21%、内存：62.5%		
				39	CPU：19%、内存：62.5%		
				103	CPU：23%、内存：62.5%		
				104	CPU：25%、内存：62.5%		
				105	CPU：22%、内存：62.5%		
				106	CPU：20%、内存：62.5%		

另外，还进行了兼容性测试，经测试 4A 系统适用测试中所有的 Windows 操作系统，并且支持测试中的各数据库系统，还支持目前主流的浏览器，并兼容 IE7 以上版本的浏览器，测试结果符合兼容性需求。

5.4 测试结论

在测试中，首先进行功能测试，对业务支撑网安全管理系统的每个模块进行了详细的测试，证明了五大功能模块（统一门户功能模块、帐号管理功能模块、认证管理功能模块、授权管理功能模块以及审计管理功能模块）可以正常合理地运行并完成相应的功能。然后进行了非功能测试，包括性能测试和就兼容性测试，测试结果表明性能测试结果符合预期指标，4A 系统的性能良好。

5.5 本章小结

本章首先介绍了测试 4A 系统的测试环境和测试工具，接着针对每个功能模块都设计了测试用例，按照测试用例进行相应的功能测试，然后进行非功能性测试，测试结果均符合预期，说明该业务网安全管理系统能够满足预期需求。

结　论

本文主要介绍了业务支撑网安全管理系统的设计与实现。通过对国内外研究现状进行分析，根据实际中移动公司的业务支撑网管理需求，对 4A 安全管理系统进行了详细的需求分析，针对各个功能点进行了详细设计，包括了数据库设计和业务逻辑设计，并在此基础上对系统进行了开发和测试，最终使得系统能够正常稳定的运行。

本论文的主要工作包含以下几点：

（1）对安全管理系统的现状进行了深入的调研，明确了要实现的基础功能点，包括统一门户构建、帐号管理、认证管理、授权管理以及审计管理五个功能模块。根据各模块需求分析的结果，明确了各功能点，对系统中要使用的数据库中的表结构进行了详细设计，并且对要实现的功能点的具体实现进行了业务逻辑结构设计。

（2）基于需求分析和系统设计，对各功能模块进行了编码实现。对系统统一门户中各功能点进行了合理的布局，方便了用户操作；实现了对系统中各种类型帐号的管理，以主帐号为例，实现了对其增、删、改、查操作，以及与其相关的属性进行管理；实现了主从帐号认证功能，对系统中使用的认证策略进行了有效的管理；实现了授权管理模块，完成了对系统中各种角色的权限管理功能，能够支持实体级别授权以及批量授权等操作；实现了对安全系统进行审计的功能，包括了审计日志数据的采集、处理和存储，并对数据进行审计分析，发现数据中的异常，来发现系统中存在的安全隐患。

（3）在完成了对系统各功能的实现后，对各功能点按照规范要求的功能点进行测试，包括功能测试和性能测试。从最后的测试结果可以看出设计的安全管理系统基本能满足业务需求。

（3）在安全管理系统界面开发的过程中，尽量的保持着良好的交互性，遵循简单明了的设计风格，方便用户进行操作。

目前系统的基本功能已经能够很好的进行实现，但是目系统还存在如下几个需要改进的地方。（1）由日志数据量巨大，现有的数据分析方法并不能够很好的满足数据量大的要求，因此需要对安全管理系统中的数据分析方法进行更新，提高安全管理系统的智能程度。（2）随着用户数量多增大，系统的访问量也会随之增加，为了保证设计管理系统的稳定性，能够同时容纳大规模用户的访问，并且提高系统的响应速度。

参考文献

[1] Debar H, Becker M, Siboni D. A Neural Network Component for an Intrusion Detection System[A]. IEEE Symposium on Security and Privacy[C].Okland: IEEE Computer Society, 1992, 25(9): 256-266.

[2] 卿斯汉, 蒋建春, 马恒太,等. 入侵检测技术研究综述[J]. 通信学报, 2004, 25(7):19-29.

[3] 杜建平. 云平台下主动防御技术的研究与实现[D]. 北京邮电大学, 2016.

[4] Department of Defense ComPuter Security Center.Department of Defense Trusted ComPuter System Evaluation Criteria.DoD 5200. 28-STD. USA: DOD, 1985.

[5] National ComPuter Security Center.Trusted Network Inter Pretation of the Trusted ComPuter System Evaluation Criteria. NCSC-TG-005. USA: DOD, 1987.

[6] Miyazaki, Kunihiko, et al. "Trusted computer system." U.S. Patent No. 7,210,043. 24 Apr. 2007.

[7] 林钰超. 专用网络中终端安全接入系统的设计与实现[D]. 电子科技大学, 2014.

[8] Spencre C. Lee. An Introduction to Identity Management, 2003.

[9] Dan E. Intelligent authentication, authorization, and administration (I3A)[J]. Information Management & Computer Security, 2006, 14(11):5-23.

[10] Chang D Y, Benantar M, Chang J Y C, et al. Authentication and authorization methods for cloud computing system security: U.S. Patent 9,288,214[P]. 2016-3-15.

[11] Kubovy J, Huber C, Jäger M, et al. A Secure Token-Based Communication for Authentication and Authorization Servers[C]//International Conference on Future Data and Security Engineering. Springer, Cham, 2016: 237-250.

[12] Li B, Ge S, Wo T, et al. Research and implementation of single sign-on mechanism for ASP pattern[C]//International Conference on Grid and Cooperative Computing. Springer, Berlin, Heidelberg, 2004: 161-166.

[13] Varadharajan V, Crall C, Pato J. Issues in the design of secure authorization service for distributed applications[C]//Global Telecommunications Conference, 1998. GLOBECOM 1998. The Bridge to Global Integration. IEEE. IEEE, 1998, 2: 874-879.

[14] Lenz T, Zwattendorfer B. Towards Cross-Border Authorization in European

eID Federations[C]//Trustcom/BigDataSE/I SPA, 2016 IEEE. IEEE, 2016: 426-434.

[15] Tumin S, Encheva S. Securing enterprise wide authorization management through delegation[C]//Proceedings of the 9th WSEAS international conference on Applications of computer engineering. World Scientific and Engineering Academy and Society (WSEAS), 2010: 81-86.

[16] Jonscher D, Moffett J D, Dittrich K R. Complex Subjects-or: The Striving for Complexity is Ruling our World[J]. 1993.

[17] Zhao G, Hu X, Li Y, et al. Scheme for digital documents management in networked environment[C]//Network Infrastructure and Digital Content, 2009. IC-NIDC 2009. IEEE International Conference on. IEEE, 2009: 995-998.

[18] 王立强. 天津移动 4A 管理系统体系设计[D]. 北京邮电大学, 2009.

[19] 赵瑞星. 4A 安全系统管理平台子系统的分析与设计[D]. 北京邮电大学, 2011.

[20] 王明强.一种基于 4A 系统的应急一体化平台[J]. 信息通信, 2017 (02):210-211.

[21] 郭敏. 基于4A管控系统的金库管理系统的设计与实现[D]. 北京交通大学, 2017.

[22] 杨诚炜. 4A 管理控制平台系统的设计[D]. 电子科技大学, 2016.

[23] 徐开勇, 龚雪容, 成茂才. 基于改进 Apriori 算法的审计日志关联规则挖掘[J]. 计算机应用, 2016, 36(07):1847-1851.

[24] 段娟. 基于 Web 应用安全日志审计系统的研究与设计[D]. 北京邮电大学, 2015.

[25] 王玉婉. 移动互联网行为审计系统的设计与实现[D]. 北京交通大学, 2014.

[26] 关振胜. 公钥基础设施 PKI 与认证机构 CA[M]. 北京: 电子工业出版社, 2002.

[27] 程念胜, 张宜生, 李德群. 一种基于令牌的单点登录认证服务[J]. 计算机应用, 2008, 28(S2):53-55.

[28] 瞿霞. 基于挑战/应答机制的短信动态口令身份认证系统研究[J]. 软件导刊, 2015,14(10):134-137.

[29] 李彦明. 多通道生物认证关键技术的研究[D]. 兰州理工大学, 2014.

[30] 杨金文. 单点登录系统的研究与实现[D]. 辽宁工业大学, 2017.

[31] 胡建鹏. 基于 Portal 的统一身份认证与系统集成研究[J]. 计算机工程与科学, 2010, 32(12):30-33.

[32] 江华. 基于角色的授权管理模型的研究与应用[D]. 广州：华南理工大学，2005.

[33] 阳小兰，钱程，赵海廷．Web 日志分析系统研究[J]. 计算机技术与发展, 2011, 21(9): 211-215.

[34] 熊熙．基于 Web 日志挖掘的个性化服务技术的研究[J]. 网络安全技术与应用, 2010,(6): 61-64.

[35] Kolari P, Joshi A. Web Mining: Research and Practice[J]. Computing in Science & Engineering, 2004, 6(4):49-53.

[36] 郑立洲. 短文本信息抽取若干技术研究[D].中国科学技术大学,2016.

[37] Nasraoui O, Soliman M, Saka E, et al. A Web Usage Mining Framework for Mining Evolving User Profiles in Dynamic Web Sites[J]. IEEE Transactions on Knowledge & Data Engineering, 2007, 20(2):202-215.

[38] Wai-KiChing, 程伟琪, 黄曦敏,等. 马尔可夫链:模型、算法与应用[M]. 清华大学出版社, 2015.

[39] Siebra C A, Lino N L, Silva F Q B, et al. On the specification of a test management solution for evaluation of handsets network operations[M]. IEEE, 2010.

[40] Akbarinasaji S, Caglayan B, Bener A. Predicting bug-fixing time: A replication study using an open source software project ☆[J]. Journal of Systems & Software, 2017.

[41] 招敏怡. TESTLINK 和 MANTIS 的优化及其应用[D]. 华南理工大学, 2010.

[42] 纪力炜. 基于 JMeter 工具的性能自动化测试平台设计与实现[D]. 南京邮电大学, 2016.

哈尔滨工业大学学位论文原创性声明和使用权限

学位论文原创性声明

本人郑重声明：此处所提交的学位论文《移动业务支撑网安全管理系统设计与实现》，是本人在导师指导下，在哈尔滨工业大学攻读学位期间独立进行研究工作所取得的成果，且学位论文中除已标注引用文献的部分外不包含他人完成或已发表的研究成果。对本学位论文的研究工作做出重要贡献的个人和集体，均已在文中以明确方式注明。

作者签名：[illegible] 日期：2018 年 10 月 16 日

学位论文使用权限

学位论文是研究生在哈尔滨工业大学攻读学位期间完成的成果，知识产权归属哈尔滨工业大学。学位论文的使用权限如下：

（1)学校可以采用影印、缩印或其他复制手段保存研究生上交的学位论文，并向国家图书馆报送学位论文；（2）学校可以将学位论文部分或全部内容编入有关数据库进行检索和提供相应阅览服务；（3）研究生毕业后发表与此学位论文研究成果相关的学术论文和其他成果时，应征得导师同意，且第一署名单位为哈尔滨工业大学。

保密论文在保密期内遵守有关保密规定，解密后适用于此使用权限规定。

本人知悉学位论文的使用权限，并将遵守有关规定。

作者签名：[illegible] 日期：2018 年 10 月 16 日

导师签名：[illegible] 日期：2018 年 10 月 16 日

致　谢

时间过得飞快，研究生生活即将结束，在哈工大读研的这几年时间里，是我的快乐时光，不仅提升了我的学习能力，更提升了我的科研水平，使得我对于软件项目开发和管理有了更深刻的认识，为以后进一步工作打下了坚实的基础。但是这些进步都离不开老师和同学们的鼓励，以及家人对我默默的支持，才使我有机会顺利的完成学业。

感谢李全龙老师对我的悉心指导，李老师在治学上非常严谨、工作中认真负责，不仅传授给我知识，还教会了我许多做人的道理。在老师的指导帮助下，我的研究工作才得以顺利的展开。尤其是在论文的修改阶段，李老师虽然工作很忙，但是还是愿意抽出大量的时间，来对我的论文提出宝贵的修改意见，大到论文的内容结构，小到一个标点符号，他都非常仔细的进行了评阅。从论文的开题到最终论文的完成，都有老师的辛勤付出。在此，我再次诚恳的对李老师说一声感谢。

感谢我的校外导师钟山在项目上给予我的大力支持，不管是从技术上还是从工程上都给了我很多的指导，让项目得以顺利开展。

感谢学校的兄弟姐妹们对我的帮助，让我的生活多了很多快乐。

感谢实习单位同事对我的指导和帮助。

感谢一直以来支持我的朋友们。

感谢我的父母，是他们给了我生命，感谢他们一直支持我的学业和工作，是他们无私的奉献，才使我坚持走到了今天。在以后的日子里，我将认真工作，回报我的家人。祝愿他们能够身体健康。

最后，感谢百忙之中抽出时间评阅我的论文并提出宝贵建议的各位老师，在此表示衷心的感谢！

个人简历

1985 年 08 月 22 日出生于黑龙江省牡丹江市。

2004 年 08 月考入黑龙江省黑河学院计算机科学与技术专业，2008 年 07 月本科毕业并获得工学学士学位。

2008 年 8 月至 2012 年 4 月，在哈尔滨华强电力自动化工程有限公司任职，职务技术经理。

2012 年 5 月至今，在亿阳信通股份有限公司任职，职务项目经理。

2013 年 12 月至今，考入哈尔滨工业大学攻读软件工程硕士。