(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103107995 B
(45)授权公告日 2015.11.25

(21)申请号 201310048802.5

(22)申请日 2013.02.06

(73)专利权人 中电长城网际系统应用有限公司
地址 100191 北京市海淀区学院路甲38号长城电脑大厦A501

(72)发明人 张雅哲 王艳霞 张大鹏

(74)专利代理机构 北京海虹嘉诚知识产权代理有限公司 11129
代理人 李翀

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 101784045 A,2010.07.21, 全文.
CN 102075542 A,2011.05.25, 全文.
JP 5164029 B2,2012.12.28, 全文.
US 20120328105 A1,2012.12.27, 全文.

审查员 谭美玲

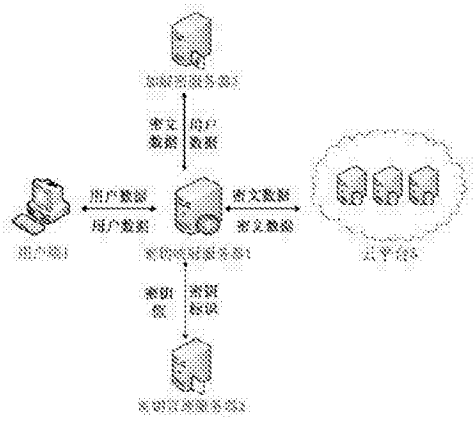
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种云计算环境数据安全存储系统和方法

(57)摘要

本发明涉及一种云计算环境数据安全存储系统和方法，它包括分别连接密钥映射服务器并与密钥映射服务器进行数据交换的密钥管理服务器、加解密服务器、用户端和云平台；通过密钥映射服务器保存和维护密钥和加密数据的映射关系，打破密钥值和密文数据之间的直接联系。当数据存储地址发送给用户端后，或用户数据发送给用户端后，密钥映射服务器删除密钥值、用户数据和密文数据；加解密服务器完成加密或解密后，删除密钥值、用户数据和密文数据。这样就使保存密钥映射关系的位置不会同时存在密钥值和密文数据，保存密文数据的位置不会同时存在密钥值和密钥映射关系，保存密钥值的位置不会同时存在密钥映射关系和密文数据，达到密钥值、密文数据、密钥映射关系的三方独立性。



CN 103107995 B

1. 一种云计算环境数据安全存储系统，其特征在于：它包括分别连接密钥映射服务器并与所述密钥映射服务器进行数据交换的密钥管理服务器、加解密服务器、用户端和云平台；所述用户端向所述密钥映射服务器提出存储请求或数据请求，所述存储请求包括用户标识和用户数据，所述数据请求包括用户标识和由所述云平台返回的数据存储地址；所述密钥映射服务器根据所述存储请求生成密钥标识，所述密钥管理服务器中生成与所述密钥标识对应的密钥值；所述密钥映射服务器根据所述数据请求分别由所述云平台和密钥管理服务器中获取密文数据和密钥值；所述加解密服务器根据所述密钥值将所述用户数据加密成密文数据，或根据所述密钥值将所述密文数据解密成所述用户数据，完成加密或解密后，删除所述密钥值、用户数据和密文数据；

所述密钥映射服务器中储存所述用户标识、密钥标识和数据存储地址的映射关系，所述密钥管理服务器中储存所述密钥标识和密钥值，所述云平台中储存所述密文数据。

2. 如权利要求 1 所述的一种云计算环境数据安全存储系统，其特征在于：所述密钥映射服务器用于使用所述密钥标识向所述密钥管理服务器提出密钥请求，接收所述密钥管理服务器生成的密钥值；或向所述加解密服务器输入所述密钥值和所述用户数据，所述加解密服务器将所述用户数据转换成密文数据，由所述密钥映射服务器将所述密文数据输入云平台中保存，所述云平台输出的数据存储地址返回所述用户端，所述密钥映射服务器中存储所述用户标识、密钥标识和数据存储地址的映射关系，删除所述密钥值、用户数据和密文数据；

或根据所述用户端的所述数据请求，向所述云平台输入所述数据存储地址，接收由所述云平台输出的与所述数据存储地址对应的所述密文数据；或根据与所述数据存储地址对应的所述密钥标识请求所述密钥管理服务器返回所述密钥值，将所述密文数据和所述密钥值一同输入所述加解密服务器，所述加解密服务器将所述密文数据转换成所述用户数据并返回所述用户端，所述密钥映射服务器删除所述密钥值、用户数据和密文数据。

3. 如权利要求 1 所述的一种云计算环境数据安全存储系统，其特征在于：所述云平台用于保存由所述密钥映射服务器输入的所述密文数据，向所述密钥映射服务器返回所述数据存储地址；或根据所述密钥映射服务器输入的所述数据存储地址查找对应的所述密文数据，向所述密钥映射服务器输出所述密文数据。

4. 如权利要求 1 或 2 或 3 所述的一种云计算环境数据安全存储系统，其特征在于：所述密钥标识为随机生成。

5. 如权利要求 1 或 2 或 3 所述的一种云计算环境数据安全存储系统，其特征在于：所述密钥映射服务器、密钥管理服务器和云平台相互独立。

6. 如权利要求 1 或 2 或 3 所述的一种云计算环境数据安全存储系统，其特征在于：所述密钥映射服务器和 / 或加解密服务器为集成于所述用户端本身的功能模块。

7. 一种云计算环境数据安全存储方法，它包括构建一云计算环境数据安全存储系统，包括分别连接密钥映射服务器并与所述密钥映射服务器进行数据交换的密钥管理服务器、加解密服务器、用户端和云平台；

其中，用户数据加密存储的步骤包括：

1）所述用户端将用户标识和用户数据传送至所述密钥映射服务器；

2）所述密钥映射服务器生成与所述用户标识对应的密钥标识，并接收由所述密钥管理

服务器生成的对应于所述密钥标识的密钥值，所述密钥管理服务器存储所述密钥标识和密钥值；

3）所述密钥映射服务器将所述密钥值和用户数据发送至所述加解密服务器将所述用户数据加密成密文数据；

4）所述云平台保存所述密文数据后将数据存储地址发送给所述用户端；

所述用户数据请求使用的步骤包括：

I）所述用户端将所述用户标识和数据存储地址传送至所述密钥映射服务器；

II）所述密钥映射服务器将所述数据存储地址输入所述云平台中检索并返回与所述数据存储地址对应的所述密文数据；

III）所述密钥映射服务器根据所述数据存储地址对应的所述密钥标识在所述密钥管理服务器中提取所述密钥值；

IV）所述密钥映射服务器将所述密文数据和密钥值一同输入所述加解密服务器中将所述密文数据解密成所述用户数据，并将所述用户数据返回所述用户端。

8. 如权利要求 7 所述的一种云计算环境数据安全存储方法，其特征在于：所述密钥映射服务器中储存所述用户标识、密钥标识和数据存储地址的映射关系；所述密钥管理服务器中储存所述密钥标识和密钥值，所述云平台中储存所述密文数据。

9. 如权利要求 7 所述的一种云计算环境数据安全存储方法，其特征在于：所述加解密服务器在完成加密或解密之后，删除所述密钥值、用户数据和密文数据。

10. 如权利要求 7 或 8 或 9 所述的一种云计算环境数据安全存储方法，其特征在于：将所述数据存储地址发送给所述用户端后，或将所述用户数据发送给所述用户端后，所述密钥映射服务器删除密钥值、用户数据和密文数据。

一种云计算环境数据安全存储系统和方法

技术领域

[0001] 本发明涉及一种信息安全系统和方法，具体涉及一种云计算环境数据安全存储系统和方法。

背景技术

[0002] 云计算是一种面向互联网的分布式计算服务，作为IT资源和服务的一种交付使用模型，它可以实现随时随地、便捷的、按需的从可配置计算资源共享池中获取所需的资源(如网络、服务器、存储、应用、服务等)，这些资源可以被迅速提供并发布，同时最小化管理成本或服务提供商的干涉。云计算是近年来IT界最热门的一个技术名词，很多专家认为，云计算会改变互联网的技术基础，甚至会影响整个产业的格局。目前，世界上几乎所有的IT产业巨头都投身于云计算的研究和应用产业中。

[0003] 当云计算系统运算处理的对象是海量数据的存储和管理时，云计算系统中就需要配置大量的存储设备，并将不同类型的存储设备通过软件集合起来协同工作，共同对外提供数据存储服务。这样，在用户看来，云计算系统的后端就是一个巨大的云平台，这个云平台被大量用户共享，用户所要做的事情就是往云平台中上传数据，而不用关心数据是如何存放的。但是，甲用户的私有数据很可能和乙用户的数据存放在同一个存储服务器上，甚至是同一个磁盘上。乙用户就有机会利用虚拟机窃取云平台中存储的数据，如果甲用户的数据是明文，那么甲用户的数据就难以得到保护，会被非法使用或修改，最终导致泄露。

[0004] 为了解决云平台中的数据安全问题，现有技术中典型的解决方案是采用加密技术对数据全文加密，将数据加密后存储至云平台。然而当涉及大量数据时，需要生成并维护管理大量的加解密密钥，由于密钥管理的专业性和复杂性，一些用户选择使用第三方提供的密钥管理服务。但是如果密钥管理方和云平台的提供方之间进行合谋攻击，用户的数据就得不到应有的保护。

发明内容

[0005] 本发明针对现有技术中在云计算环境中云计算环境尤其是云存储环境中存在的数据安全风险问题，提出了一种能够打破密钥和密文数据之间的联系，由第三方来维护密钥和密文数据的映射关系，在不依赖于云服务提供商以及密钥管理服务提供商可靠性的前提下，为使用云计算的用户提供数据机密性安全保护的云计算环境数据安全存储系统，及实现上述系统的云计算环境数据安全存储方法。

[0006] 本发明的技术方案如下：

[0007] 一种云计算环境数据安全存储系统，其特征在于：它包括分别连接密钥映射服务器并与所述密钥映射服务器进行数据交换的密钥管理服务器、加解密服务器、用户端和云平台；所述用户端向所述密钥映射服务器提出存储请求或数据请求，所述存储请求包括用户标识和用户数据，所述数据请求包括用户标识和由所述云平台返回的数据存储地址；所述密钥映射服务器根据所述存储请求生成密钥标识，所述密钥管理服务器中生成与所述密

钥标识对应的密钥值；所述密钥映射服务器根据所述数据请求分别由所述云平台和密钥管理服务器中获取密文数据和密钥值；所述加解密服务器根据所述密钥值将所述用户数据加密成密文数据，或根据所述密钥值将所述密文数据解密成所述用户数据，完成加密或解密后，删除所述密钥值、用户数据和密文数据；

[0008] 所述密钥映射服务器中储存所述用户标识、密钥标识和数据存储地址的映射关系，所述密钥管理服务器中储存所述密钥标识和密钥值，所述云平台中储存所述密文数据。

[0009] 所述密钥映射服务器用于使用所述密钥标识向所述密钥管理服务器提出密钥请求，接收所述密钥管理服务器生成的密钥值；或向所述加解密服务器输入所述密钥值和所述用户数据，所述加解密服务器将所述用户数据转换成密文数据，由所述密钥映射服务器将所述密文数据输入云平台中保存，所述云平台输出的数据存储地址返回所述用户端，所述密钥映射服务器中存储所述用户标识、密钥标识和数据存储地址的映射关系，删除所述密钥值、用户数据和密文数据；

[0010] 或根据所述用户端的所述数据请求，向所述云平台输入所述数据存储地址，接收由所述云平台输出的与所述数据存储地址对应的所述密文数据；或根据与所述数据存储地址对应的所述密钥标识请求所述密钥管理服务器返回所述密钥值，将所述密文数据和所述密钥值一同输入所述加解密服务器，所述加解密服务器将所述密文数据转换成所述用户数据并返回所述用户端，所述密钥映射服务器删除所述密钥值、用户数据和密文数据。

[0011] 所述云平台用于保存由所述密钥映射服务器输入的所述密文数据，向所述密钥映射服务器返回所述数据存储地址；或根据所述密钥映射服务器输入的所述数据存储地址查找对应的所述密文数据，向所述密钥映射服务器输出所述密文数据。

[0012] 所述密钥标识为随机生成。

[0013] 所述密钥映射服务器、密钥管理服务器和云平台相互独立。

[0014] 所述密钥映射服务器和/或加解密服务器为集成于所述用户端本身的功能模块。

[0015] 一种实现所述云计算环境数据安全存储系统的云计算环境数据安全存储方法，它包括构建一云计算环境数据安全存储系统，包括分别连接密钥映射服务器并与所述密钥映射服务器进行数据交换的密钥管理服务器、加解密服务器、用户端和云平台；

[0016] 其中，用户数据加密存储的步骤包括：

[0017] 1）所述用户端将用户标识和用户数据传送至所述密钥映射服务器；

[0018] 2）所述密钥映射服务器生成与所述用户标识对应的密钥标识，并接收由所述密钥管理服务器生成的对应于所述密钥标识的密钥值，所述密钥管理服务器存储所述密钥标识和密钥值；

[0019] 3）所述密钥映射服务器将所述密钥值和用户数据发送至所述加解密服务器将所述用户数据加密成密文数据；

[0020] 4）所述云平台保存所述密文数据后将数据存储地址发送给所述用户端；

[0021] 所述用户数据请求使用的步骤包括：

[0022] I）所述用户端将所述用户标识和数据存储地址传送至所述密钥映射服务器；

[0023] II）所述密钥映射服务器将所述数据存储地址输入所述云平台中检索并返回与所述数据存储地址对应的所述密文数据；

[0024] III）所述密钥映射服务器根据所述数据存储地址对应的所述密钥标识在所述密

钥管理服务器中提取所述密钥值；

[0025] IV）所述密钥映射服务器将所述密文数据和密钥值一同输入所述加解密服务器中将所述密文数据解密成所述用户数据，并将所述用户数据返回所述用户端。

[0026] 所述密钥映射服务器中储存所述用户标识、密钥标识和数据存储地址的映射关系；所述密钥管理服务器中储存所述密钥标识和密钥值，所述云平台中储存所述密文数据。

[0027] 所述加解密服务器在完成加密或解密之后，删除所述密钥值、用户数据和密文数据。

[0028] 将所述数据存储地址发送给所述用户端后，或将所述用户数据发送给所述用户端后，所述密钥映射服务器删除密钥值、用户数据和密文数据。

[0029] 本发明的技术效果如下：

[0030] 本发明的一种云计算环境数据安全存储系统和方法，其特征在于：一种云计算环境数据安全存储系统，其特征在于：它包括分别连接密钥映射服务器并与密钥映射服务器进行数据交换的密钥管理服务器、加解密服务器、用户端和云平台；用户端向密钥映射服务器提出存储请求或数据请求，存储请求包括用户标识和用户数据，数据请求包括用户标识和由云平台返回的数据存储地址；密钥映射服务器根据存储请求生成密钥标识，密钥管理服务器中生成与密钥标识对应的密钥值；密钥映射服务器根据数据请求分别由云平台和密钥管理服务器中获取密文数据和密钥值；加解密服务器根据密钥值将用户数据加密成密文数据，或根据密钥值将密文数据解密成用户数据，完成加密或解密后，删除密钥值、用户数据和密文数据。本发明通过应用密钥映射技术，引入用于密钥映射管理的第三方，即密钥值、密文数据、密钥映射关系均分开保存，使分别存储这些数据的任意两方合谋或数据泄漏都无法破解密文数据的机密性，有效的解决了密钥管理方和云存储提供方的合谋攻击问题，实现了云计算环境下数据安全存储方案。

[0031] 本发明通过在密钥映射服务器中储存用户标识、密钥标识和数据存储地址的映射关系，密钥管理服务器中储存密钥标识和密钥值，云平台中储存密文数据，从而打破密钥值和密文数据之间的直接联系。且当数据存储地址发送给用户端后，或用户数据发送给用户端后，密钥映射服务器删除密钥值、用户数据和密文数据；加解密服务器完成加密或解密后，删除密钥值、用户数据和密文数据。这样就使保存密钥映射关系的位置不会同时存在密钥值和密文数据，保存密文数据的位置不会同时存在密钥值和密钥映射关系，保存密钥值的位置不会同时存在密钥映射关系和密文数据，达到密钥值、密文数据、密钥映射关系的三方独立性，有效的保证了用户的数据安全，防止了用户数据被恶意篡改或泄漏问题。

[0032] 本发明中，密钥信息的生成和管理过程、密钥映射过程、数据加解密过程均由相应的服务器来完成，用户只需维护自身的用户标识和数据存储地址信息，可大大节省用户繁琐的密钥生成及管理、数据加解密等操作，因此具有良好的用户体验。

附图说明

[0033] 图 1 是本发明的云计算环境数据安全存储系统结构示意图

[0034] 图 2 是本发明的用户数据加密存储过程的流程示意图

[0035] 图 3 是本发明的用户数据请求使用过程的流程示意图

具体实施方式

[0036] 下面结合附图对本发明进行说明。

[0037] 在以下描述中，一些具体细节为计算机领域的技术人员提供对本发明的整体理解。在实施例中，以示意图或者框图的形式表明实现具体功能的元件，以便突出技术重点，而不会在不必要的细节方面模糊本发明。比如，由于本领域普通技术人员的理解范围中涵盖了关于网络通信、电磁信号指令技术、用户端接口或输入 / 输出技术等本领域中公开的、常识性的细节，因而在实施例中最大程度上省略了上述技术细节，而不认为这些细节是获得本发明完整技术方案所必须的特征。

[0038] 如图 1 所示，本发明的云计算环境数据安全存储系统包括密钥映射服务器 1、密钥管理服务器 2、加解密服务器 3 和用户端 4，密钥映射服务器 1 分别与密钥管理服务器 2、加解密服务器 3 和用户端 4 连接，并进行数据交换，密钥映射服务器 1 还与云平台 5 连接，实现密文数据的上传和下载。其中 ：

[0039] 用户端 4 作为云计算系统的使用者，可向密钥映射服务器 1 提出上传用户数据的存储请求和接收用户数据的数据请求 ；其中存储请求的内容为用户标识 User_id 和用户数据 Plain_Data，数据请求内容为用户标识 User_id 和数据存储地址 Data_url。由于同一个用户端 4 可能拥有多份数据，因此相对于用户端 4 而言用户标识 User_id 不唯一，但是相对于用户标识 User_id 而言数据存储地址 Data_url 具有唯一性。其中数据存储地址 Data_url 用于标识密文数据在云平台 4 中的存储位置。

[0040] 密钥映射服务器 1 根据用户端 4 的存储请求随机生成一个与用户标识 User_id 对应的密钥标识 Key_id，并使用密钥标识 Key_id 向密钥管理服务器 2 提出密钥请求，之后接收由密钥管理服务器 2 生成的密钥值 Key ；或向加解密服务器 3 输入密钥值 Key 和用户数据 Plain_Data，请求将用户数据 Plain_Data 转换成密文数据 Cipher_Data，并将转换后的密文数据 Cipher_Data 输入云平台 5，最后将云平台 5 输出的数据存储地址 Data_url 通过密钥映射服务器 1 返回用户端 4，储存用户标识 User_id、密钥标识 Key_id 和数据存储地址 Data_url 的映射关系，删除密钥值 Key、用户数据 Plain_Data 和密文数据 Cipher_Data ；

[0041] 或根据用户端 4 的数据请求，验证由用户端 4 输入的用户标识 User_id 和数据存储地址 Data_url 是否匹配，确认后向云平台 5 提出包括数据存储地址 Data_url 的密文数据请求，之后接收由云平台 5 输出的与数据存储地址 Data_url 对应的密文数据 Cipher_Data ；或根据之前存储的数据存储地址 Data_url 对应的密钥标识 Key_id 请求密钥管理服务器 2 返回密钥值 Key，之后将密文数据 Cipher_Data 和密钥值 Key 一同输入加解密服务器 3，请求将密文数据 Cipher_Data 转换成用户数据 Plain_Data，并将转换后的用户数据 Plain_Data 返回给用户端 4，同时删除密钥值 Key、用户数据 Plain_Data 和密文数据 Cipher_Data。

[0042] 在密钥映射服务器 1 上仅储存维护用户标识 User_id、密钥标识 Key_id 和数据存储地址 Data_url 的映射关系，典型的映射关系如 (User_id, Key_id, Data_url)，而不长期存储任何密钥值 Key、用户数据 Plain_Data 或密文数据 Cipher_Data 信息。

[0043] 密钥管理服务器 2 应密钥映射服务器 1 的密钥请求为用户端 4 生成对应于密钥标识 Key_id 的密钥值 Key，并管理、维护密钥信息，典型的密钥信息包含密钥标识 Key_id 及其对应的密钥值 Key。

[0044] 加解密服务器 3 用于提供数据加解密服务，根据密钥映射服务器 1 输入的密钥值 Key 和用户数据 Plain_Data，将用户数据 Plain_Data 转换成密文数据 Cipher_Data，之后将密文数据 Cipher_Data 返回密钥映射服务器 1 ；或根据密钥映射服务器 1 输入的密钥值 Key 和密文数据 Cipher_Data，将密文数据 Cipher_Data 转换成用户数据 Plain_Data，之后将用户数据 Plain_Data 返回密钥映射服务器 1。在完成加密操作或解密操作之后，加解密服务器 3 删除密钥值 Key、用户数据 Plain_Data 和密文数据 Cipher_Data。

[0045] 云平台 5 即云计算服务平台，用于向用户端 4 提供计算或存储服务，保存由密钥映射服务器 1 输入的密文数据 Cipher_Data，并向密钥映射服务器 1 返回数据存储地址 Data_url ；或根据密钥映射服务器 1 输入的数据存储地址 Data_url 查找对应的密文数据 Cipher_Data，并向密钥映射服务器 1 输出密文数据 Cipher_Data。

[0046] 对于上述实施例，密钥映射服务器 1、密钥管理服务器 2 和云平台 4 为独立的三方实体，任意两方合谋或数据泄漏都无法得到用户端 4 的用户数据 Plain_Data。其中密钥映射服务器 1 和加解密服务器 3 既可以是两个完全独立于用户端 4 的服务器实体，也可以是集成于用户端 4 本身的功能模块，即密钥映射模块和加解密模块。

[0047] 本发明的云计算环境数据安全存储方法主要包括用户数据加密存储和用户数据请求使用两个过程。其中 ：

[0048] 如图 2 所示，用户数据加密存储过程描述的是用户端 4 将用户数据 Plain_Data 采用加密的形式存储至云平台 5，同时运用密钥映射技术保证云平台 5 中数据的安全性，包括以下步骤 ：

[0049] 1)用户端 4 使用安全传输通道，如 SSL 加密通道，将用户标识 User_id 和用户数据 Plain_Data 传送至密钥映射服务器 1，提出上传用户数据的存储请求 ；

[0050] 2) 密钥映射服务器 1 根据用户端 4 的存储请求随机生成一个对应于用户标识 User_id 的密钥标识 Key_id，并使用密钥标识 Key_id 向密钥管理服务器 2 提出密钥请求 ；

[0051] 3)密钥管理服务器 2 应密钥映射服务器 1 的密钥请求为用户端 4 生成对应于密钥标识 Key_id 的密钥值 Key，并将密钥信息 (Key_id,Key) 存储至密钥管理服务器 2 中 ；

[0052] 4) 密钥管理服务器 4 向密钥映射服务器 1 返回密钥信息 (Key_id,Key) ；

[0053] 5) 密钥映射服务器 1 将密钥值 Key 和用户数据 Plain_Data 发送至加解密服务器 3，请求加密操作 ；

[0054] 6) 加解密服务器 3 依据收到的密钥值 Key 将用户数据 Plain_Data 转换成密文数据 Cipher_Data ；

[0055] 7) 加解密服务器 3 将密文数据 Cipher_Data 返回至密钥映射服务器 1，之后删除密钥值 Key、用户数据 Plain_Data 和密文数据 Cipher_Data ；

[0056] 8) 密钥映射服务器 1 将收到的密文数据 Cipher_Data 发送至云平台 5 ；

[0057] 9) 云平台 5 将密文数据 Cipher_Data 存储至相关的存储设备中 ；

[0058] 10) 云平台 5 将数据存储地址 Data_url 返回给密钥映射服务器 1 ；

[0059] 11)密钥映射服务器 1 中存储映射对 (Key_id,Data_url)，同时删除密钥值 Key、用户数据 Plain_Data 和密文数据 Cipher_Data ；

[0060] 12) 密钥映射服务器 1 将数据存储地址 Data_url 返回给用户端 4。

[0061] 如图 3 所示，用户端数据请求使用过程描述的是用户端 4 请求数据时，密钥映射服

务器 1 首先从云平台 5 中取得密文数据 Cipher_Data，根据在密钥映射服务器 1 中存储的密钥标识 Key_id 和数据存储地址 Data_url 的映射关系取得密钥值 Key，将密文数据 Cipher_Data 解密后返回给用户端 4 的过程。其包括以下步骤：

[0062] I）用户端 4 向密钥映射服务器 1 提出接收用户数据的数据请求，数据请求的内容包括用户标识 User_id 和数据存储地址 Data_url；

[0063] II）密钥映射服务器 1 根据用户端 4 的数据请求，根据数据存储地址 Data_url 向云平台 5 提出包括数据存储地址 Data_url 的密文数据请求；

[0064] III)云平台 5 根据数据存储地址 Data_url 检索并返回与数据存储地址 Data_url 对应的密文数据 Cipher_Data 给密钥映射服务器 1；

[0065] IV）密钥映射服务器 1 根据映射关系 (User_id,Key_id,Data_url) 中数据存储地址 Data_url 对应的密钥标识 Key_id；

[0066] V）密钥映射服务器 1 根据密钥标识 Key_id 向密钥管理服务器 2 提出密钥请求；

[0067] VI）密钥管理服务器 2 根据密钥标识 Key_id 查询对应的密钥值 Key，并将密钥值 Key 返回给密钥映射服务器 1；

[0068] VII)密钥映射服务器 1 将密文数据 Cipher_Data 和密钥值 Key 一同给加解密服务器 3，请求解密操作；

[0069] VIII）加解密服务器 3 将密文数据 Cipher_Data 转换成用户数据 Plain_Data，之后将用户数据 Plain_Data 输入给密钥映射服务器 1；

[0070] IX）密钥映射服务器 1 返回用户数据 Plain_Data 给用户端 4。

[0071] 应当指出，以上所述具体实施方式可以使本领域的技术人员更全面地理解本发明创造，但不以任何方式限制本发明创造。因此，尽管本说明书参照附图和实施例对本发明创造已进行了详细的说明，但是，本领域技术人员应当理解，仍然可以对本发明创造进行修改或者等同替换，总之，一切不脱离本发明创造的精神和范围的技术方案及其改进，其均应涵盖在本发明创造专利的保护范围当中。

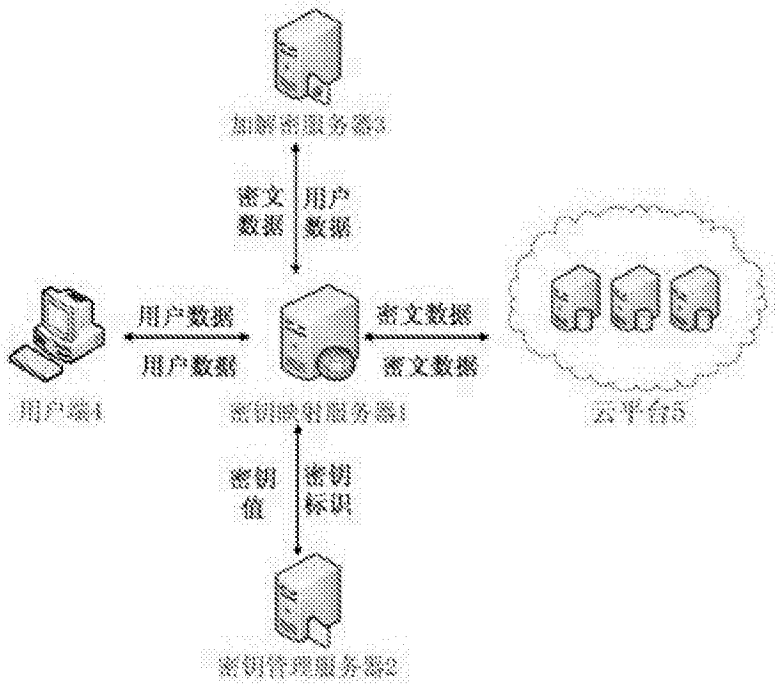

加解密服务器3
密文数据
用户数据
用户数据
用户数据
密文数据
密文数据
用户端4
密钥映射服务器1
云平台5
密钥值
密钥标识
密钥管理服务器2

图 1

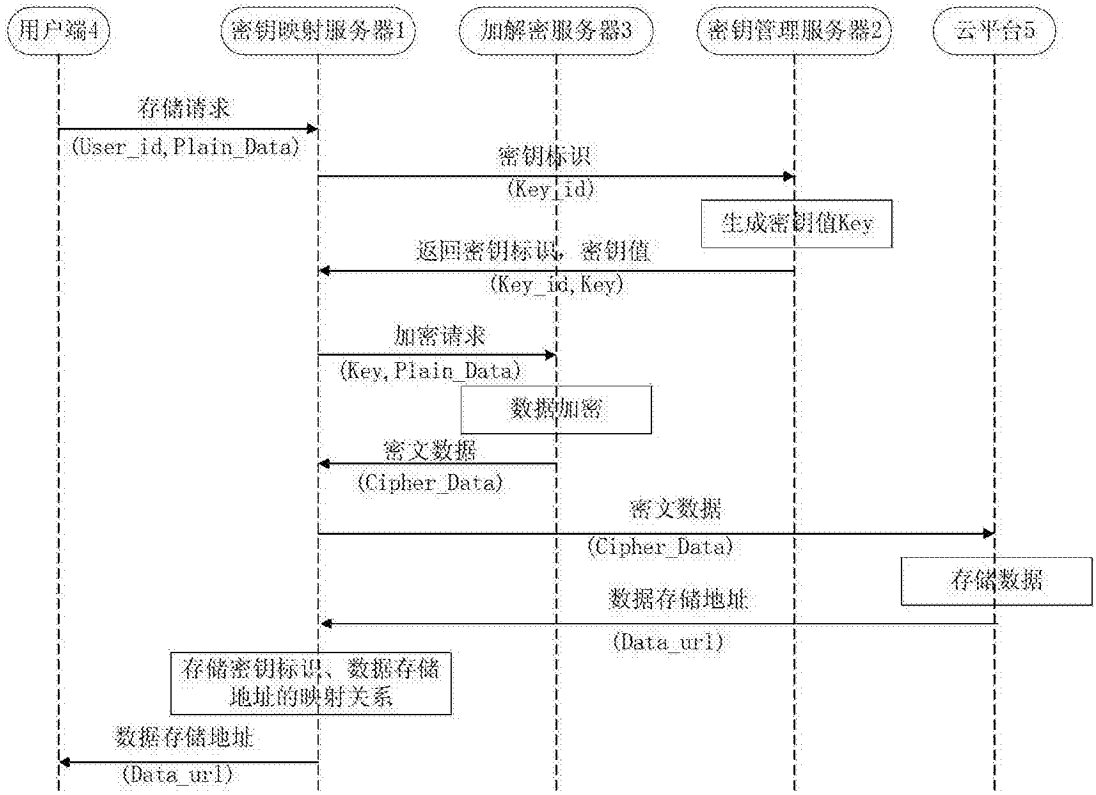

用户端4
密钥映射服务器1
加解密服务器3
密钥管理服务器2
云平台5
存储请求
(User_id,Plain_Data)
密钥标识
(Key_id)
生成密钥值Key
返回密钥标识、密钥值
(Key_id,Key)
加密请求
(Key,Plain_Data)
数据加密
密文数据
(Cipher_Data)
密文数据
(Cipher_Data)
存储数据
数据存储地址
(Data_url)
存储密钥标识、数据存储地址的映射关系
数据存储地址
(Data_url)

图 2

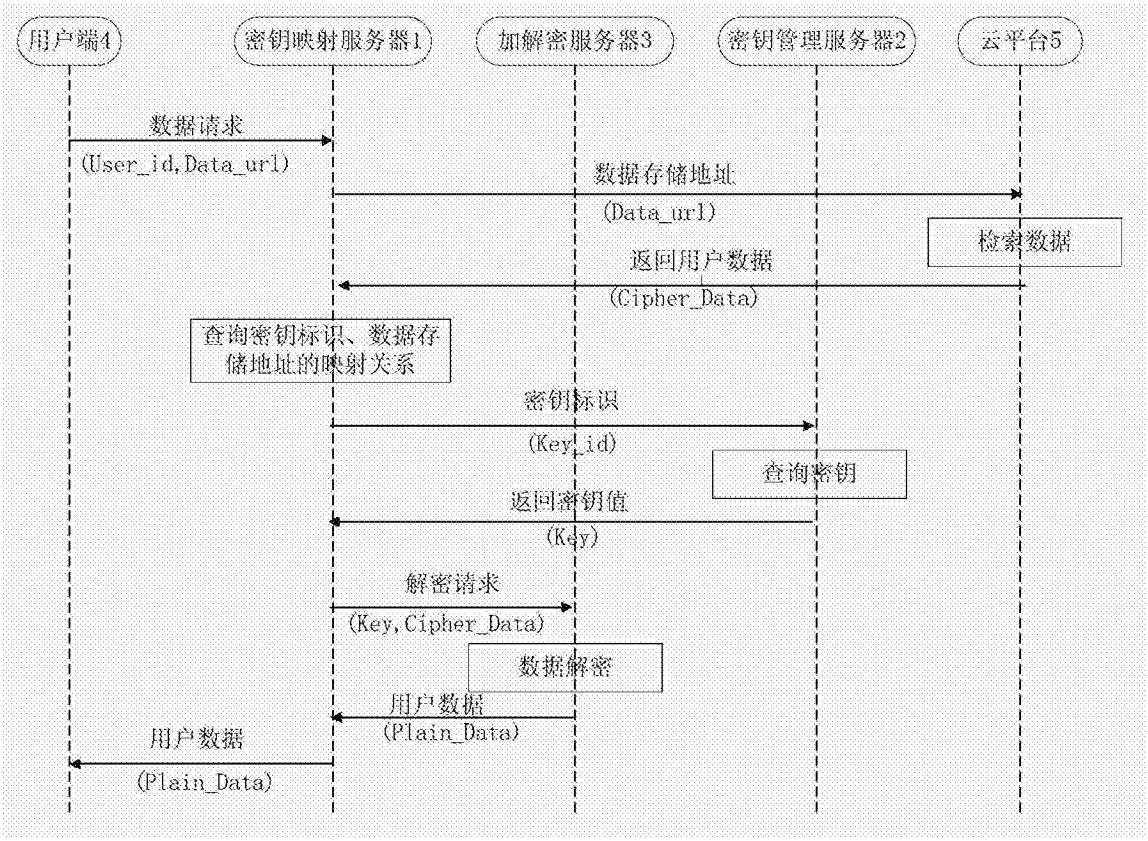

用户端4
密钥映射服务器1
加解密服务器3
密钥管理服务器2
云平台5
数据请求
(User_id,Data_url)
数据存储地址
(Data_url)
检索数据
返回用户数据
(Cipher_Data)
查询密钥标识、数据存储地址的映射关系
密钥标识
(Key_id)
查询密钥
返回密钥值
(Key)
解密请求
(Key,Cipher_Data)
数据解密
用户数据
(Plain_Data)
用户数据
(Plain_Data)

图 3