文章编号:1671-4598(2018)05-0242-03 DOI:10.16526/j.cnki.11—4762/tp.2018.05.060 中图分类号:TP309 文献标识码:A

云计算存储数据安全访问控制机制研究

张雪亚
(宝鸡文理学院,陕西 宝鸡 721016)

摘要:传统控制机制存在角色分配不合理、加密解密时间耗费长、用户不能安全访问等问题,提出研究一种云计算存储数据安全访问控制机制;根据角色加密原理,构建角色加密混合云存储框架,为了更好访问子系统中各个模块,对用户可信度与行为监控进行分析,以此实现动态监控访问控制机制;通过实验验证可知,该机制能够有效进行角色分配,并对加密、解密和用户访问进行准确控制。

关键词:云计算;存储数据;安全访问;控制机制

Research on Secure Access Control Mechanism of Cloud Computing Storage Data

Zhang Xueya
(Baoji University of Arts and Sciences, Baoji 721016, China)

Abstract: Traditional control mechanisms include irrational role allocation, long time of encryption and decryption, and users can not access safely. According to the role encryption principle, a role encryption hybrid cloud storage framework is built. In order to better access each module in the subsystem, we analyze the user credibility and behavior monitoring, in order to achieve the dynamic monitoring access control mechanism. The experimental verification shows that the mechanism can effectively allocate the role and control the encryption, decryption and user access accurately.

Keywords: cloud computing; storage data; secure access; control mechanism

0 引言

“云计算”这一词汇是在2016年由谷歌浏览器首次提出的,一直保持着迅猛发展的势头,并逐渐被人们所熟知,不同行业所积累的数据全部存储在云端中,促使云计算得到了广泛应用,不管是地方企业还政府部门,都希望存储在云端的数据具有安全性,并拥有足够大的内存空间供数据存储,其灵活的管理方式也受到人们的青睐,但是,在近几年,大多数用户都出现了数据丢失、被盗等安全问题。云存储结果一般有两种,分别是公共云和私有云,公共云采取付费方式为用户提供服务,而私有云只有通过群体或组织才可获取资源,安全与可靠性较强,但是存在资源封锁,不能共享的缺点,为此,如何提高云存储安全性问题,成为了当下人们热烈讨论的话题[1]。

根据云存储安全重要性,采用传统控制机制可临时保护数据存储安全,但是随着时间增加,存在角色分配不合理、加密解密时间耗费长、用户不能安全访问等问题[2]。基于此,提出面向云计算数据存储方式的安全访问控制机制研究。该机制融合角色访问控制原理,构建安全的混合云存储框架,在角色加密原理基础上,实现动态监控访问整体控制,并通过实验验证可知,该机制能够有效进行角色分配,同时对加密、解密和用户访问有效控制,实用性较强。

收稿日期:2018-03-01; **修回日期**:2018-03-27。

基金项目:陕西省教育厅科学研究计划项目(16JK1045);宝鸡市科技计划工业公关项目(14GYGG-4);宝鸡文理学院科学研究重点项目(ZK14083)。

作者简介:张雪亚(1980-),女,陕西咸阳人,硕士研究生,讲师,主要从事云计算、大数据分析、软件测试技术方向的研究。

1 安全访问控制机制原理

基于云计算的存储数据安全访问控制机制原理中,最关键的是角色加密原理,然后在该原理基础上构建角色加密混合云存储框架,由此构成了面向云计算数据存储方式的安全访问控制机制,安全访问控制机制基本原理如图1所示。

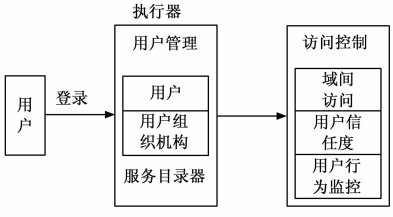


图1 安全访问控制机制原理图

1.1 角色加密过程设计

对于不同用户进行访问控制,其基本原理是基于角色加密模式对其进行控制,按照构建→推理→管理→用户增加→用户撤销→加密解密过程实现的,具体描述如下所示。

1.1.1 构建

当用户访问时,系统会随机产生:①三个群,分别是W_1、W_2、W_3;②一个双线性的映射$W_1 \times W_2 \rightarrow W_3$;③两个生成元:$a \in W_1$、$b \in W_2$;④两个秘密值:$g$、$h$;⑤两个函数。此时的主密钥和系统密钥都会被重新赋予定义来满足不同用户在不同角色层次中所表达的深度含义,以此信息作为因素,构建加密环境[3]。

1.1.2 推理

当访问ID得到确认后,用户的身份也得到了验证,计算系统用户密钥,将其设置为自己特有的密钥,用于对重要数据

的加密；经过身份验证后的系统管理者还可计算用户特有的密钥，计算完成后再次传输给用户，进行角色推理。

1.1.3　管理

设用户 P 的身份为 ID_P，XP_P 表示后代角色所有身份的集合，在该层次中，如果需要对用户 P 进行角色放置，验证身份 ID_P 是否在 XP_P 集合当中，并利用云计算方式，将所有数据组发布，供用户自行管理。

1.1.4　用户增加操作

如果用户 P_i 的角色管理者想要增加一个用户的身份认证，那么该身份认证就是 P_i 的 n 个用户集合，角色管理者立刻将此集合信息发送给云端，当云端接收到集合信息后，开始计算参数，并将结果返回给角色管理者。

1.1.5　用户撤销操作

为了将角色从用户记录中撤销，需假设一个角色管理者集合，其中包括 n 个用户数据，角色管理者首先从集合中去除一个身份认证 ID，并将 ID 发送至云端，当云端接收到用户身份认证信息后，计算参数，然后将参数传送至角色管理者，管理者可完成用户的撤销[4]。

1.1.6　加密过程设计

假设用户相对私密信息进行加密，系统需根据角色集合，将用户拥有的全部数据随机选择，然后设置参数，计算百分比，计算结束后，用户使用百分比机制对数据进行加密，并将密文发送至云端。

1.1.7　解密过程设计

针对任何一个角色集合，数据都是被加密的，集合拥有一个祖先角色集合，想要对集合进行解密，那就需要对祖先角色集合解密。假设用户想对密文 C 解密时，需从云端中将数据提取出来接收密文，为此，需向云端发送密文请求[5]。当云端接收到请求信号后，将加密信息传送给用户，用户开始解密，首先需计算密文参数，然后再恢复系统加密密钥，用户通过使用该密钥就可完成解密。

1.2　混合云存储架构设计

根据角色加密原理，构建面向云计算的数据存储结构，该结构是由私有云和公共云共同组成的，在混合模式下的私有云可对敏感信息进行存储，比如用户身份信息和会员信息；公共云可对实际数据进行存储，并进行加密处理，公共云可与用户进行数据共享，具体混合云存储结构如图 2 所示。

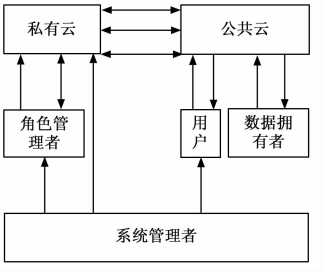


图 2　角色加密混合云存储框架

由图 2 可知：该存储架构主要是由私有云、公共云、角色管理者、用户、数据拥有者、系统管理者组成的，系统管理者主要负责对相关文件授权、产生相应参数、分发凭证、层次结构管理、角色适应、信息存储，一旦出现角色层次结构变化情况时，管理者需将参数进行更新，进行更新后的参数将全部存储在私有云中，用户可对公共云的数据进行分享，当用户身份信息经过检验后，会被赋予一个新的密钥，经过管理员动态监测与验证，可实现公共云的数据分享，但是数据持有者可随时处理数据，并将处理后的数据加密，存储在公共云中[6]。按照基于角色控制原理，数据持有者可规范用户访问数据的次数，并在进行数据处理时进行加密，加密后的数据是不允许在私有云中进行共享的。将管理者的职责进行重新划分，严格管理角色与用户之间的关系，并使用参数来表示，由于参数是不能被定义的，为此将参数转化为概念形式存储在私有云中，如果这些定义出现在用户访问首页时，那么该用户具有访问权力；如果没出现，说明该用户不具有访问权力[7]。管理者不需要了解用户更新信息，只需将结果存储在私有云中，在对用户赋予新角色之前，管理者从私有云中提取信息对用户身份进行验证。基础设备提供方主要是由公共云扮演的，主要负责对用户数据进行加密传输，未经过授权的用户是没有权利对空间进行访问的，因为其缺少密钥，无法对已经加密的空间数据进行解密。私有云将全部数据堆积在中心内部，并由特定程序进行管理与操作，其作用是对重要和可信度高的用户角色信息进行存储[8]。由于用户不能对私有云信息进行直接操作，为此只有减少没有经过授权的用户对私有云的非法入侵才能保证数据的安全。

1.3　访问控制子系统

访问控制子系统的控制机制为：角色用户在登录平台之后，系统需根据用户信用情况来确定是否具有访问资源的权限，如果未经过授权，那么界面显示无法登录，如果经过授权，那么界面显示显示登录成功，用户可对资源进行访问并操作[9]。在操作过程中，由于系统会对用户行为进行实时监测，计算用户的可信度，如果用户可信度不能满足要求，那么系统将迫使用户停止操作，并强制退出程序。每一次操作完成后，子系统会根据用户可信度进行综合评价，判定用户下一次访问是否具有权力。

为了更好访问子系统中的各个模块，需对用户可信度与行为监控进行分析：

1）初始可信度：用户在首次访问时，系统会根据用户以往的信用记录计算出一个可信度，即为默认的初始可信度。

2）行为可信度加权：根据用户访问数据的行为进行分级，判断不同用户访问系统的不同等级，将获取的用户可信度作为因子，计算行为可信度加权来保证用户数据的安全访问。

3）用户操作监控时间：针对用户监控的操作时间间隔是为了更好对用户进行动态监测来保证系统的安全性，系统会根据用户操作行为分等级来计算时间间隔。

4）实时可信度：当用户对数据进行访问时，通过等级的划分来规范用户操作权限，由此可修改用户可信度。

5）用户最终可信度：在每次用户完成数据资源访问后，系统需根据历史记录对用户可信度进行分析，如果不是本地操作，那么需重新计算用户的可信度，并记录，为用户下一次访问缩短验证时间。

6）用户可信度：通过对用户信任度阈值验证后，利用访问机制计算用户可信度值，并以该值作为判断是否具有登录权限的标准之一。

7）历史可信度：记录当前用户所有的可信度值，为最终可信度值提供计算数据，当完成计算后，用户的最终可信度值

会被赋予新的信用状态。

2 动态监控访问控制机制的实现

结合访问子系统中的各个模块特征来实现动态监控访问控制机制，具体的访问操作流程如下所示：

1）①登录系统；②用户认证，获得角色和权限，由此获取用户初始信用度；③判断用户可信度是否满足阈值范围，如果满足则对资源进行直接方位；如果不满足则被强迫退出访问[10]。

2）①域间访问控制子模块；②用户信任度计算；③判断两条用户信用度是否在阈值范围内，如果在，则需进行监控；如果不在，则需计算用户最终信用度。

3）①用户行为监控子模块；②判断用户可信度是否存在恶意行为，如果存在，则需计算用户最终信用度；如果不存在，需进行监控。

4）将步骤 2）和 3）中的监控数据传输到 1）中的用户直接访问操作步骤当中，实现用户的动态访问。

由上述流程可知：当用户填写用户名和密码后可成功登陆系统，此时的系统会赋予用户新的角色和权限，用于对秘密资源的访问，此时的命令已经被下达到各个资源核心处。系统会判断用户可信度是否满足访问阈值范围，如果不满足，那么用户将没有权限访问，如果满足，那么用户具有权力进行访问。在用户操作的过程中，系统需同时监控用户行为、用户可信度和初始的可信度，其中用户行为是在所有监控子模块中的行为，会实时判断用户是否存在恶意的行为，如果存在，可直接强制用户停止访问，并退出系统登录；如果不存在，那么继续监控。用户可信度的计算子模块会被同步到用户登录的界面，用于对可信度的实时查询，并进行动态监控。监控时间长短是由用户行为所决定的，计算用户实时信用度可预防用户历史操作中的可信度累计被故意抬高的不安全现象发生。每次对用户可信度子模块进行计算时，都会进行一次判断，如果可信度满足要求，则需继续操作，如果不满足，那么结算用户最终可信度，并强制退出系统。用户对系统进行安全和访问操作之后，会获得最终用户可信度，由此可完成动态监控的访问控制。

3 实验

进行实验验证云计算存储数据安全访问控制机制的可信性，并根据实验内容对实验结果展开分析。

3.1 实验环境搭建

构建改进的云计算安全存储访问机制实验环境，需采用 JAVA 作为实验开发语言，Web 作为服务主要装置，将该装置放置于平台上，进行云端存储，利用 SQL 数据库作为实验开发数据库，从中选择实验数据，为客户端提供相应数据。将密钥镶嵌在该程序中，每一个机器都具有四个内核处理器以及 4GB 的随机存取存储器和两个 4800 软件包管理器硬盘，通过千兆以太网进行网络连接。以此为基础，采用非对称性的线群输入不同参数，作为实验密码库。

3.2 实验结果与分析

为了验证云计算存储数据安全访问控制机制的可信性，将传统控制机制与改进研究的控制机器可信度进行对比结果如下所示：

3.2.1 明文大小、角色多少和密文大小之间关系

选取明文大小分别为 200 字节、15 000 字节、50 000 字节，用户角色分别为 5、500 和 5 000，在该实验条件下，验证两种方法中明文大小、角色多少和密文大小之间关系来确定该方法是否具有可信度，结果如表 1 所示。

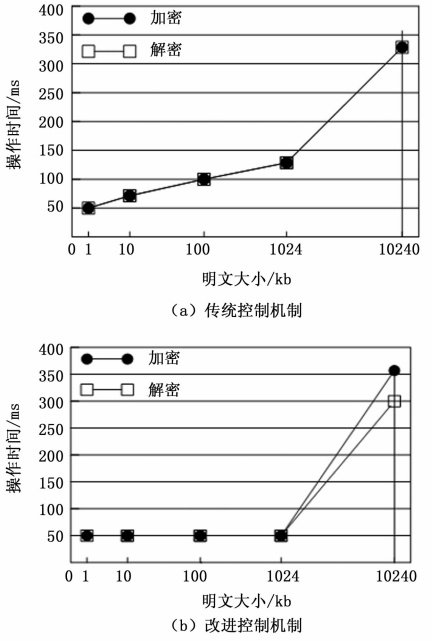
表 1 两种方法明文大小、角色多少和密文大小之间关系对比结果

明文大小	传统方法 用户角色			改进方法 用户角色		
	5	500	5000	5	500	5000
200	749	756	831	832	832	832
15000	16753	17920	18991	19837	19837	19837
50000	38512	38991	39143	40193	40193	40193

由表 1 可知：采用传统方法，密文大小随着明文和用户角色的增加逐渐变大；而采用改进方法，密文大小随着明文增多逐渐变大，具有线性关系，但不会随着用户角色增多与减少发生改变。由此可看出，改进方法可有效控制密文随着明文长短发生改变，不会受到任务数量影响而产生变化。

3.2.2 明文大小与控制机制所需时间关系

从 SQL 数据库中选取 5 个角色和 10 个普通用户，对文件进行加密，加密的时间是从对文件选择之后，电点击文件上传之前；而进行解密的时间是从用户接收到密文到将明文存储在磁盘中的过程，为此对加密与解密的明文大小与控制机制所需时间进行检验，结果如图 3（a）、（b）所示。



（a）传统控制机制

（b）改进控制机制

图 3 两种方法明文大小与控制机制所需时间对比结果

由图 3 可知：采用传统方法无论是加密时间还是解密时间都会随着明文的增打而逐渐增加；采用改进方法进行验证时，当明文大小小于等于 1 024 kb 时，加密和解密所耗费的时间不会发生改变。当名为大小大于 1 024 kb 时，加密和解密所耗费的时间会随着明文的增加逐渐变大，呈正比例关系。

3.3 实验结论

综合以上实验结果可得：在角色多少、密文大小和明文大小三个方面，传统方法不如改进方法控制效果好，密文大小具

（下转第 248 页）