(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 103973715 A
(43)申请公布日 2014.08.06

(21)申请号 201410235655.7

(22)申请日 2014.05.29

(71)申请人 广东轩辕网络科技股份有限公司
地址 510000 广东省广州市天河区高普路1033号第8层

(72)发明人 曹继翔

(74)专利代理机构 北京商专永信知识产权代理事务所（普通合伙）11400
代理人 许春兰 高之波

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

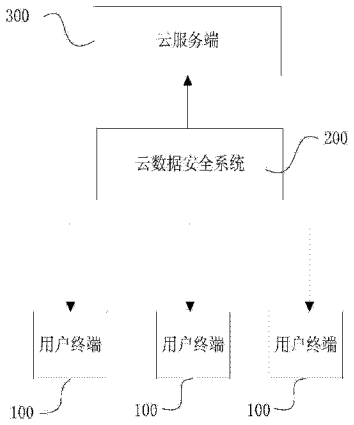
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种云计算安全系统和方法

(57)摘要

本发明提供数据一种云计算安全系统，包括多个用户终端、云数据安全系统和云服务端，用户终端包括：通过互联网和/或移动互联网与云服务端的登录系统相连的业务系统，业务系统向登录系统发送心跳包。与互联网和/或移动互联网通信连接的用户终端网络接口，用于用户终端与云服务端的数据交互。以及设置在用户终端内存中，供开发者植入其所开发的应用软件的软件开发包。云数据安全系统包括：用于监听用户的读取和写入操作的监听系统。用于过滤无需加密处理的文件数据的过滤系统。用于数据加密处理和数据解密处理的加解密系统。



CN 103973715 A

1. 一种云计算安全系统，包括多个用户终端（100）、云数据安全系统（200）和云服务端（300），其中

所述云服务端（300）包括接入系统（301）、登录系统（302），业务连接系统（303），业务处理与缓存系统（304），数据库（305），和云服务端网络接口（306）

所述接入系统（301）控制所述用户终端（100）接入所述云服务端（300）；所述登录系统（302）接收心跳包和消息实时推送服务，将接收的所述心跳包发送给业务处理与缓存系统（304）；所述业务连接系统（303）处理所述用户终端（100）的连接业务，与所述用户终端（100）的所述业务系统（102）进行数据交互；

所述数据库（305）存储用户终端（100）的统计信息和存储信息；

所述用户终端（100）包括：

通过互联网和/或移动互联网与云服务端（300）的所述登录系统（302）相连的业务系统（102），所述业务系统（102）向所述登录系统（302）发送心跳包；

与互联网和/或移动互联网通信连接的用户终端网络接口（101），用于所述用户终端（100）与所述云服务端（300）的数据交互；以及

设置在所述用户终端（100）内存中，供开发者植入其所开发的应用软件的软件开发包（103）；

所述云数据安全系统（200）包括：

与所述用户端网络接口（101）建立数据连接，用于监听用户终端（100）的读取和写入操作的监听系统（201）；

用于过滤无需加密处理的文件数据的过滤系统（202）；

与所述云服务端网络接口（306）建立数据连接，用于数据加密处理和数据解密处理的加解密系统（203）。

2. 根据权利要求 1 所述的一种云计算安全系统，其中所述接入系统（301）管理各区域的情况，包括当前用户终端（100）数量、闲置用户终端（100）数量和连接用户终端（100）数量，控制所述云服务端（300）与所述用户终端网络接口（101）的数据交互；所述登录系统（302）接收所述心跳包和连接消息实时推送服务，通过接收所述心跳包确定所述用户终端（100）与所述云服务端的连接状态，所述登录系统（302）获取所述用户终端（100）的信息，将该信息发送给所述业务处理与缓存系统（304）。

3. 根据权利要求 1 所述的一种云计算安全系统，其中所述监听系统（201）还包括用于监听用户终端（100）的写入操作的写入监听系统；用于监听用户终端（100）的读取操作读取监听系统。

4. 根据权利要求 1 所述的一种云计算安全系统，其中所述过滤系统（202）还包括：用于过滤无需加密处理的文件数据的文件数据过滤系统；用于确定用户终端（100）操作方式的识别系统，所述识别系统对所述监听系统（201）中的文件数据进行过滤和识别处理。

5. 根据权利要求 1 所述的一种云计算安全系统，其中所述加解密系统（203）包括：用于数据加密处理的加密系统；用于数据解密处理的解密系统；用于备份和还原用户终端（100）数据的备份系统；以及用于用户终端（100）自定义开发加解密方法的自定义加解密方法系统。

6. 根据权利要求 1 所述的一种云计算安全系统，其中所述数据库（305）负责存储用户

终端 (100) 的统计信息和用户终端 (100) 请求储存的数据，所述用户终端 (100) 的统计信息包括用户终端 (100) 信息和连接信息，所述用户终端 (100) 信息包括用户终端 (100) 账号信息和用于确认用户终端 (100) 身份及特征的信息。

7. 一种云计算安全方法，包括：

用户终端 (100) 登录云数据安全系统 (200) 时，登录系统 (302) 验证用户终端 100 登录用户信息；

用户终端 (100) 访问云数据安全系统 (200) 的监听系统 (201)，在云数据安全系统 (200) 的监听系统 (201) 中选择监听文件数据的位置，配置无需监听的文件数据，监听系统 (201) 监听用户终端 (100) 的读取和写入操作，将文件数据发送至过滤系统 (202)；

过滤系统 (202) 过滤用户终端 (100) 配置的无需监听加密的文件数据并确定用户终端 (100) 的操作是读取还是写入，将确定需要加密的写入数据或需要解密的读取数据传输到加解密系统 (203)；

加解密系统 (203) 对过滤系统 (202) 过滤后的数据进行相应的加密或解密处理。

8. 根据权利要求 7 所述的一种云计算安全方法，其中所述所述备份文件数据储存在所述云服务端 (300) 的数据库 (305) 中。

一种云计算安全系统和方法

技术领域

[0001] 本发明涉及云计算领域，具体涉及一种云计算安全系统和方法。

背景技术

[0002] 云计算是当前信息领域的热门话题。目前云计算分为公有云、私有云和混合云三种。各种类型的云基础设施平台、云服务、云存储系统等层出不穷。但是当前云计算的发展仍面临一系列技术挑战。不论是公有云、私有云还是混合云，数据信息安全都是一个重要挑战。作为云计算使用者，特别关心自己的数据安全及隐私能否得到保障护，如担心数据网络安全、担心把自己的代码和数据交给云服务商后，云服务商也具有数据的控制权和并享有优先访问权，自己将缺少对数据控制权与安全保障能力。解决云计算中存在的数据安全问题是很有必要的。

[0003] 在云计算环境中，由于云服务提供商不可完全信任，导致访问控制实施部件运行在不可信的环境中，无法正确实施用户制定的访问控制策略。传统的数据或文件存储都是以明文形式存储在存储器上，或者使用某些工具对其中的文件夹加密进行锁定来实现简单的数据保密。传统形式的弊端在于只要使用者能够打开对应电脑、进入相应工作界面就能够打开、查看数据或文件，或者能够破解锁定的文件夹就可以查看到数据。由于以上种种问题，迫切需要一种可完全脱离云服务商又能保证数据安全、完整的方案。

发明内容

[0004] 本发明的目的在于提供一种云计算安全系统和方法，能够保证数据传输与查看的安全性和可靠性。

[0005] 本发明一方面提供的一种云计算安全系统，包括多个用户终端、云数据安全系统和云服务端，其中云服务端包括：用于控制用户终端接入云服务端，存有业务处理与缓存系统的用户终端状态的接入系统。登录系统，接收心跳包和消息实时推送服务，将接收的心跳包发送给业务处理与缓存系统，用于处理用户终端的连接业务，与用户终端的业务系统进行数据交互的业务连接系统。业务处理与缓存系统用于处理用户终端的连接业务。数据库，存储用户终端的统计信息和存储信息；以及与互联网和/或移动互联网通信连接的服务端网络接口。用户终端包括：通过互联网和/或移动互联网与云服务端的登录系统相连的业务系统，业务系统向登录系统发送心跳包。与互联网和/或移动互联网通信连接的用户终端网络接口，用于用户终端与云服务端的数据交互。以及设置在用户终端内存中，供开发者植入其所开发的应用软件的软件开发包。云数据安全系统包括：用于监听用户的读取和写入操作的监听系统。用于过滤无需加密处理的文件数据的过滤系统。用于数据加密处理和数据解密处理的加解密系统。

[0006] 在一些实施方式中，接入系统管理各区域的情况，包括当前用户终端数量、闲置用户终端数量和连接用户终端数量，控制云服务端与用户终端网络接口的数据交互；登录系统接收心跳包和连接消息实时推送服务，通过接收心跳包确定用户终端与服务端的连接状

态，登录系统获取用户终端的信息，将该信息发送给业务处理与缓存系统。

[0007] 在一些实施方式中，监听系统还包括用于监听用户终端的写入操作的写入监听系统；用于监听用户终端的读取操作读取监听系统。

[0008] 在一些实施方式中，过滤系统还包括：用于过滤无需加密处理的文件数据的文件数据过滤系统；用于确定用户终端操作方式的识别系统，识别系统对监听系统中的文件数据进行过滤和识别处理。

[0009] 在一些实施方式中，加解密系统包括：用于数据加密处理的加密系统；用于数据解密处理的解密系统；用于备份和还原用户终端数据的备份系统；以及用于用户终端自定义开发加解密方法的自定义加解密方法模板。

[0010] 在一些实施方式中，数据库负责存储用户终端的统计信息和用户终端请求储存的数据，用户终端的统计信息包括用户终端信息和连接信息，用户终端信息包括用户终端账号信息和用于确认用户终端身份及特征的信息。

[0011] 本发明另一方面提供的一种云计算安全方法，包括：用户终端访问云服务端网络接口，云服务端网络接口访问接入系统，用户终端在登录系统服务端发起登录请求；用户终端登录云数据安全系统。用户终端初始化云数据安全系统，在云数据安全系统监听系统中选择监听位置。用户终端在云数据安全系统的过滤系统中，过滤用户配置的无需监听加密的文件，并确定用户的操作。用户终端在云数据安全系统的加解密系统中，配置加解密方法，加解密系统处理过滤系统过滤后的数据，并做备份。

[0012] 在一些实施方式中，备份文件数据储存在云服务端的数据库中。

[0013] 本发明能提供了监听用户存取机制，过滤不必要处理的文件数据，再对监听过滤后的文件进行相应的加密和解密操作，在加解密方面，提供了多种方法选择，并且提供用户自定义的加解密方法，以增强数据的安全保障。

附图说明

[0014] 图 1 为本发明一种实施方式的一种云计算安全系统示意图。

[0015] 图 2 为本发明一种实施方式的一种云计算安全系统的云服务端示意图；

[0016] 图 3 为本发明一种实施方式的一种云计算安全系统的用户终端示意图；

[0017] 图 4 为本发明一种实施方式的一种云计算安全系统的云数据安全系统示意图；

[0018] 图 5 为本发明一种实施方式的一种云计算安全方法示意图。

具体实施方式

[0019] 下面结合附图及具体实施例，以云计算数据传输为例，对本发明作进一步的详细说明。

[0020] 本发明一方面提供了一种云计算安全系统，如图 1 所示，包括多个用户终端 100、云数据安全系统 200 和云服务端 300，本实施例中以用户终端 100 与云服务端 300 进行数据交互为例进行说明。如图 3 所示，用户终端 100 包括业务系统 102、与互联网和 / 或移动互联网通信连接的用户终端网络接口 101 以及软件开发包 103。如图 2 所示，云服务端 300 包括接入系统 301、登录系统 302、业务连接系统 303、业务处理与缓存系统 304、数据库 305 以及与互联网和 / 或移动互联网通信连接的云服务端网络接口 306。如图 4 所示，云数据安

全系统 200 包括监听系统 201、过滤系统 202 和加解密系统 203。用户终端 100 发送数据给云服务端 300 时，用户终端 100 发送数据给云数据安全系统 200，云数据安全系统 200 接收用户终端 100 数据，对用户终端 100 发送的数据进行加密处理后发送给云服务端 300。用户终端 100 接收储存在云服务端 300 的数据时，云服务端 300 发送数据给云数据安全系统 200，云数据安全系统 200 接收云服务端 300 数据，对云服务端 300 发送的数据进行解密处理后发送给用户终端 100。

[0021] 业务系统 102 通过互联网和 / 或移动互联网与云服务端 300 的登录系统 302 相连。用户终端 100 通过业务系统 102 向登录系统 302 发送心跳包，维持与云服务端 300 的连接。心跳包是在用户终端 100 和服务端间定时通知对方自己状态的一个自己定义的命令字，按照一定的时间间隔发送，用来判断用户终端 100 是否正常运行。即，采用定时发送简单的通讯包，如果在指定时间段内未收到对方响应，则判断用户终端 100 不与服务端进行数据通信。用户终端 100 通过安装的软件开发包 103 可以实现不同网络中的用户终端 100 应用本发明进行数据交互。

[0022] 用户终端网络接口 101 可以通过互联网和 / 或移动互联网与云服务端网络接口 306 连接，实现用户终端 100 与云服务端 300 的数据交互。

[0023] 软件开发包 103 设置在用户终端 100 内存中，软件开发包 103 封装成软件安装包为现有技术，应用本实施方式中无需调整或改进。

[0024] 接入系统 301 用于控制用户终端 100 接入云服务端 300。

[0025] 登录系统 302 负责连接心跳包和消息实时推送服务，通过接收心跳包来确定用户终端 100 与云服务端 300 是否有连接，如果在指定时间段内未收到对方响应，则判断对方已经离线、或未与服务端连接。登录系统 302 获取用户终端 100 的信息，并将该信息发送给业务处理与缓存系统 304。用户终端 100 的信息包括用户终端 100 云账号信息和用于确认用户终端 100 身份及特征的信息；用户终端 100 云账号信息包括用户终端 100 云账号名、密码、真实姓名、性别、年龄、所在城市、职业、手机号码、邮件地址、签名档；用于确认用户终端 100 身份及特征的信息包括云账号信息和身份特征信息；云账号信息包括云账号名、密码、签名；身份特征信息包括真实姓名、性别、年龄、所在城市、职业、手机号码、邮件地址。

[0026] 业务连接系统 303 负责处理用户终端 100 的连接业务，与用户终端 100 的业务系统 102 进行数据交互，接受用户终端 100 提出的业务需求，当用户终端 100 向云服务端 300 发送数据包，请求连接云服务端 300 实现数据交互时，云服务端 300 的业务连接系统 303 接收用户终端 100 的请求。

[0027] 业务处理与缓存系统 304 负责处理用户终端 100 的连接业务，缓存用户终端 100 发送的请求数据。业务处理与缓存系统 304 还存储用户终端 100 信息和连接信息，可以有多个，每个业务处理与缓存系统 304 属于一个区域，每个区域有一个区域标识，业务处理与缓存系统 304 存储挂靠在该区域的用户终端 100 连接数量。接入系统 301 管理各个区域，当用户终端 100 数量大时，服务器数量会有很多，不同服务器处理不同区域的业务。例如，南通一个服务器，北京一个服务器，业务处理与缓存系统 304 启动时需要向接入系统 301 注册。

[0028] 数据库 305 负责存储用户终端的统计信息和用户终端请求储存的数据，用户终端 100 的统计信息包括用户终端信息和用户终端连接信息。用户终端信息包括用户终端账

号信息和用于确认用户终端身份及特征的信息；用户终端账号信息包括用户终端账号名、密码、真实姓名、性别、年龄、所在城市、职业、手机号码、邮件地址、签名档；用于确认用户终端身份及特征的信息包括账号信息和身份特征信息；身份特征信息包括真实姓名、性别、年龄、所在城市、职业、手机号码、邮件地址；连接信息包括连接标识和连接的用户终端 100 标识。

[0029] 监听系统 201 包括写入监听系统，用于监听用户终端 100 的写入操作功能；读取监听系统，用于监听用户终端 100 的读取操作功能。监听系统 201 主要的功能是监听是否有数据变化，如有变化则记录下来；监听系统 201 主要包括操作系统适配器功能，用来识别并选择所对应的操作系统采用的监听实现技术。本发明为 windows 操作系统，采用 API HOOK 技术监听文件读写操作，在本发明的该实施例中，是基于 windows 操作系统的。但本发明并不限于此。如果是 liunx 操作系统，采用 Inotify 相关技术实现文件监听操作。监听系统 201 在加解密过程中的作用主要是只针对在变化的文件和数据进行加密，不需要全盘扫描后再进行判断加密。监听系统为用户终端 100 提供监听位置选择、文件过滤选择、开始监听和停止监听功能，所述监听位置选择，用于供用户终端 100 自定义选择需要监听的位置；文件过滤选择，用于过滤用户终端 100 不需要监听的文件，可进行模糊匹配，模糊匹配的文件格式为：*.txt。通过采用 B/S 架构来实现以上功能，如使用 C++、JAVA 等技术实现用户终端 100 监听位置选择并控制、文件过滤、启动和停止功能。此为现有技术，在此不做详细说明。

[0030] 过滤系统 202 包括：文件数据过滤系统，用于过滤不需要加密的文件数据，可进行模糊过滤。识别系统，用于区分文件是否读取操作还是写入操作功能。识别系统实现对上述监听系统 201 所得到的文件或数据进行过滤和识别。采用 C++、JAVA 技术、.NET 技术等主流技术实现该系统功能，本发明采用 JAVA 文件输入输出流实现。此为现有技术，在此不做详细说明。过滤系统 202 在加解密过程中的作用主要是判断是采用加密还是解密方法。

[0031] 加解密系统 203，包括：加密系统，用于数据加密处理；解密系统，用于数据解密处理，加解密系统 203 采用现有的技术实现，如 AES、DES 等，并提供用户终端 100 自定义开发加解密方法。备份系统，用于备份用户终端 100 数据，可用来还原数据。加解密系统 203 可执行自定义加解密方法，实现自定义加解密操作，包括：系统自带加解密方法库选择，用于对数据进行加解密的方法。自定义加解密方法模板，可用于用户终端 100 自定义开发加解密方法，导入自定义加解密方法，用于导入用户终端 100 自定义开发的方法到系统中，自定义开发加解密方法的好处是可以增强数据的安全性，并可以不断更新加解密算法，可不依赖于任何一方，加解密方法完全掌握在自己手上，同时增加加解密方法的可选择性，验证加解密方法，用于验证用户终端 100 自定义开发的方法是否正确，加解密系统 203 提供用户上传加密方法及解密方法入口，供用户自己编写加密方法以及对应的解密方法，系统相当于提供一个可运行平台，用户只要上传自己的可运行程序即可运行，比如用户采用 JAVA 语言自定义开了一个加密可运行压缩包，从加解密系统 203 上传到系统中，用户在选择加密方式时，除了系统本身自带的加密技术，还多了这里上传的一项加密方法；除了加密压缩包，还需解密压缩包，供数据解密使用，运行原理同加密压缩包是一样的；由于加密解密压缩包是由用户自己编写而来的，所以压缩包里面的算法只有用户自己知道，大大提高了加密的安全性。备份还原功能，用于数据的备份和还原，备份还原功能为现有技术，在此不做详细说明。

[0032] 根据本发明的另一方面的一种云计算安全方法，如图5所示，包括：用户终端100通过软件安装包安装云数据安全系统200，将云数据安全系统200接入到云服务端300和用户终端100数据传输层之间，在接入传输层前，先在云数据安全系统200中配置连接云服务端300的参数及配置数据，配置AES、DES运行环境，相应的加解密方法。具体操作如下：

[0033] S1. 用户终端100登录云数据安全系统200（步骤401），登录系统302，输入账号和密码，输入正确才可进入系统，如果错误，在读取文件数据时会自动提示需要登录，另一种实施例将云数据安全系统200封装成加密狗，使用时必须先接入加密狗，否则读取到的文件均为加密后的文件数据，不使用时拔出。密码验证正确，用户终端100成功登录云数据安全系统200（步骤402）。

[0034] S2. 用户终端100初始化系统，在云数据安全系统200监听系统中选择监听位置（步骤403），在用户终端100为选择时默认监听所有文件数据，用户终端100可以选择监听指定存储位置的读写操作，用户终端100配置无需监听的文件数据（步骤404），配置时支持text.txt格式的精确监听和*.txt格式的模糊监听，云数据安全系统200确定读写操作的重命名文件数据名，Out_文件名表示读取操作例如Out_text.txt，In_文件数据名表示写入操作例如In_text.txt，用来确定是读取还是写入操作，同时监听系统还提供停止监控功能，停止监听后对数据传输过程中不接入云数据安全系统200（步骤405）。

[0035] S3. 在过滤系统中，过滤用户终端100配置的无需监听加密的文件数据（步骤406），并确定用户终端100的操作是读取还是写入（步骤407），确定方法与监听系统一致，将确定的读取或写入数据传输到加解密系统203。

[0036] S4. 在加解密系统203中，先配置加解密方法（步骤408），加解密系统203处理过滤系统202过滤后的数据，并做备份，如果是写入操作，则按照系统配置的加密方式加密执行加密操作（步骤409）。如果是读取操作，则执行解密操作并恢复原文件数据（步骤410）。

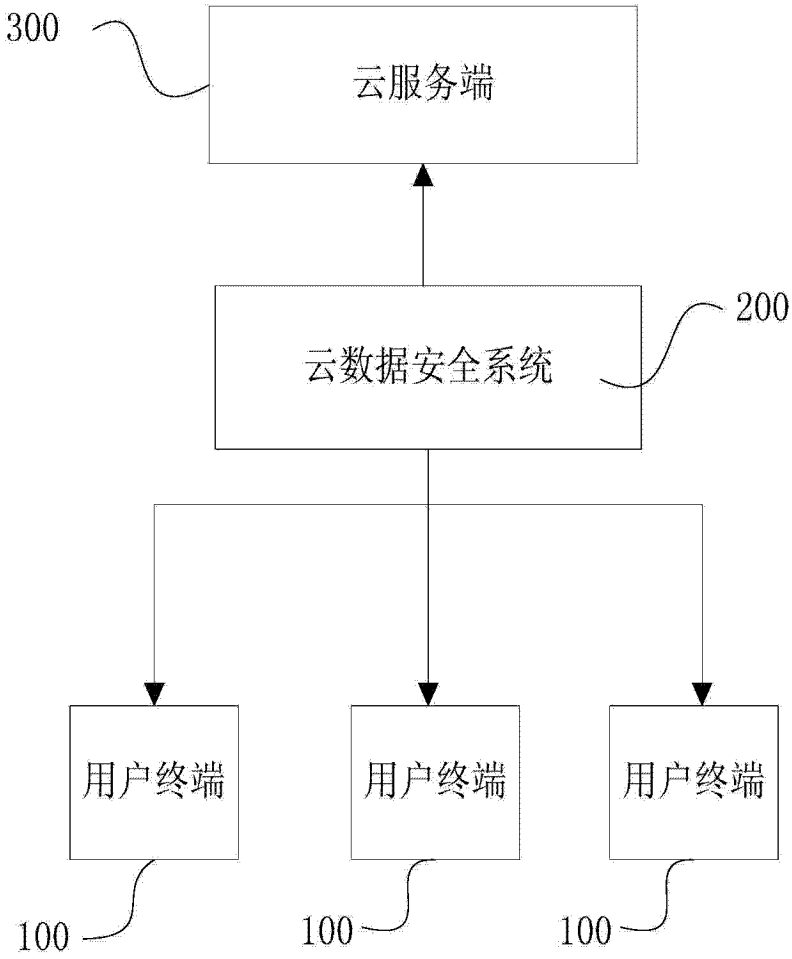

300
云服务端
200
云数据安全系统
用户终端
用户终端
用户终端
100
100
100

图 1

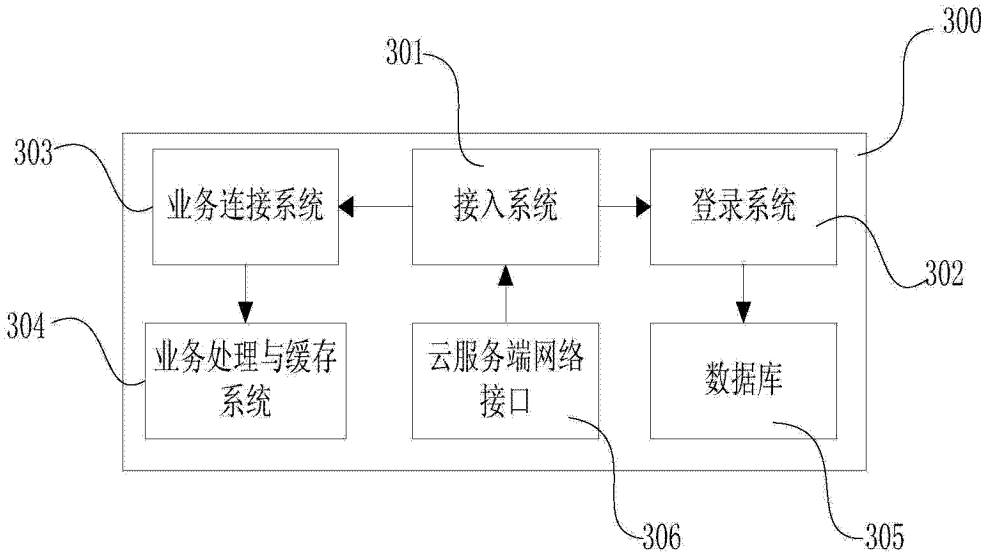

300
301
303
业务连接系统
接入系统
登录系统
302
304
业务处理与缓存系统
云服务端网络接口
数据库
306
305

图 2

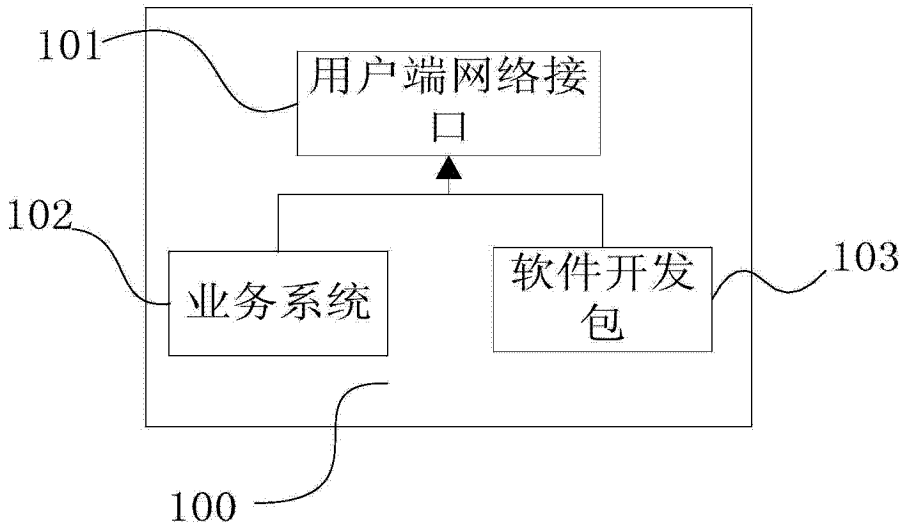

101
用户端网络接口
102
业务系统
软件开发包
103
100

图 3

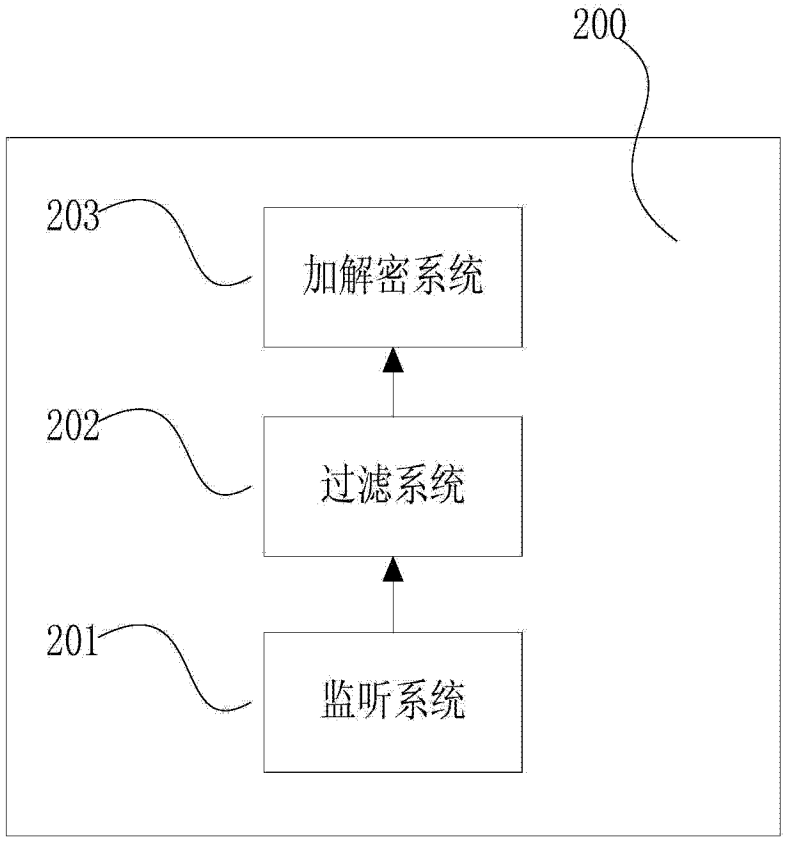

200
203
加解密系统
202
过滤系统
201
监听系统

图 4

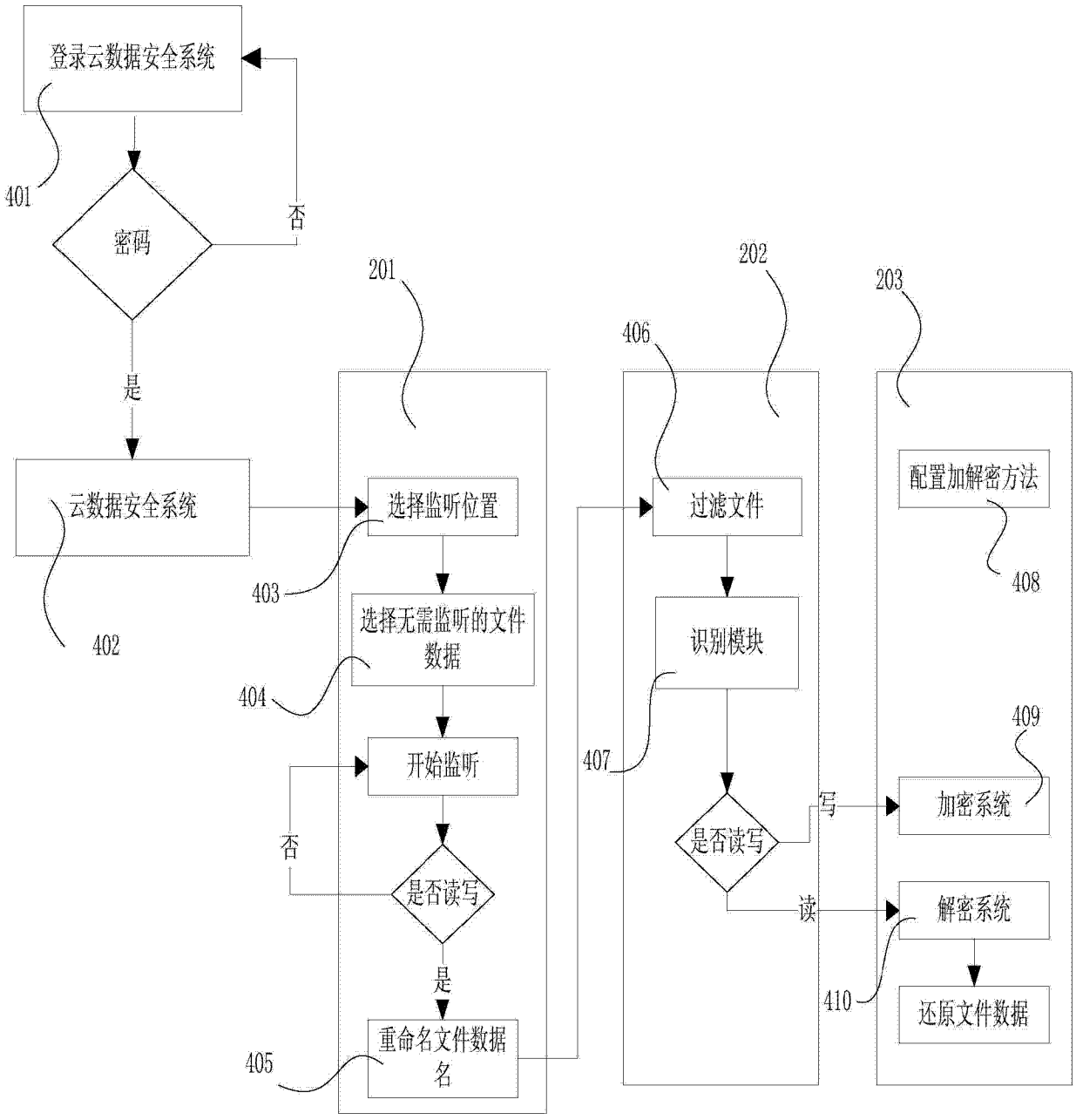

登录云数据安全系统
401
密码
否
是
云数据安全系统
402
201
选择监听位置
403
选择无需监听的文件数据
404
开始监听
否
是否读写
是
重命名文件数据名
405
202
406
过滤文件
识别模块
407
是否读写
写
读
203
配置加解密方法
408
409
加密系统
解密系统
410
还原文件数据

图 5