Inline Text Wrapping Picture

北京邮电大学

硕士研究生学位论文开题报告

学 号: 2019180167

姓 名: 赵昱

学 院: 计算机学院(国家示范性软件学院)

专业(领域): 软件工程

研究方向: 企业信息化

导师姓名: 修佳鹏

攻 读 学 位: 工程硕士

2020年11月29日

|  |  |  |  |
| --- | --- | --- | --- |
| 论文题目 | 基于区块链的信息系统安全审计方案的研究与原型开发 | | |
| 选题来源 | 其他 | 论文类型 | 应用研究 |
| 开题日期 | 2020-11-28 | 开题地点 | 新科研楼118教室 |
| **一、立题依据（包括研究目的、意义、国内外研究现状和发展趋势，需结合科学研究发展趋势来论述科学意义；或结合国民经济和社会发展中迫切需要解决的关键科技问题来论述其应用前景。附主要参考文献目录）（不少于800字）**  随着Internet的飞速发展，Web 应用正在从传统的小型业务应用逐渐向大型、关键型业务应用发展，它的普及已经全面渗透到社会的各个领域，成为电子政务、教育、经济贸易、电子商务、公共服务、文化传播、生活娱乐等的新型助力和变革力量，促进信息社会的发展。现代社会中人们越来越离不开各种信息网络和信息系统，信息化已经成为世界发展的潮流，深刻的改变着人们的工作、学习、交往等生活的方方面面。但是信息化就好像一把双刃剑一样，在给人们的生活提供便利的同时，其中涉及的各种安全问题也越来越困扰着人们，人们也越来越重视信息安全问题。  政府机关的信息系统中保存有重要的政府公文和资料，企业的信息系统中保存有重要的客户数据和核心的技术资料，这些单位的内部人员有合法的身份和合法的访问权限，并能接触到重要的单位内部数据，他们由于误操作或故意窃取数据给单位造成的损失非常大。  这些安全问题靠以往的外网安全产品如防火墙、入侵检测系统和反病毒木马软件是难以解决的。Web访问日志中包含了大量的用户浏览信息，通过对Web日志中用户行为数据的提取， 能够反映Web系统的应用情况。为了解决信息系统的安全问题，安全审计系统作为解决方案被提出来。  安全审计系统能够及时地将用户操作以日志的形式记录下来,并且对违规操作进行阻断，日志信息可以为事后取证提供证据。安全审计系统对内部人员的违规操作起到了威慑作用，保证了信息系统的安全。  然而日志本身的安全问题也是同等重要，因为日志服务器无法有效地避免日志篡改问题。  区块链技术的发展，为实现日志信息的保护提供了可能。区块链技术具有去中心化、不可篡改和追踪溯源等特性，其应用场景已涉及医疗、电网、农产品追溯等方向。区块链技术可以为产品的日志保护问题提供更为有效的解决方案，区块链中的交易记录具备防篡改的功能，一旦某个交易被篡改，区块链网络中的节点会快速检测出该行为。通过区块链技术有效地解决了日志文件易被篡改的问题，同时通过特殊的日志共享机制，在保障隐私的前提下极大地提高了日志的利用价值。 | | | |

|  |
| --- |
| **二、研究内容和目标（说明课题的具体研究内容，研究目标和效果，以及拟解决的关键科学问题。此部分为重点阐述内容）（不少于2500字）**  1. 研究内容  1.1 安全审计系统的需求分析  安全审计系统通过日志信息监控用户对各种信息系统的操作行为，将用户的操作行为以日志的形式记录下来，按照审计人员自定义的规则判断操作行为是否合法，如果是违规操作则进行阻断并且发出警报，使得违规操作无法执行，提供事后取证的证据以追究相关人员的责任。  1)告警响应  安全审计的目的是发现监管用户的上网行为，及时发现危险行为，所以实时告警功能很有必要。实时报警规则可以根据预先设定，如何种可疑行为告警或者告警信息发送的目的邮箱等。将违反安全规则的上网信息即时报告给系统管理员或监控中心。报警规则（策略）一般可由系统管理员制定，根据系统的应用场景，选择对系统或网络安全性能影响严重的时间，制定合适的报警方式。当安全事件发生时给用户发出警告同时把告警信息反馈给管理员。  2)规则配置  审计人员可以在配置界面添加、删除或修改审计规则信息。当用户选择了某个信息系统后,可以添加、修改或删除其所对应的各种审计规则。审计规则应该包括如下信息：监控的用户操作，用户操作的具体信息，安全审计系统针对用户操作的反应(允许或拒绝)。  3)规则匹配  接受日志采集模块发来的日志信息，按照审计规则进行判断。若审计规则允许该用户操作行为，则该用户操作行为被放行；若审计规则拒绝该用户行为，则发出警报，由日志模块记录下该违规操作的日志信息。  4)权限管理  安全审计系统可以有多个用户，不同的用户对应不同的信息系统，可以看到用户各自的审计界面  5)审计分析  利用统计分析方法对历史审计数据按照某些规则进行分析，发现其中潜在的安全威胁和漏洞。  6)审计浏览  经过授权的管理人员可以对审计记录访问，可以以多种维度对日志信息进行浏览分析。  1.2日志模块的研究与实现  日志模块基于Log4j，Log4j是Apache的一个开放源代码项目，通过使用Log4j，可以控制日志信息输送的目的地是控制台、文件、GUI组件、甚至是套接口服务器、NT的事件记录器、UNIX Syslog守护进程等；也可以控制每一条日志的输出格式；通过定义每一条日志信息的级别，能够更加细致地控制日志的生成过程。这些可以通过一个配置文件来灵活地进行配置，而不需要修改应用的代码。  1.3日志系统的研究与搭建  在复杂的企业应用服务群中，记录日志方式多种多样，并且不易归档以及提供日志监控的机制。无论是开发人员还是运维人员都无法准确的定位服务、服务器上面出现的种种问题，也没有高效搜索日志内容从而快速定位问题的方式，因此需要一个集中式、独立的、搜集管理各个服务和服务器上的日志信息，集中管理，并提供良好的UI界面进行数据展示，处理分析，而ELK提供一套开源的解决方案，能高效、简便的满足以上场景，ELK日志系统Elasticsearch、Logstash、Kibana、Filebeat等开源软件的组合，在实时数据检索和分析场合，通常是配合共用。  1) Elasticsearch是一个开源分布式搜索引擎，提供搜集、分析、存储数据三大功能。它的特点有：分布式，零配置，自动发现，索引自动分片，索引副本机制，restful风格接口，多数据源，自动搜索负载等。  2) Logstash主要是用来日志的搜集、分析、过滤日志的工具，支持大量的数据获取方式。一般工作方式为c/s架构，client端安装在需要收集日志的主机上，server端负责将收到的各节点日志进行过滤、修改等操作在一并发往Elasticsearch上去。  3) Kibana也是一个开源和免费的工具，Kibana可以为Logstash和Elasticsearch提供日志分析友好的Web界面，可以帮助汇总、分析和搜索重要数据日志。  4) Filebeat通过增量的方式负责收集日志内容，并将日志发送至Logstash。  1.4区块链的研究及搭建  区块链因为比特币的出现为人们所熟知，从产生迄今，在金融、证券、资本和科技行业的应用呈现出爆发式增长。虽然比特币是区块链最著名的应用，但区块链可以应用于远不止加密货币的各种应用。由于它可以在没有银行或任何第三方可信中间机构的情况下在双方之间完成支付，区块链可以应用于数字资产、汇款以及在线支付等各种金融服务。此外，构建于区块链技术之上的各种应用，例如智能合约应用、物联网和安全服务等，也正在成为构建下一代互联网应用最有前景的技术之一。  比特币、以太坊是公有链的著名代表，除比特币、以太坊这类所有节点都可以自由进入和退出的公有链平台外，只对经过授权的组织团体开放的联盟链平台近年来也成为了关注的热点。  相比传统中心化技术架构，联盟链吸收了公有链的技术特点，融汇了分布式架构、分布式存储、点对点网络协议、加密算法、共识算法、智能合约等多类技术，能够很好地解决企业间的效率和信任等合作问题; 同时，相比于公有链技术架构，联盟链拥有更好的安全性及性能，同时对监管友好，能够支持穿透式或集中式的监管。  联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入与退出网络。各机构组织组成利益相关的联盟，共同维护区块链的健康运转。  FISCO BCOS是由国内企业主导研发、对外开源、安全可控的企业级金融联盟链底层平台，由金链盟开源工作组协作打造，并于2017年正式对外开源。社区以开源链接多方，截止2020年5月，汇聚了超1000家企业及机构、逾万名社区成员参与共建共治，发展成为最大最活跃的国产开源联盟链生态圈。底层平台可用性经广泛应用实践检验，数百个应用项目基于FISCO BCOS底层平台研发，超80个已在生产环境中稳定运行，覆盖文化版权、司法服务、政务服务、物联网、金融、智慧社区等领域。  1.5智能合约的研究与实现  智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。以太坊是一个构建于区块链技术之上的去中心化应用平台，通过引入智能合约及去中心化的虚拟机，允许任何人在该平台上建立去中心化的应用。相较于通过道德或法律等手段推动履行的传统合约，智能合约最大的不同点在于当合约执行的条件被触发后，计算机程序会保证合约一定会被及时地执行。由于区块链的去中心化特性，智能合约的执行是一个无法逆转的单向过程，因而具有客观性。从以太坊开始，区块链逐渐从加密数字货币的代名词演变为一种可信服务的基础组件。  Solidity 是一门面向合约的、为实现智能合约而创建的高级编程语言。这门语言受到了 C++，Python 和 Javascript 语言的影响，设计的目的是能在以太坊虚拟机（EVM）上运行。  2.研究目标  本课题最终目标是设计一个安全审计系统，该系统能够满足的基本需求为：  1)日志生成需求：按照格式化标准生成日志  2)日志数据管理需求：能够实现用户上传日志数据操作以及系统实现将日志数据的数据指纹存储到区块链的具体位置  3)日志数据展示需求：使存储日志数据相关信息可视化，用户能够查询到存储的日志数据的具体内容以及日志数据存储凭证的相关信息  4)日志数据校验需求：管理员能够通过相应的功能模块查询日志数据的完整性，以及系统定时对日志进行审计  根据上述功能需求可将安全审计系统整体架构分为6个模块：  1)日志模块：主要是对日志数据的来源、附加信息以及格式进行一些限制，实现日志标准化的输出  2)日志获取模块：负责以增量式地读取日志文本文件的方式来获取日志，并且将日志传输到下游Logstash  3)日志存储模块，为日志提供存储服务，系统中的存储服务器包括Elasticsearch以及区块链。Elasticsearch中的数据主要用来进行日志检索，区块链中的数据主要用来进行数据校验，为日志信息的上链编写智能合约  4)数据校验模块，实现日志信息的校验功能，包括日志数据以及区块链信息校验。  5)定时审计模块：对日志进行定时审计，出现错误日志则将错误信息推送至安全审计系统  6) 页面展示模块，实现日志信息的展示功能，包括日志数据的展示以及告警信息的展示。  3. 关键科学问题  3.1对日志的建模  日志用来记录用户操作、系统运行状态等，是一个系统的重要组成部分。然而，由于日志通常不属于系统的核心功能，所以常常不被团队成员所重视，但是良好的日志可以保证系统可靠的运行。  好的日志可以帮助系统的开发和运维人员：了解线上系统的运行状态；快速准确定位线上问题；发现系统瓶颈；预警系统潜在风险；挖掘产品最大价值。  不好的日志导致：对系统的运行状态一知半解，甚至一无所知；系统出现问题无法定位，或者需要花费巨大的时间和精力；无法发现系统瓶颈，不知优化从何做起；无法基于日志对系统运行过程中的错误和潜在风险进行监控和报警；对挖掘用户行为和提升产品价值毫无帮助。  系统中的日志生成模块需要帮助用户系统记录更多有效的日志，通过调研论文以及实际的日志系统，找到一种日志记录的最佳实践。设计和实现一种易于使用、高效、对业务代码无侵入地获取Java应用的日志数据的方式，同时，该模块需要满足系统的整体设计目标，对获取的日志的格式进行规范化处理。 |

|  |
| --- |
| **三、研究方案设计及可行性分析（包括：研究方法，技术路线，理论分析、计算、实验方法和步骤及其可行性等）（不少于800字）** |

|  |
| --- |
| **四、本研究课题可能的创新之处（不少于500字）**  一般我们需要进行日志分析场景：直接在日志文件中通过命令grep、awk操作就可以获得自己想要的信息。但在规模较大的场景中，此方法效率低下，面临问题包括日志量太大如何归档、文本搜索太慢、多维度查询，因此需要集中化的日志管理，所有服务器上的日志收集汇总。常见解决思路是建立集中式日志收集系统，将所有节点上的日志统一收集、管理、访问。ELK提供了一整套解决方案，并且都是开源软件，之间互相配合使用，完美衔接，高效的满足了很多场合的应用，是目前主流的一种日志系统。  安全审计系统用于系统安全管理，通过分析日志可以及时发现系统异常或违规操作，并为入侵行为提供证据。但日志经常是入侵者的主要攻击目标，容易受到篡改、删除、伪造等破坏，给审计日志安全性带来了极大隐患。因此，必须健全审计日志保护机制，保证日志完整性。  区块链本质上是一个去中心化的数据库，将信任关系从中心化的机构转移到所有参与计算的个体上。在远端上的每一个交易都由区块链中的网络节点通过共识机制进行验证。区块链中的交易记录具备防篡改的功能。一旦某个交易被篡改，区块链网络中的节点会快速检测出该行为。区块链针对系统的数据校验需求，具备去中心化、不可篡改性、公开透明等优势。  基于区块链技术，保证了安全审计系统的可信，防止日志记录被篡改。 |
| **五、研究基础与工作条件（1.与本项目相关的研究工作积累基础 2.包括已具备的实验条件，尚缺少的实验条件和拟解决途径）（不少于500字）**  1. 与本项目相关的研究工作积累基础  本人研究生阶段是一名软件工程专业的学生，一直致力于软件开发领域的学习和工作，熟悉常用的编程语言、开发工具和开发框架，同时在服务器应用程序的开发上有着较多的经验，对于B/S或者C/S结构的设计与实现，以及前后端之间的通信和交互有比较多的经验。熟悉软件工程的完整过程，对于应该选择何种开发模型，如何进行系统测试有着较多的经验。  与此同时，由于要开发的这套系统是基于区块链的，所以在开始具体项目之前，我已经学习了项目中将要使用的联盟链框架FISCO BCOS的基本操作，对FISCO BCOS平台有了一定的了解，已经在服务器上搭建了FISCO BCOS的平台。  2.实验条件  2.1已具备的实验条件  1) 由于项目基于联盟链FISCO BCOS，实验室提供了可供部署、运行的服务器，已经在服务器上搭建了FISCO BCOS的平台。  2) 本人已经学习及开发过多个后台系统，技术上会使用Spring Boot框架构建后台系统，Vue.js框架构建前端页面。  3) 知识方面可以通过学校及实验室提供的资源，查阅文献资料，遇到的技术性问题可以与导师、同学进行交流，寻找解决方案。  2.2尚缺少的实验条件和拟解决途径  对日志系统的解决方案ELK还不了解，后续可以通过查阅文献资料和书籍对ELK解决方案进行深入学习，了解技术背后的知识，另外要在服务器上部署ELK的集群。 |

**学位论文工作计划**

|  |  |  |
| --- | --- | --- |
| 时间 | 研究内容 | 预期效果 |
| 2020.11-2020.12 | 课题调研，准备开题 | 完成开题报告 |
| 2021.01-2021.03 | 研究日志模块的实现 | 完成日志模块的开发 |
| 2021.04-2021.05 | 研究ELK日志系统的内部原理 | 完成ELK日志系统的搭建 |
| 2021.06-2021.07 | 学习智能合约 | 完成项目中使用的智能合约的编写 |
| 2021.08-2021.10 | 编写定时审计模块，将所有模块组合进行联调 | 完成整个系统并测试通过 |
| 2021.11-2022.02 | 撰写论文 | 完成毕业论文 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 评  定  小  组  成  员 | 姓 名 | 职 称 | 单位名称 | 职务 |
| 杨正球 | 教授 | 北京邮电大学 | 组长 |
| 修佳鹏 | 副教授 | 北京邮电大学 | 成员 |
| 王安生 | 副研究员 | 北京邮电大学 | 成员 |
| 夏亚梅 | 副教授 | 北京邮电大学 | 成员 |
| 刘辰 | 副教授 | 北京邮电大学 | 成员 |
|  |  |  |  |
| 导师意见： | | | | |
| 区块链是数据防篡改的有效解决方案，论文将其应用到信息系统安全审计中，选题具有一定的研究价值和实用参考价值，同意开题。 | | | | |
| 导师（签名）：  日期： 年 月 日 | | | | |
| 开题报告小组意见： | | | | |
| 组长（签名）：  日期： 年 月 日 | | | | |
| 学院意见（签章）： | | | | |
| 负责人：  日期： 年 月 日 | | | | |