****

**毕业设计（论文）开题报告**

**题目：企业服务器文件完整性检查系统的设计与实现**

**专 业 网络空间安全**

**学 生 陈锦前**

**学 号 160700226**

**班 号 1604301**

**指导教师 董开坤**

**日 期 2020.01.08**

**目录**

**1.课题背景及研究的目的和意义 2**

1.1课题背景 2

1.2研究的目的和意义 2

**2.国内外在该方向的研究现状及分析 2**

2.1国外现状及分析 2

2.2国内现状及分析 2

**3.研究内容及拟解决的关键问题 3**

3.1研究内容 3

3.2拟解决的关键问题 3

**4.拟采取的研究方法和技术路线、进度安排、预期达到的目标 4**

4.1拟采取的研究方法和技术路线 4

4.1.1研究方法 4

4.1.2技术路线 9

4.2进度安排 10

4.3预期达到的目标 10

**5.课题已具备和所需的条件 10**

**6.研究过程中可能遇到的困难和问题，解决的措施 10**

**7.参考文献 10**

1．课题背景及研究的目的和意义

1.1课题背景

随着现代网络技术的快速发展和网络规模的不断扩大，计算机网络已渗透到了社会的各个领域，人们在享受网络带来的资源共享及信息交流方便快捷的同时，也不得不面对越来越多的来自网上的恶意攻击和各种黑客入侵等，也存在个人隐私泄露、重要文件篡改等安全问题，而且日新月异，人们对于网络安全的需求与日俱增[1]。

互联网与生俱有的开放性、交互性和分散性特征，使人类所憧憬的信息共享、开放、灵活和快速等需求得到满足。网络环境为信息共享、信息交流、信息服务创造了理想空间，为人类社会的进步提供了巨大推动力。然而也正是由于互联网的上述特性，产生了许多安全问题[2]。尤其当今网上支付、数字货币技术不断成熟，保护企业的文件至关重要。

攻击者越来越多,攻击工具和手法日趋复杂多样,单防火墙技术已经无法完全阻止网络入侵这一日益严重的网络安全问题。所以需要在防火墙后提供新的安全保障，网络的防卫必须采用一种纵深的、多样的手段[3]。入侵检侧系统(IDS)是一种不同于防火瑞的主动保护网络资派的网络安全系统,是防范网络攻击的最后一道防城,是作为防火堵有益补充而出现的网络第二道防线产品,在网络安全技术中起着不可替代的作用[4]。

1.2研究的目的和意义

按照美国国防部1983年制定的可信计算机系统评测标准，信息安全应当确保信息的机密性(Confidentiality)、完整性(Integrity)和可用性(Availability)这三个基本标准要求。其中,完整性指防止信息遭受以非授权方式所作的篡改或破坏,它作为信息安全三个基本标准要求之一,占有举足轻重的作用[5]。

系统的安全是一个体系,建立在各种安全机制集成的基础上,入侵检测系统(IntrusionDeteetionSystem,简称IDS)作为系统安全的一道重要防线,主要是通过多种手段监控系统来发现入侵。文件完整性检查是IDS中的关键部分之一,它通过检查系统关键资源的变化情况来为入侵的发现提供依据。文件完整性检查系统的目的在于:保证被保护主机的关键资源不被恶意更改。所谓关键资源是指系统中不应也不能被经常更改的关键成分,如:内核、配置文件、可执行程序、库等,以及那些由第三方提供的可能影响到主机运行的资源[6]。

文件完整性检查系统的优点：①从数学上分析，攻克文件完整性检查系统，无论是时间上还是空间上都是不可能的。文件完整性检查系统是非常强劲的检测文件被修改的工具。②文件完整性检查系统具有相当的灵活性，可以配置成为监测系统中所有文件或某些重要文件。③当一个入侵者攻击系统时，他会干两件事：首先，他要掩盖他的踪迹，即他要通过更改系统中的可执行文件、库文件或日志文件来隐藏他的活动；其次，他要作一些改动保证下次能够继续入侵。这两种活动都能够被文件完整性检查系统检测出[7]。

通过研究企业服务器文件完整性检查系统的设计与实现，可以有效地检测攻击，可以更有效地保护系统关键文件不被篡改，防止木马、病毒等对系统的破坏，保障企业正常运行[8]。

2．国内外在该方向的研究现状及分析

2.1国外现状及分析

2014年Mark Kedgley通过分析当前黑客的攻击行为以及网络环境，指出了当前杀毒软件的不足之处，例如无法有效抵御基于0-day漏洞的攻击行为，同时阐明了文件完整性检查系统的优点及可靠性[9]。

2014年，日本学者Watanabe,H根据在日本使用广泛的Gfarm分布式文件管理系统，在已有的基于时间戳的文件完整性检查系统基础上，设计了一套改进系统，大幅度提升了该系统的效率[10]。

云存储系统中数据的所有权和管理权分离,导致用户数据隐私泄露、完整性破坏等一系列安全问题。2018年Pinheiro Alexandre等人设计了一套基于实时监控云端数据及服务器行为的系统用于保护用户隐私[11]。

同时Googel公司申请了大量关于文件完整性的专利，例如：File metadata verification in a distributed file system（JC Davis, WA Davis - US Patent App. 15/806,399, 2019）、Storing and verifying the integrity of event related data（D Patton, R Mehta - US Patent 10,467,067, 2019）、[Methods for identifying audio or video content](https://s2.sci-hub.org.cn/extdomains/patents.google.com/patent/US10007723B2/en)（WY Conwell- US Patent App. 10/007,723,2018）、Verification of peer-to-peer multimedia content（S Holtmanns, J Ignatius - US Patent 9,578,041, 2017）为自己的搜索引擎以及Youtube视频网站提供保护。

2.2国内现状及分析

近年来中国学者在文件完整性检查研究方向取得了不断进步，尤其在云计算以及云存储方向，根据云计算环境下平台系统的特点,刘海永提出了一套新型的文件完整性检测系统的设计方案，采用了新型的SHA-3安全算法生成文件摘要，将安全系统与被检测主机相互分离，将安全检测负载与被检测主机适当分离。实现了检测系统的运行的大部分负载从被监控主机转移,从而适用于云计算环境[12]。

随着云端存储技术的不断成熟，目前已有的数据完整性证明机制还存在不支持全动态操作,通信和计算开销大等各种问题。因此贾倍提出了支持数据隐私的数据完整性证明机制、一个带秩的多分支路径结构(MBT,Multi-branch Tree)和数据完整性检测算法、以及基于MBT的数据完整性证明机制，该方案不仅保护了数据对第三方验证者的隐私性,而且支持全动态操作与批量审计操作,简化了数据完整性证明信息的获取过程[13]。

刘广沛利用移动Agent技术在云端部署分布式虚拟机代理模型,同时通过虚拟机代理模型构建基于区块链的完整性保护框架,使用默克尔哈希树生成文件对应的唯一散列哈希值,借助区块链上的智能合约监控数据变化,及时向数据拥有者发出数据篡改的警告信息，另外,利用“挑战-应答”模式构造基于区块链的云数据完整性验证方案[14]。

移动可信平台需要经常进行大量完整性校验,然而其各种资源却十分有限。张永棠教授提出了一种可以配合各种成熟的HASH算法使用的完整性校验方法——RMAC(Random-MAC)。从不同版本的Linux系统中,搜集了不同格式的ELF文件,随机抽取粒度样本,进行完整性校验分析。由于其引入随机性,每次计算产生的摘要都不同,使目前已有的病毒都无法做到每次都能通过RMAC校验。RMAC提供的障碍有效地降低了病毒的繁殖速度,可以阻止病毒的大规模爆发[15]。

3．研究内容及拟解决的关键问题

3.1研究内容

主要研究内容是设计一个企业服务器文件完整性检查系统，对企业服务器中的文件信息进行提取、分析、检查，以实现在复杂的网络环境下，根据文件属性或者文件摘要进行文件完整性检查，判断文件是否受到恶意篡改。系统的研究分为以下几个方面：

(1)研究基于文件属性的文件完整性检查技术

通常攻击者对文件系统攻击，极有可能改变文件的相关属性，例如：文件大小、修改时间、权限，可以生成文件相关属性的数据库，检查时进行比对，检测是否发生变化。

（2）研究基于文件摘要的文件完整性检查技术

用密码学的方法来检验文件的完整性是大多数软件的共同考虑，常用MD5等算法对文件产生信息摘要(messageid-gest)。由于这些算法中使用的单向散列函数的单向性,入侵者很难逆推,也极难找到两个随机信息使其产生相同的摘要,从而使产生的摘要具有高度安全性。

（3）研究基于FTP协议获取服务器文件信息技术

FTP（File Transfer Protocol，文件传输协议）是TCP/IP协议组中的协议之一。FTP协议包括两个组成部分，其一为FTP服务器，其二为FTP客户端。其中FTP服务器用来存储文件，用户可以使用FTP客户端通过FTP协议访问位于FTP服务器上的资源。由于FTP传输效率非常高，在网络上传输大的文件时，一般也采用该协议。

3.2拟解决的关键问题

综合上文提到的研究目的与研究内容，拟解决的关键问题主要包括以下几点：

（1）用数据库来保存文件系统的正确状态

完整性检查系统在运行之初,先要建立被保护系统安全的初始状态档案。采用数据库可以使记录的保存结构化,迅速索引和定位、方便检查和更新。

（2）生成文件摘要信息

基于文件摘要值的文件完整性的检查是比较文件前后两次的摘要值是否相同，如果被篡改，摘要值将发生改变，因此可以有效检测出文件是否完整。我们要采用合适的算法快速生成文件摘要，并存储到数据库中。

（3）采用快速有效的查找匹配算法

在实际使用中，文件完整性检查系统的效率至关重要，否则无法进行有效的防御，因此在比较文件前后两次的属性或者摘要值时，要采用合适的数据库存储结构以及高效的字符串匹配算法。

(4)从分布式服务器获取文件目录与文件信息

本课题研究的是企业服务器文件完整性检查系统的设计与实现，因此如何快速地从不同的服务器获取文件目录及文件信息也是必须解决的关键问题。

4.拟采取的研究方法和技术路线、进度安排、预期达到的目标

4.1拟采取的研究方法和技术路线

4.1.1 研究方法

根据系统实际功能需求，本次课题将系统分为文件信息收集层、文件信息分析存储层、文件信息对比层和文件完整性检查结果输出层四大层次，整体架构如图4-1所示。

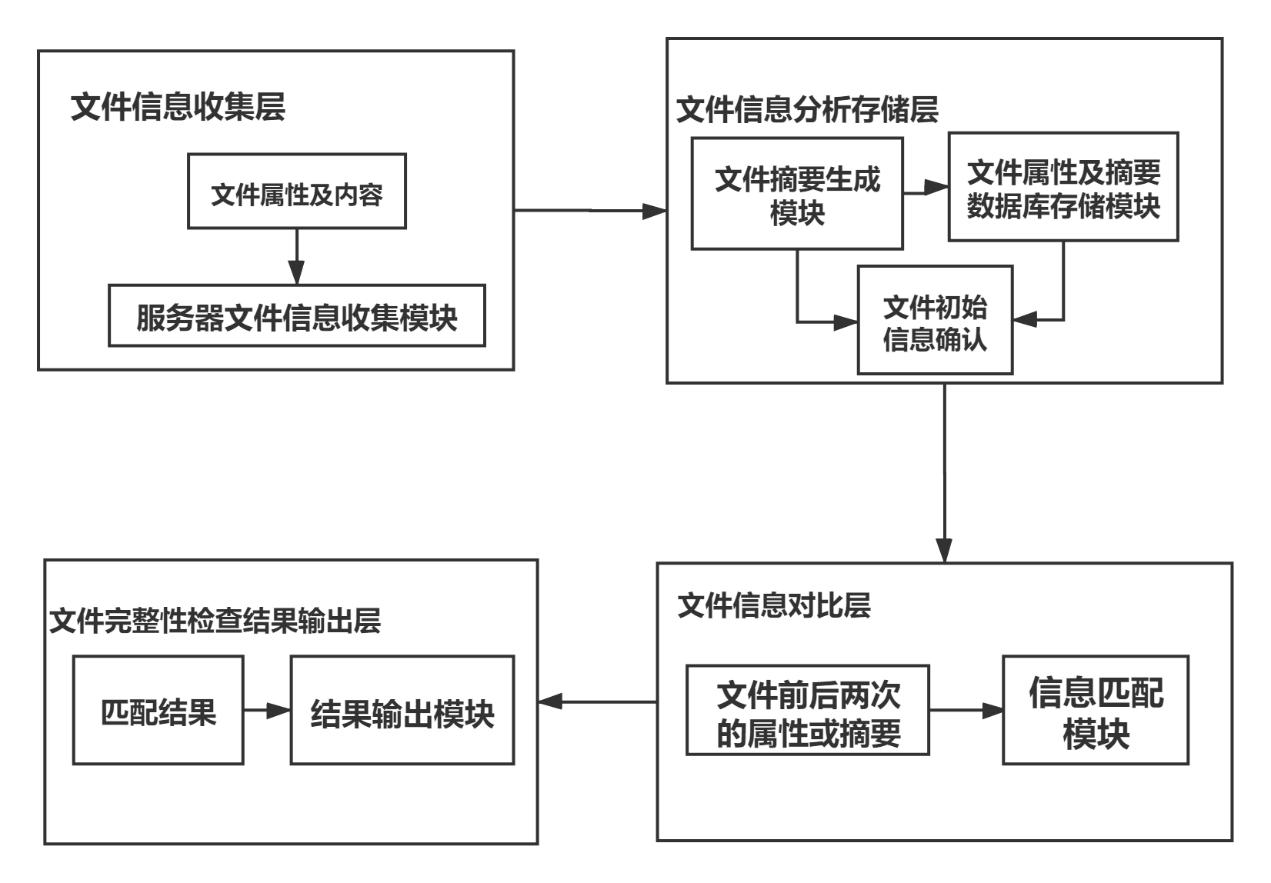


图4-1 系统架构图

1.文件信息收集层

本次课题，我们将模拟真实企业服务器搭建实验设施，构造企业级文件系统。在实现文件完整性检查系统之前，首先需要从不同服务器获取到文件信息。

文件信息收集层流程如图4-2所示。

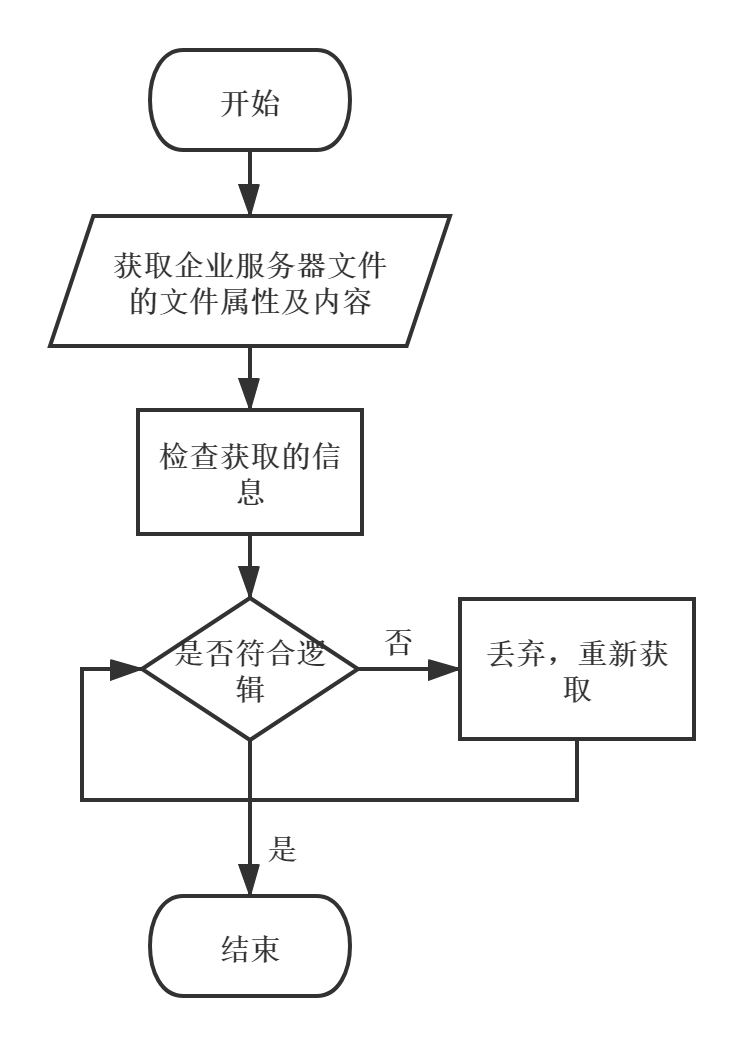


图4-2 文件信息收集层流程图

2.文件信息分析存储层

本层次获得文件信息收集层交付的文件属性及内容信息，首先经过“文件摘要生成模块”生成相应的文件摘要，再将文件摘要及文件属性交给“文件属性及摘要数据库存储模块”正确存储到数据库中。

文件摘要生成模块：使用MD5算法将文件内容转换为固定长度的字符串。

文件属性及摘要数据库存储模块：搭建合适的数据库存储文件属性值及摘要值。

文件信息分析存储层流程如图4-3所示。

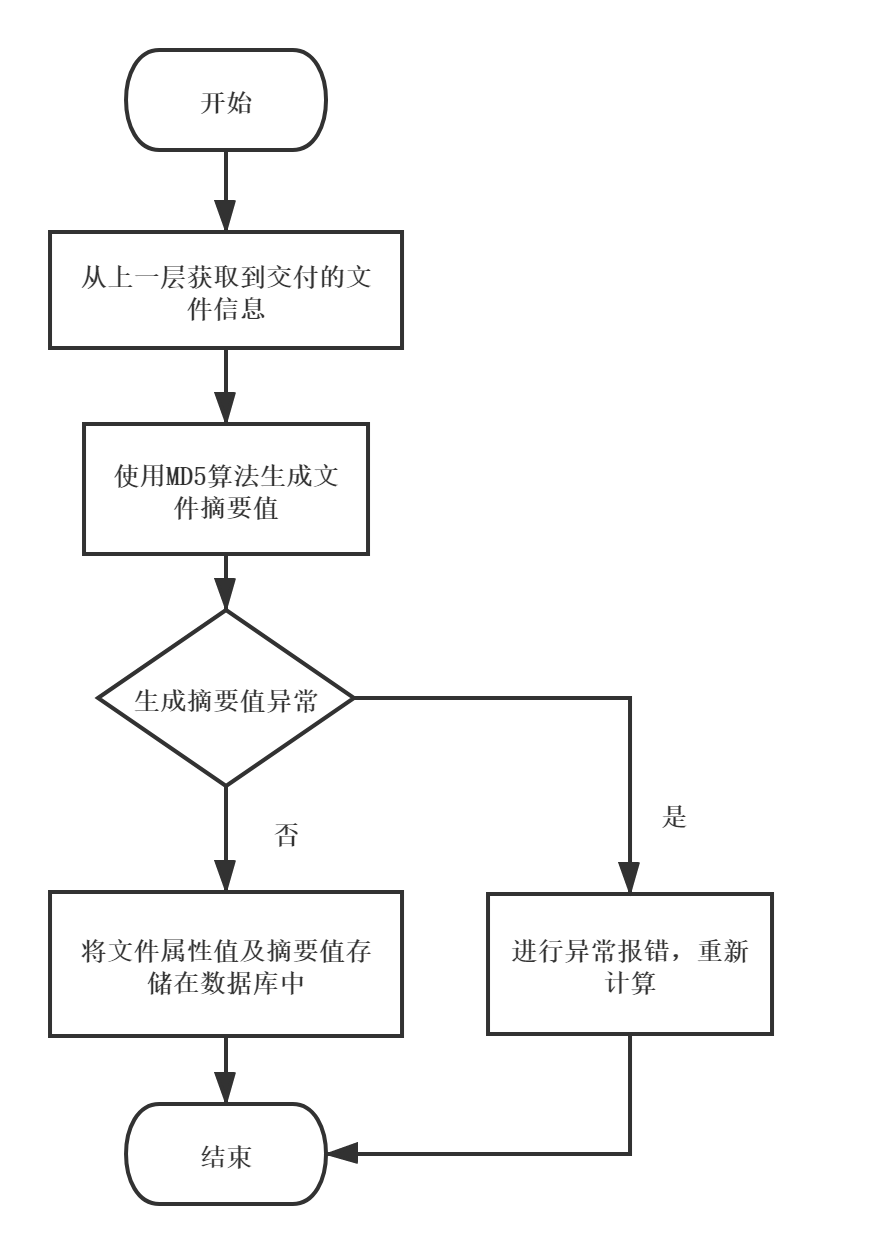


图4-3 文件信息分析存储层流程图

3.文件信息对比层

本层次包括“信息匹配模块”，实现将服务器当前文件信息与用户端数据库存储的文件信息进行对比，并将对比结果交付给文件完整性检查结果输出层，供用户判断是否遭受到攻击。

信息匹配模块：采用合适的匹配算法，将前后两次文件信息进行快速对比，得到匹配结果。

文件信息对比层流程如图4-4所示

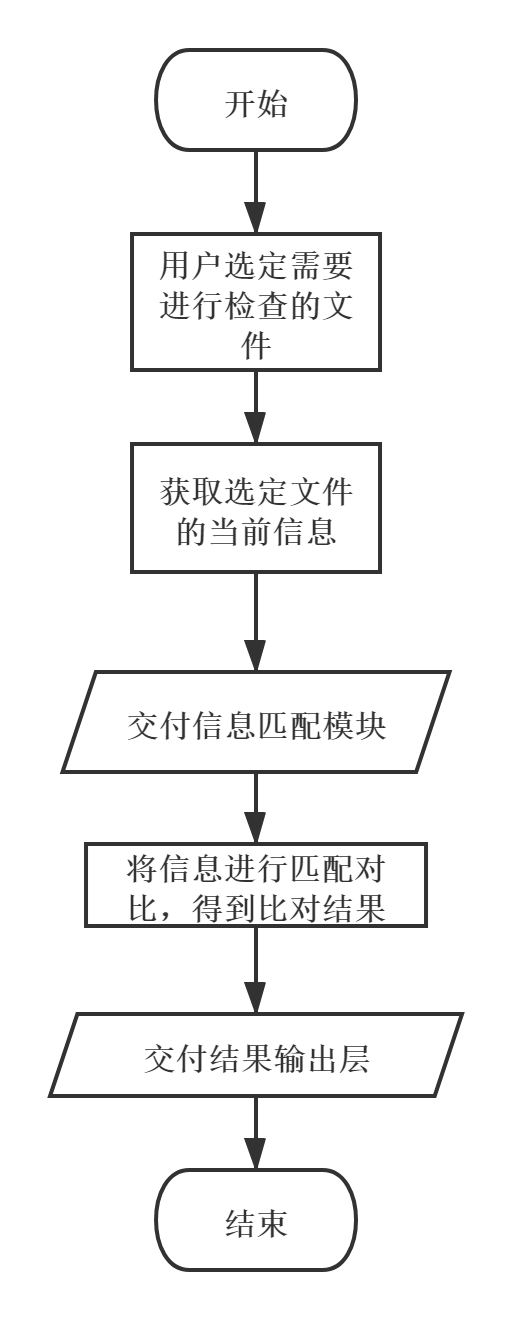


图4-4 文件信息对比层流程图

4.文件完整性检查结果输出层

本层次包括“结果输出模块”，获取文件信息对比层的对比结果，将文件信息发生变化的文件告知用户。

结果输出模块：将文件属性值或摘要值发生改变的文件在用户窗口显示出来，发出遭受攻击警示。

文件完整性检查结果输出层流程如图4-5所示

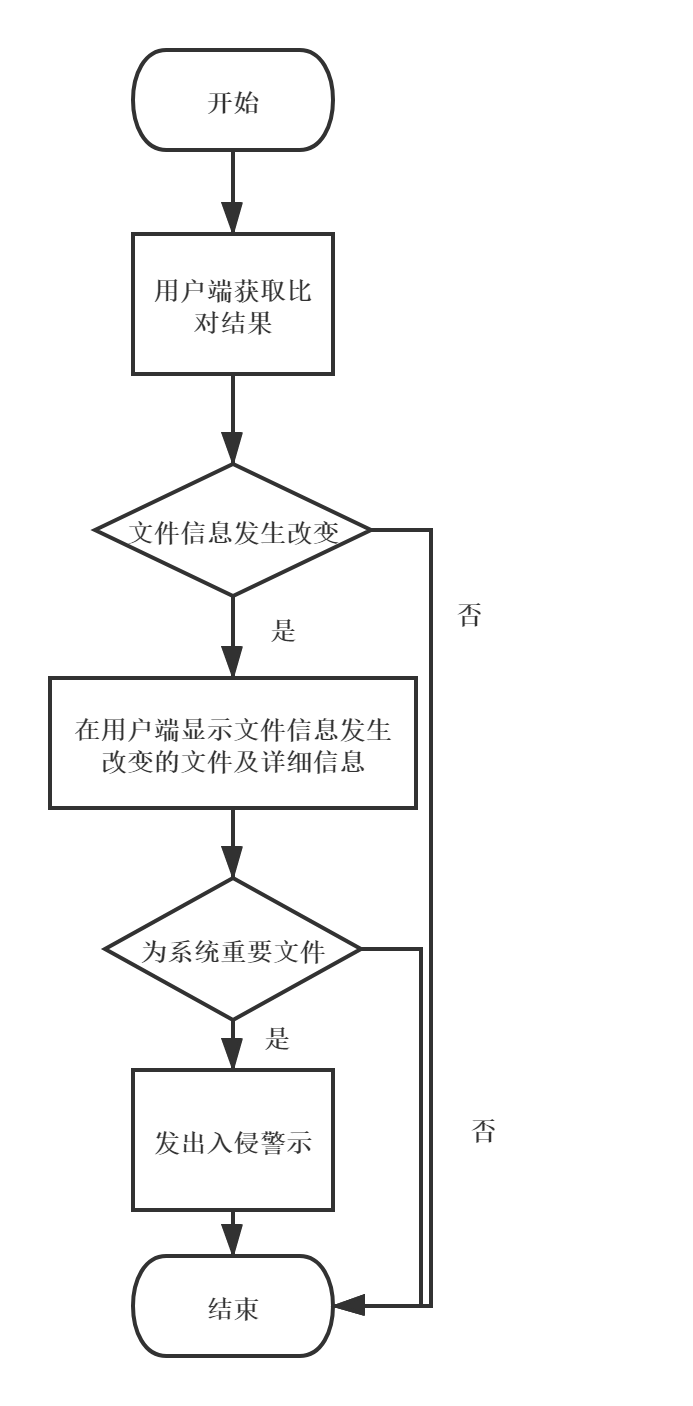


图4-5 文件完整性检查结果输出层流程图

4.1.2 技术路线

1.文件摘要值生成

我们使用基于MD5算法实现生成文件摘要值，MD5算法存在于大量的开源库中。

美国密码学家Ronald Linn Rivest在MD4算法基础上，于1992年设计出更为趋于成熟的MD5算法，使用该算法可以将任意长度的文本转换为一个固定长度的字符串。由于不同文件产生出相同字符串的概率极小，可以将该字符串视为该文件的摘要信息，且被篡改摘要值必发生改变。

2.数据库设计

我们使用MySQL数据库存储文件的属性值及摘要值。

MySQL是一款关系型数据库，具有开发成本低，占用空间小，处理速度快等优点。根据系统功能，设计出三个实体：服务器实体（服务器id、服务器名），文件目录实体（目录名、目录路径）、文件实体（文件名、MD5摘要值、文件属性值）。

4.2进度安排

2020 年 1 月 搜集相关资料，完成前期知识储备和构建,完成实验环境搭建；

2020 年 2 月—3 月 开始进行实验，着手编写各功能模块代码；

2020 年 3 月—4 月 完成代码构建，系统整体联调联试；

2020 年 5 月 完善整体设计，完成论文书写。

4.3预期达到的目标

（1）实现文件完整性检查功能，能够检查出文件的完整性。

（2）列出服务器文件的目录，系统具有默认的检查策略，同时用户可以自主修改检查策略。

（3）能够实时地显示当前检查进程的进度及当前的检查结果。

（4）用户可以随时停止检查进程。

（5）扫描结束时，为用户提供检查结果统计信息并发出警示。

5．课题已具备和所需的条件

MD5生成文件摘要值的算法、MySQL数据库的搭建、分布式服务器的搭建

6．研究过程中可能遇到的困难和问题，解决的措施

系统整体组织架构的构建以及各模块之间的耦合可能存在设计方面的问题。需要及时向有经验的相关人员请教、充分利用网络资源检索解决方法。

获取服务器文件信息过程中，可能存在获取不到完整信息的问题。需要查阅相关资料，搭建正常的实验环境。

在数据库使用过程中，可能存在原理性问题，需要及时在官网查阅使用规则来解决问题。

7．参考文献

[1]靳燕.基于MD5算法的文件完整性检测系统分析及设计[J].网络安全技术与应用,2019(11):36-38.

[2]温强.文件完整性检测的设计与实现[J].科技情报开发与经济,2011,21(09):137-139.

[3]田楠.基于网络的入侵检测技术的研究[J].信息与电脑(理论版),2011(09):155-156.

[4]许军.浅谈入侵检测系统——IDS[J].广西大学梧州分校学报,2004(04):75-77.

[5]陈昕,杨寿保.入侵检测系统中文件完整性检查的研究[J].计算机科学,2002(09):101-103.

[6]陈琦珺,陈性元,唐慧林,牛琳.面向抗攻击测试的完整性检测系统设计[J].微计算机信息,2007(33):65-67.

[7]姚玉献.浅析网络安全与入侵检测系统[J].网络安全技术与应用,2007(12):23-25.

[8]石蕊,高立刚,马一腾.企业级文件完整性监控技术浅析[J].中国金融电脑,2012(12):43-45.

[9]Mark Kedgley. File integrity monitoring in the modern threat landscape[J]. Network Security,2014,2014(2).

[10] H. Watanabe, T. Iwama, K. T. Murata, S. Ushiyama and Y. Muto, Improvement of the Integrity Verification Application Using Timestamp Mechanism for Distributed File System, [J]2014 IEEE 38th International Computer Software and Applications Conference Workshops, Vasteras, 2014, pp. 158-163.

[11]Pinheiro Alexandre,Dias Canedo Edna,de Sousa Junior Rafael Timoteo,de Oliveira Albuquerque Robson,García Villalba Luis Javier,Kim Tai-Hoon. Security Architecture and Protocol for Trust Verifications Regarding the Integrity of Files Stored in Cloud Services.[J]. Sensors (Basel, Switzerland),2018,18(3).

[12]刘海永.云计算环境下文件完整性检测系统的设计[J].信息技术与信息化,2019(03):61-64.

[13]贾倍. 云存储中大数据完整性证明机制研究[D].西安电子科技大学,2018.

[14]刘广沛. 基于区块链的云数据完整性保护机制[D].南京邮电大学,2018.

[15]张永棠.一种移动可信平台ELF文件完整性校验方法[J].井冈山大学学报(自然科学版),2017,38(02):55-60.

指导教师评语：

指导教师签字： 检查日期：