(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103095720 A
(43)申请公布日 2013.05.08

(21)申请号 201310036927.6
(22)申请日 2013.01.30
(71)申请人 中国科学院自动化研究所
地址 100190 北京市海淀区中关村东路 95 号
申请人 东莞中国科学院云计算产业技术创新与育成中心
(72)发明人 王飞跃 邹哲峰 孔庆杰 熊刚 朱凤华
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 宋焰琴
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

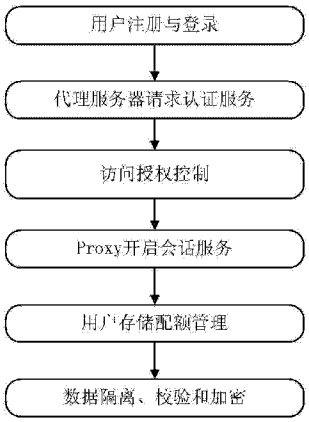
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种基于会话管理服务器的云存储系统的安全管理方法

(57)摘要

本发明公开了一种基于会话管理服务器的云存储安全管理方法，包括下列步骤：1. 用户注册与登录；2. 代理服务器请求认证服务；3. 访问授权控制；4. Proxy 开启会话服务；5. 用户存储配额管理；6. 数据隔离、校验和加密。采用本方法提出的方法，用户可以从云存储系统全局状态安全管理和保护数据，通过会话管理服务器，与数据库之间建立对用户信息以及文件系统信息的同步更新与查询，支持多用户的访问与授权管理，优化用户信息的配额管理。另外，基于会话管理服务器的受损数据检查与隔离策略，完成云存储系统用户的数据保护和恢复功能，还可以通过数据完整性校验和可靠的加密机制，防止用户数据被篡改。



CN 103095720 A

1. 一种基于会话管理服务器的云存储系统安全管理方法，其包括下列步骤：

步骤 1：用户向会话管理服务器进行注册，并在注册成功后进行登录；

步骤 2：用户在登录时，向会话管理服务器提交认证请求；

步骤 3：会话管理服务器在接收到所述认证请求后，查看数据库中是否存在与所述认证请求相匹配的项，如果有则认证通过；

步骤 4：用户身份认证通过以后，会话管理服务器发送资源页面给用户；

步骤 5：用户通过所述资源页面访问文件系统服务器；Proxy 为用户的此次访问请求开启会话，会话管理服务器将该会话访问添加至会话列表中。

2. 如权利要求 1 所述的方法，其特征在于，步骤 1 具体包括：

步骤 11：用户通过客户端进行注册，并通过 Proxy 向会话管理服务器提交注册请求；

步骤 12：会话管理服务器接收到所述注册请求后，通过 Proxy 向用户返回注册成功或失败的消息；

步骤 13：用户在注册成功后，通过客户端进行登录。

3. 如权利要求 1 所述的方法，其特征在于，步骤 2 具体包括：

步骤 21：用户登录时，向 Proxy 提交登录请求；

步骤 22：Proxy 在接收到用户的登录请求后，通过名字服务转换器进行用户名称解析，还通过可插入认证模块用于用户登录信息的记录，然后向会话管理服务器提交认证请求。

4. 如权利要求 1 所述的方法，其特征在于，步骤 3 具体包括：

步骤 31：会话管理服务器接收到所述认证请求后，对所述认证请求包含的请求内容进行摘要加密；

步骤 32：会话管理服务器根据所述加密后的摘要数据，查看数据库中是否存在与所述认证请求的请求内容相匹配的项，如果存在则认证通过，并向客户端返回用户信息。

5. 如权利要求 1 所述的方法，其特征在于，步骤 4 还包括：

步骤 41：当会话管理服务器发送资源页面给用户后，用户修改个人信息；

步骤 42：当用户提交修改后的个人信息后，系统管理员定义和修改用户的身份和权限，或删除用户信息并强制在线用户退出。

6. 如权利要求 1 所述的方法，其特征在于，步骤 5 具体包括：

步骤 51：用户接收到所述资源页面后，通过 Proxy 向会话管理服务器发送文件系统服务器的访问操作请求；

步骤 52：会话管理服务器接收到所述访问操作请求后，确定用户是否具有相应的操作权限；

步骤 53：在用户具有相应的操作权限时，会话管理服务器发送授权信息给 Proxy；

步骤 54：Proxy 接收到所述授权信息后，为用户的此次访问操作请求开启会话，并且将该会话发送给会话管理服务器；

步骤 55：会话管理服务器记录将该会话记录在会话列表中，并建立用户与文件系统服务器之间的连接。

7. 如权利要求 1 所述的方法，其特征在于，该方法还包括：系统管理员通过会话管理服务器调整用户存储空间，并根据用户提交的敏感或受损数据信息，查询并处理敏感数据和受损数据，对数据进行加密管理。

8. 如权利要求 1 所述的方法，其特征在于，该方法还包括 ：用户在通过身份认证请求以后，通过会话管理服务器发送的资源页面提交敏感数据或受损数据信息。

9. 如权利要求 1 所述的方法，其特征在于，该方法还包括用户权限列表的维护，具体包括 ：系统管理员通过 Proxy 向会话管理服务器发送用户权限更新事件，若是权限添加事件，则会话管理服务器将权限信息添加至权限列表中，若是权限回收事件，则会话管理服务器将权限信息从权限列表中删除。

10. 如权利要求 8 所述的方法，其特征在于，用户提交受损数据信息的具体过程包括 ：当用户发现数据被损坏时，通过 Proxy 发送受损数据事件处理请求 ；Proxy 根据接收到的所述受损数据事件处理请求，进行相应地受损数据处理。

11. 如权利要求 10 所述的方法，其特征在于，Proxy 对接收到的受损数据进行相应的处理具体包括 ：

对于受损数据隔离事件，Proxy 则解析所要隔离的目标地址和隔离目录信息，并将解析出的隔离目标地址和隔离目录信息发给会话管理服务器，如果会话管理服务器允许隔离操作，则 Proxy 对文件系统中的所述隔离目标地址和隔离目录信息对应的数据进行隔离操作，并更新内存信息 ；

对于受损数据恢复事件，Proxy 则解析数据恢复目标地址和恢复目录信息，并将解析出的恢复目标地址和恢复目录信息转发给会话管理服务器，如果会话管理服务器允许恢复操作，则 Proxy 对文件系统中的恢复目标地址和恢复目录信息对应的受损数据进行完整性恢复，并根据数据恢复指令更新内存 ；

对于受损数据查询事件，Proxy 接收所述受损数据查询请求，从内存中获得受损数据的相关信息，直接返回给 GUI 客户端。

对于受损数据检查事件，Proxy 接收所述受损数据检查请求，根据内存中的受损数据信息，对文件系统中的受损数据进行完整性检查。

一种基于会话管理服务器的云存储系统的安全管理方法

技术领域

[0001] 本发明涉及云存储系统的安全管理技术领域，涉及一种基于会话管理服务器的云存储系统的安全管理方法。

背景技术

[0002] 由于云存储系统规模的巨大性、开放性和复杂性等特点，一旦其遭受恶意攻击，将会带来严重的信息安全事故。云存储系统带来极大便利和效益的同时，也引发了用户信息泄露、系统数据破坏和被滥用等安全问题，因此，云存储系统的安全管理方法就显得尤为重要。

[0003] 2009 年，云安全联盟 (Cloud Security Alliance，CSA) 发布了《云计算关键领域安全指南》，主要从攻击者角度归纳了云存储环境可能面临的主要威胁，着重总结了云存储的技术架构模型、安全控制模型以及模型之间的映射关系，从用户角度阐述了可能存在的商业隐患、安全威胁，以及推荐采取的安全措施。此外，Google 的 Hadoop 平台能够建立一个高度容错的分布式文件系统，能够安全管理各种文件，同时还支持 PB 级的大文件安全存储方法，但是仅限于文件级的保护，缺少对于系统的全局管控 ；Sun 公司发布的开源云计算安全工具可为 Amazon 的 EC2、S3 以及虚拟私有云平台提供安全保护。为 Amazon EC2 设计的安全增强软件 VMIs，包括非可执行堆栈，加密交换和默认情况下启用审核等 ；云安全盒 (cloud safety box) 能够自动对内容进行压缩、加密和拆分，简化云中加密内容的管理等，其重点在于数据的加密管理。虽然诸多组织和公司意识到了云存储系统安全的重要性，也开展了相关工作，但是针对用户数据的安全管理，特别是对于云存储系统的全局管理，缺乏有效可靠的解决方案。现有的云存储系统管理方法存在以下不足 ：1、缺少对特定身份的认证服务，授权访问和控制权限机制不完善 ；2、未能部署云存储系统全局状态管理模块 ；3、用户数据容易被篡改 ；4、未能满足授权后的用户信息和数据访问与数据库之间的同步更新需求。

[0004] 因此，设计一种既能满足用户数据的安全组织与管理，又能从云存储系统全局状态对数据进行高可靠管理的方法，就显得相当必要了。

发明内容

[0005] 本发明提出一种基于会话管理服务器的云存储系统的安全管理方法，能够从云存储系统的全局状态安全管理用户数据。会话管理服务器负责云存储系统各代理服务器之间以及与其他组件的交互，为用户和管理者提供数据信息的查询端点，能够对用户的摘要信息进行加密管理，对受损数据进行隔离与查询，对客户端的授权对象实施下发策略。会话管理服务器与数据库之间建立对用户信息以及文件系统信息的同步更新。为了查询数据库中多用户的配额属性，会话管理服务器将云存储系统所有节点的状态保持在分布式文件系统中，对系统各节点状态的更新信息会传输到文件系统服务器中。

[0006] 会话管理服务器的管理策略更注重安全性和可靠性，当用户通过客户端访问文件

系统时，会话管理服务器会通过 MYSQL 数据库获取用户信息，并转发访问请求；大量的失败请求、敏感数据、受损数据信息以及验证信息也经由会话管理服务器处理。会话管理服务器还负责数据库用户信息的管理与更新。

[0007] 本发明提出的基于会话管理服务器的云存储系统安全管理方法，其包括下列步骤：

[0008] 步骤 1：用户向会话管理服务器进行注册，并在注册成功后进行登录；

[0009] 步骤 2：用户在登录时，向会话管理服务器提交认证请求；

[0010] 步骤 3：会话管理服务器在接收到所述认证请求后，查看数据库中是否存在与所述认证请求相匹配的项，如果有则认证通过；

[0011] 步骤 4：用户身份认证通过以后，会话管理服务器发送资源页面给用户；

[0012] 步骤 5：用户通过所述资源页面访问文件系统服务器；Proxy 为用户的此次访问请求开启会话，会话管理服务器将该会话访问添加至会话列表中。

[0013] 本发明的显著效果在于：

[0014] 本发明提供对云存储系统全局状态的管理以及与其他组件的操作交互，与数据库之间建立对用户信息以及文件系统信息的同步更新与查询，支持多用户的访问与授权管理，优化用户信息的配额管理。

[0015] 本发明针对云存储系统的安全性提出更可靠的安全管理策略，不仅提供身份与认证服务，还支持查看、浏览与检索用户登录情况功能，管理员可以在线强制用户退出当前的应用登录，确保云存储系统的安全性。本发明的受损数据处理采用多用户数据隔离策略，完成云存储系统用户的数据保护和恢复功能，检查并隔离受损数据。此外，本发明提供端到端的数据完整性校验，防止数据被篡改，并提供高可靠的数据加密机制。

附图说明

[0016] 图 1 是本发明的基于会话管理服务器的云存储系统架构图；

[0017] 图 2 是本发明的基于会话管理服务器的安全管理方法的总体流程图；

[0018] 图 3 是本发明的云存储系统权限列表维护流程图。

[0019] 图 4 是本发明的会话管理服务器会话处理流程图。

[0020] 图 5 是本发明的会话管理服务器的受损数据处理流程图。

具体实施方式

[0021] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本发明进一步详细说明。

[0022] 图 1 是基于会话管理服务器的云存储系统架构图。如图 1 所示，云存储系统包括 GUI 客户端、代理服务器、会话管理服务器和底层的分布式文件系统 moosefs（简称 MFS）。其中代理服务器包括：Proxy，其用于用户的分级管理，设置不同的访问权限，在客户端和文件系统之间起到中转作用；名字服务转换器 NSS，其用于数据资源配置定位问题，提供了多种常见的配置数据库和名称解析机制的来源；可插入认证模块 PAM，其用于提供会话的管理和记录，将系统提供的服务和该服务的认证方式分开，灵活地提供认证管理；文件系统服务器，其用于分布式文件系统的配置、调度与管理。所述会话管理服务器包括：会话管理模块

和 MYSQL 数据库。会话管理服务器的管理策略更注重安全性和可靠性，当用户通过客户端访问所述分布式文件系统 MFS 时，会话管理模块会通过 MYSQL 数据库获取用户信息，并转发访问请求给所述分布式文件系统；大量的失败请求、敏感数据、受损数据信息以及验证信息也经由会话管理服务器处理。会话管理服务器的主要功能可以总结为：查询信息，处理失败请求，中转对象。

[0023] 图 2 是本发明的基于会话管理服务器的安全管理方法的总体流程图。如图 2 所示，本发明所述的基于会话管理服务器的云存储系统安全管理方法，包括下列步骤：

[0024] (1) 用户注册与登录。

[0025] 会话管理服务器实现统一的用户身份服务，实现系统的用户、角色和组织机构统一化管理。用户注册与登录的详细步骤如下：

[0026] (1-1) 用户通过 GUI 客户端注册专有账号，并通过 Proxy 向会话管理服务器提交注册申请，GUI 客户端与代理服务器之间采用 SSH2/SFTP 作为安全认证协议，会话管理服务器接收到注册申请后将向用户返回注册成功与失败的信息。

[0027] (1-2) 注册成功后，用户通过 GUI 客户端进行登录，在登录的过程中要输入用户的相关信息，包括用户名和密码，并通过 Proxy 转发给会话管理服务器，会话管理服务器收到登录请求之后，对用户登录信息进行认证。

[0028] (2) 代理服务器请求认证服务

[0029] 用户的登录操作需要代理服务器向会话管理服务器发送认证请求，详细步骤包括以下几步：

[0030] (2-1)Proxy 在接收到用户登录请求后，通过名字服务转换器 NSS 和可插入认证模块 PAM，向会话管理服务器提交认证请求，包括身份、权限等。其中，名字服务转换器 NSS 用于完成用户名称解析，以便会话管理服务器在 MYSQL 数据库中查询用户姓名、权限、身份等信息；可插入认证模块 PAM 用于记录用户的登录请求，便于向会话管理服务器添加可靠的认证方式。

[0031] (2-2) 会话管理服务器在接收到认证请求后，先对认证请求的内容（身份、权限等）进行摘要加密，如可以使用 Openssl 中的算法 3AES。

[0032] (2-3) 会话管理服务器根据加密后的摘要数据，查询 MYSQL 数据库，如用户表 user_table，看数据库中是否有匹配项，如果有则通过认证请求，并向 GUI 客户端返回用户成功登录的信息。

[0033] (3) 访问授权控制

[0034] 当用户通过身份认证后，会话管理模块会通过文件系统服务器发送资源页面到用户 GUI 客户端，用户可以修改个人信息，还可以通过 Proxy 向会话管理服务器发送文件系统的操作请求，若用户具有文件系统操作权限，则会话管理服务器允许该操作请求，否则拒绝操作请求。会话管理服务器将操作请求的授权信息以一组随机生成的序列向对应的 Proxy 发送，并允许相连的 GUI 客户端访问分布式文件系统服务器。

[0035] 会话管理服务器提供统一的，可以扩展的权限管理及接口，支持用户权限列表维护操作，能够定义管理多种权限级别策略；系统管理员还可以查看、浏览与检索用户登录信息，并强制在线用户退出当前的应用。

[0036] (4)Proxy 开启会话服务

[0037] Proxy 能够为用户启动会话。当用户通过访问授权后，可以再次发起会话请求，Proxy 通过会话管理模块将其添加到会话列表中并与文件系统服务器建立连接，开启会话服务，用户可以通过文件系统服务器实现分布式文件系统的数据存储和资源信息查询功能；会话服务处理完成后，Proxy 将查询结果返回给会话服务对应的 GUI 客户端。

[0038] 会话管理服务器支持包括用户数据、敏感数据、受损数据的查询，保护数据的安全性，并且及时更新数据库中的数据表信息。

[0039] (5) 用户存储配额管理

[0040] 通过会话管理服务器，系统管理员可以查询各个用户的空间信息，包括存储的配额、已使用的空间等。同时，系统管理员可以通过会话管理服务器删除用户的信息（用户表、授权表等）、调整服务器上的配额数据库。

[0041] (6) 数据隔离、校验和加密

[0042] 会话管理服务器能够实现多用户数据隔离、校验和加密功能，完成共享虚拟化资源池的数据保护功能。代理服务器将文件系统的受损数据信息转发给会话管理服务器，存入 MYSQL 数据库（受损数据表：用户名，路径），会话管理服务器要将隔离数据信息（包括数据表、大小、位置、）通知到其它的 Proxy，并更新内存信息；数据校验（防篡改）模块提供端到端的数据完整性校验，防止数据被篡改；数据加密模块提供具有对敏感数据进行加密的数据加密机制，采用 3AES 加密算法。图 3 是本发明的云存储系统权限列表维护流程图。图 3 进一步解释了图 2 访问授权控制中的用户权限列表维护操作和多权限级别策略，如图 3 所示，会话管理服务器在访问授权控制中，支持用户权限列表维护，具体操作步骤如下：

[0043] (1) 当系统管理员更新用户权限时，可以通过 Proxy 向会话管理服务器发送用户权限更新事件，会话管理服务器判断权限更新类型，权限更新类型包括权限添加和权限回收两种。

[0044] (2) 若权限更新类型是权限添加事件，则会话管理服务器将权限信息添加至 MYSQL 数据库的权限列表；若是权限回收事件，则会话管理服务器将权限信息从 MYSQL 数据库的权限列表删除。

[0045] (3) 文件系统服务器接收 GUI 客户端刷新事件，并向客户端返回最新文件系统信息。

[0046] 图 4 是本发明的会话管理服务器会话处理流程图。如图 4 所示，会话管理服务器会维护一个会话列表 (Session List)。当一个新的访问请求到达时，将增加新的会话服务，并添加到会话列表里面，如果之后还有查询或修改数据的请求到达，会话管理服务器就从会话列表中查找该请求对应的会话服务，处理数据查询或修改请求，完成后将结果返回给会话服务对应的客户端。

[0047] 图 5 是本发明的会话管理服务器的受损数据处理流程图。受损数据处理为云存储系统提供了可靠的安全管理方法，包括受损数据隔离、受损数据恢复、受损数据查询和受损数据检查四个方面，操作步骤如下：

[0048] (1) 当用户发现数据被损坏时，可以通过 Proxy 代理发送受损数据信息及事件处理类型。

[0049] (2)Proxy 判断若为受损数据隔离事件，则解析 GUI 客户端的隔离目标地址和隔离目录信息，并将该隔离信息转发给会话管理服务器，如果会话管理服务器允许隔离操作，则

Proxy 对文件系统中的数据进行隔离操作并更新内存信息，之后向 GUI 客户端返回成功信息。

[0050] (3) 若为受损数据恢复，则 Proxy 解析 GUI 客户端的数据恢复目标地址和恢复目录信息，并将该恢复信息和恢复目录信息转发给会话管理服务器，如果会话管理服务器允许恢复操作，则 Proxy 对文件系统中的受损数据进行完整性恢复，并根据数据恢复指令更新内存，之后向 GUI 客户端返回成功信息。

[0051] (4) 若为受损数据查询，则 Proxy 接收 GUI 客户端的受损数据查询请求，从内存中获得受损数据的相关信息，返回给 GUI 客户端。

[0052] (5) 若为受损数据检查，则 Proxy 接收 GUI 客户端的数据检查请求，之后根据内存中的受损数据信息，对文件系统中的受损数据进行数据完整性检查。

[0053] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

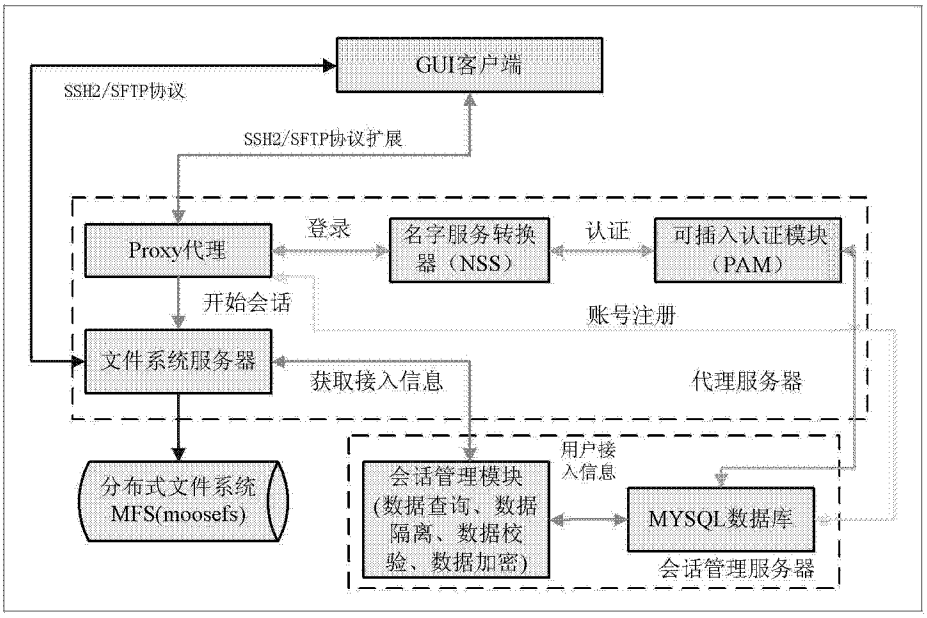

GUI客户端
SSH2/SFTP协议
SSH2/SFTP协议扩展
Proxy代理
登录
名字服务转换器（NSS）
认证
可插入认证模块（PAM）
开始会话
账号注册
文件系统服务器
获取接入信息
代理服务器
分布式文件系统MFS(moosefs)
会话管理模块(数据查询、数据隔离、数据校验、数据加密)
用户接入信息
MYSQL数据库
会话管理服务器

图 1

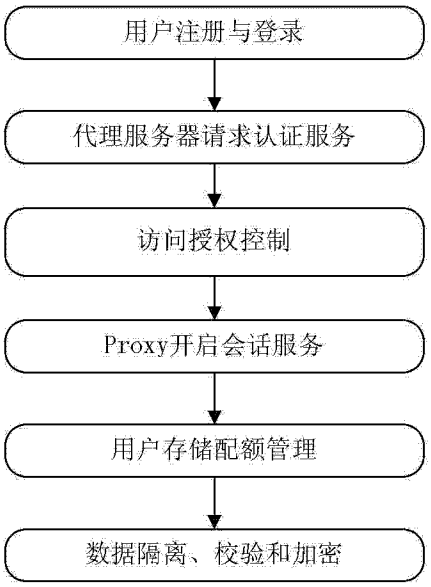

用户注册与登录
代理服务器请求认证服务
访问授权控制
Proxy开启会话服务
用户存储配额管理
数据隔离、校验和加密

图 2

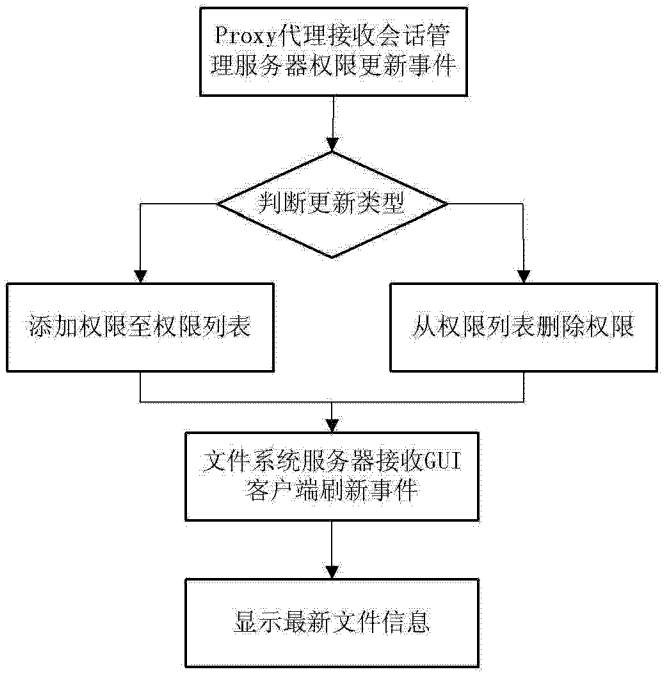

Proxy代理接收会话管理服务器权限更新事件
判断更新类型
添加权限至权限列表
从权限列表删除权限
文件系统服务器接收GUI客户端刷新事件
显示最新文件信息

图 3

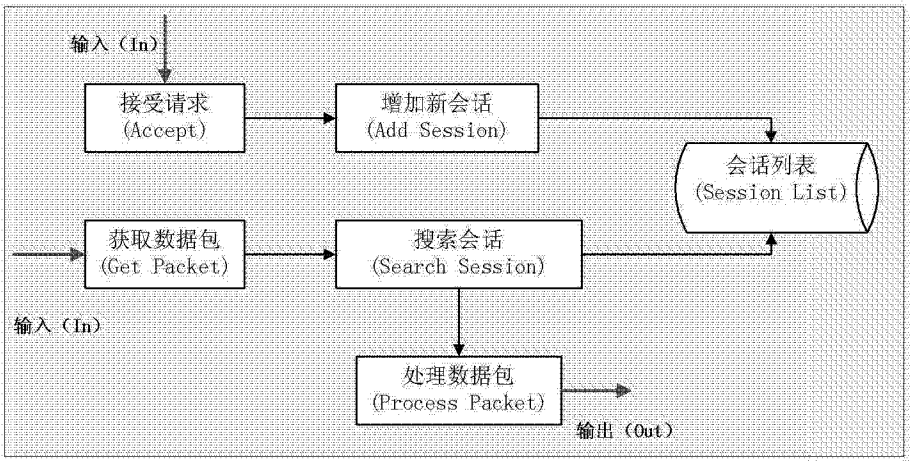

输入（In）
接受请求
(Accept)
增加新会话
(Add Session)
会话列表
(Session List)
获取数据包
(Get Packet)
搜索会话
(Search Session)
输入（In）
处理数据包
(Process Packet)
输出（Out）

图 4

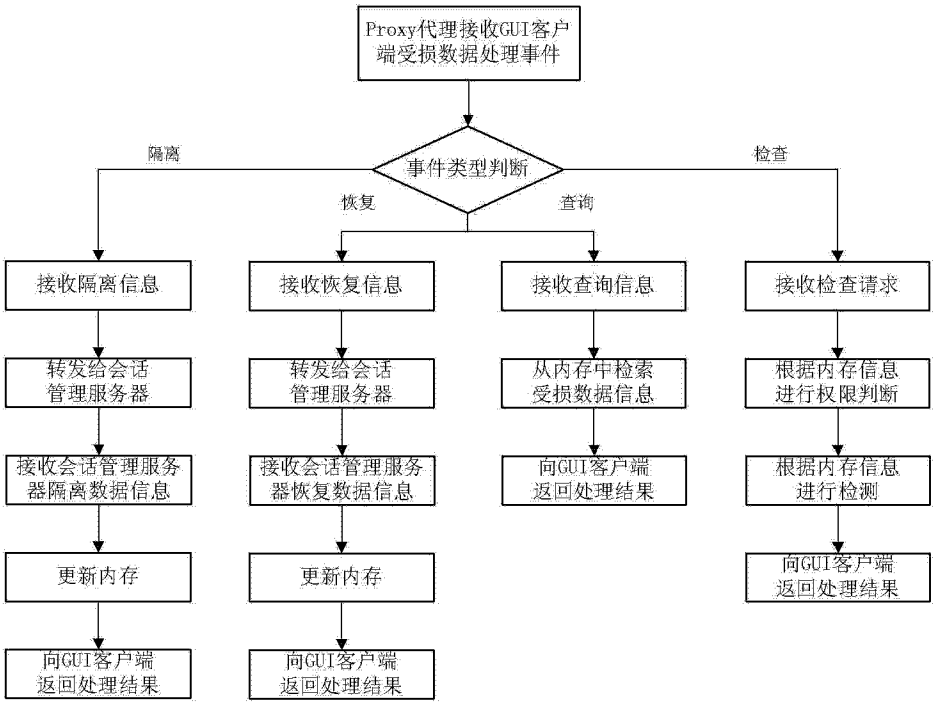

Proxy代理接收GUI客户端受损数据处理事件
事件类型判断
隔离
恢复
查询
检查
接收隔离信息
转发给会话管理服务器
接收会话管理服务器隔离数据信息
更新内存
向GUI客户端返回处理结果
接收恢复信息
转发给会话管理服务器
接收会话管理服务器恢复数据信息
更新内存
向GUI客户端返回处理结果
接收查询信息
从内存中检索受损数据信息
向GUI客户端返回处理结果
接收检查请求
根据内存信息进行权限判断
根据内存信息进行检测
向GUI客户端返回处理结果

图 5