学校编码：10384　　分类号_____ 密级 _____

学号：X2012231269　　UDC_____

厦门大学

工 程 硕 士 学 位 论 文

基于 J2EE 银行信息安全监控系统设计与实现

Design and Implementation of Bank Information Security Monitoring System Platform Based on J2EE

张美娜

指导教师姓名： 杨 律 青 教 授

专 业 名 称： 软 件 工 程

论文提交日期： 2016 年 09 月

论文答辩日期： 2016 年 11 月

学位授予日期： 2016 年 12 月

指 导 教 师：_____

答辩委员会主席：_____

2016 年 9 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　年　月　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

随着外部应用系统的多样化、复杂化，全行的安全信息和事件分布零散，没有进行全面统一收集，数据内容杂乱、各种安全日志信息和事件缺乏必要的关联分析。让安全人员很难进行深度的挖掘有效信息，数据安全人员难以从数据中发现问题、难以掌控整体的安全趋势，缺乏安全事件监控。导致安全部门难以持续跟踪并及时处理突发安全事件，安全事件未能及时反馈，不能很好的把控数据安全问题。

怎样从海量数据中快速及有效地精炼信息，为人工决策提供支撑，为一线日常 IT 风险管理提供高效的、有效的辅助工具，验证在恰当的地方运用了有效的安全策略，并确保当前的安全控制完全、有效地遵循了安全策略，理解和控制风险、发现威胁和违规行为，为制定补救措施提供参考依据，遵循监管制度对日志和事件数据进行归档、保护的要求，满足安全管理、审计、报告的需要。有效地解决以上问题就需要一个平台来统一收集各个系统的数据安全信息，对多样化的复杂的数据进行统一采集抽取、按统一数据规范化处理规则有效转换日志数据、将规范化后的数据加载到一个统一的数据仓库里。

通过数据采集器收集各终端安全系统的日志信息，监控全行终端安全的使用和运行情况，通过展示各安全客户端的管理现状，发现安全客户端的缺陷及不足。在全行的整个网络系统内实施统一的安全访问策略，实现基于用户、终端设备类型、设备接入时间、设备接入地点以及设备的接入方式等多种维度的认证和授权，满足多层次、泛终端的接入认证方式的需求。同时对访问用户进行全生命流程管理，以提高访客的工作效率。通过统一访问安全策略管理控制提升终端的安全等级，阻止不安全的终端、不满足统一方位的安全策略的终端接入网络，来提升安全客户端的安全性。

从海量数据中精炼信息，为后续的企业决策活动提供有效的支撑。通过数据分析，理解和控制风险、发行危胁和违规行为，为制定补救措施提供参考依据。依据总、分行一线 IT 安全管理的日常工作和规则制度需求，提供较全面的、易用、有效的信息检索和报表功能，使安全监控组件成为 IT 安全管理人员提高工作效率和准确性的日常性辅助工具。

关键词：信息安全；采集分析；J2EE

Abstract

With external application of diverse and complex, the company's security information and events are scattered, no comprehensive unified collection, data content messy, all kinds of security log information and event lacks the necessary correlation analysis. The defects let the staff of security department difficult to mining the valid information, data security problems difficult found from the data, it is difficult to control overall security trends, lack of security event monitoring. Led to the security department is difficult to continue to track and timely handling of security incidents, security incidents failed to timely feedback, can not be a good control of data security issues.

How to quickly and efficiently refine information from massive data, to provide support for decision-making manual, to provide effective and efficient aid for the daily IT risk management, verify that the appropriate place to use an effective security policy, and make sure the safety of the current control completely and effectively follow the security policies, understand and control risks, identify threats and violations, provide a reference basis for remedial measures, follow regulatory system log and event data archiving, protection requirements, meet the security management, auditing, need to be reported. Data security information effectively solve the above problem requires a unified platform to collect each system, unified collection, extraction to various complex data according to the unified data standardization processing rules for effective conversion of log data, the normalized data is loaded into a unified data warehouse. Effectively solve these problems we need a unified platform to collect safety data information for each system, unified collecting and extractiing the diverse and complex data, according to the unifion and normalization data processing rules to convert the log data effectively, and then load the normalization data to a unified data warehouse.

Through the data collector to collect log information for each terminal security system, monitoring the terminal security of bank using and operation, by showing the

status of each client security management, found the security clients's defects and deficiencies. Throughout the whole bank network to implement the unified security access policies, based on the user, terminal device type, device access time, location of the equipment and the access way of the equipment, etc. With the multiple dimensions of authentication and authorization to meet the needs of multiple-level, extensive terminal access authentication methods'. While the access users get on the life process management, in order to improve the visitors' efficiency of operations. By the unified access the security policy management to controlling and approving the security level of the terminal, prevent the unsafe terminal and the not satisfied unified orientation’s policy of the terminal which is access the netword, to improve the safety of the security client.

Refining information from the massive data, and to provide the effective support for the follow up of the corporate decision. Through data analysis, understanding and control risks, finding the threats and violations, provide the references of the development of remedial measures. According to the daily work of IT security management and the requirements of the rules of the head office and the branches, provide a more comprehensive, easy use, the effective information retrivel and the report functions, make the safety monitoring component to become the IT security managers to improve the work efficiency and accuracy of routine tools.

Key Words: Data Security; Data Collection and Analysis; J2EE

目 录

Contents

第一章 绪论

1.1 研究背景

外部应用系统越来越多样化、复杂化，全行的安全信息和事件分布零散，没有进行全面统一收集，数据内容杂乱、各种安全日志信息和事件缺乏必要的关联分析，让安全人员很难进行深度的挖掘有效信息，数据安全人员难以从数据中发现问题、难以掌控整体的安全趋势，缺乏安全事件监控，难以持续跟踪处理突发安全事件，未能及时反馈、把控数据安全问题。

怎样从海量数据中快速、有效地精炼信息，为人工决策提供有效支撑，为一线日常 IT 风险管理提供高效的、有效的辅助工具，验证在恰当的地方运用了有效的安全策略，并确保当前的安全控制完全、有效地遵循了安全策略，理解和控制风险、发现威胁和违规行为，为制定补救措施提供参考依据，遵循监管制度对日志和事件数据进行归档、保护的要求，满足安全管理、审计、报告的需要。解决以上问题需要一个公共平台来统一收集各个子系统及外部系统的安全信息数据，将信息安全原始日志数据按采集规则进行统一抽取、将抽取的数据进行规范化数据转换、最后将转换后的规范化数据加载到一个统一的数据仓库里。

1.2 研究目标

建立统一的采集平台、集中存储管理安全日志，从海量数据中快速、有效地精炼出符合需求的数据信息，扩大安全信息和分析数据范围，全面及时的采集各内部及外部系统的安全信息和事件，为全行信息安全监控中心的决策活动提供有效的支撑。实现多维度关联分析发现安全风险及用户登录类风险关联分析功能，对数据进行深度数据挖掘；集中展示安全事件及风险分析报告，一体化、多视角呈现全行安全风险视图和风险态势；提供安全事件取证和跟踪技术手段实现原始日志数据的检索、查询功能。通过收集各终端安全系统的日志信息，监控全行终端安全的使用和运行情况，展示终端安全的管理现状、发现终端安全的缺陷及不足。通过数据分析，理解和控制风险、发行危胁和违规行为，为制定补救措施提供参考依据。依据总、分行一线 IT 安全管理的日常工作和规则制度需求，提供

较全面的、易用、有效的信息检索和报表功能，使安全监控组件成为 IT 安全管理人员提高工作效率和准确性的日常性辅助工具。

1.3 研究内容

（1）Oracle、Hive 和 CTBase 数据库表结构设计及开发；

（2）应用 Oracle、Hive、CTBase 数据表分析安全信息业务逻辑关系；

（3）Hadoop 进行大数据存储；

（4）HBase 开发；

（5）应用 Highcharts 图表功能展示安全监控系统信息安全，实现对信息安全的实时监控、按图表展示信息进一步数据挖掘信息安全问题；

（6）在 J2EE 平台下，用 Struts2、Highcharts、JSP、MyBatis 等开发技术应用的研究；

（7）学习了解软件开发的生命周期原理，掌握需求分析与软件设计技能。

1.4 本论文结构安排

本论文针对银行信息安全监控分析系统的设计目标与业务需求重点做了探讨；然后，对信息安全监控系统的总体设计、功能模块设计、数据模型设计以及数据安全设计做了详细介绍；再者，给出了系统的具体功能实现与软件测试部分；最后，对本系统从需求到功能实现做了总结和未来系统需要进一步优化做了展望。

全文共六章，大致可分为三部分。第一至第二章构成第一部分，第三至第五章构成第二部分，最后一章为第三部分。具体内容如下：

第一章：绪论，主要论述了本文的研究背景、研究目标和研究内容。

第二章：相关技术介绍，本章主要介绍开发过程中需要应用到的一些主要技术，明确本系统将采用的技术框架和设计原则。

第三章：需求分析，论述系统的需求分析，内容包括：用户需求、用户角色定义、功能需求和非功能性需求等方面。本章节重点对业务功能，包括监控信息数据分析与统计等需求进行介绍。

第四章：系统设计，本章主要针对系统的总体设计、功能模块设计、数据库