(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 106209847 A
(43)申请公布日 2016.12.07

(21)申请号 201610548737.6

(22)申请日 2016.07.13

(71)申请人 国网河南省电力公司南阳供电公司
地址 473000 河南省南阳市人民北路268号

(72)发明人 付静 石国松 马宏瑾

(74)专利代理机构 郑州知己知识产权代理有限公司 41132
代理人 季发军

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

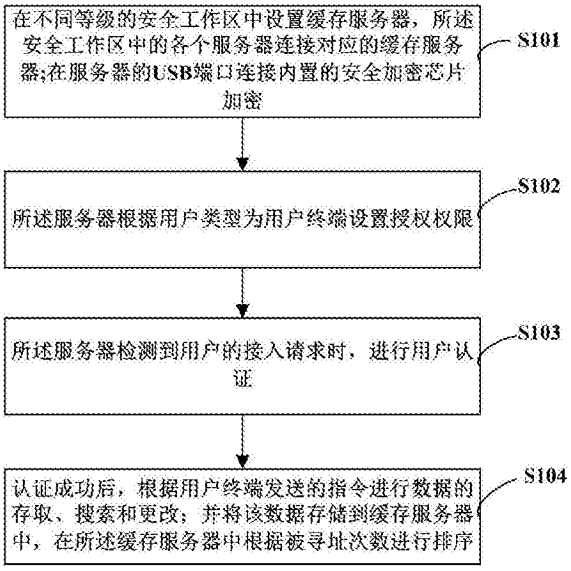
权利要求书2页 说明书6页 附图2页

(54)发明名称

电力数据传输方法及装置

(57)摘要

本发明公开了一种电力数据传输方法及装置，在不同等级的安全工作区中设置缓存服务器，所述安全工作区中的各个服务器连接对应的缓存服务器，服务器与缓存服务器之间经虚拟专用网VPN连接；服务器的USB端口连接内置的安全加密芯片加密，设置BIOS，使系统只能从指定USB端口的安全加密芯片启动；所述服务器根据用户类型为用户终端设置授权权限；所述服务器检测到用户的接入请求时，进行用户认证；认证成功后，根据用户终端发送的指令进行数据的存取、搜索和更改；并将该数据存储到缓存服务器中，在所述缓存服务器中根据被寻址次数进行排序。本发明用以实现电力数据传输，通用性好，适用于电力部门对数据安全要求较高的场合。



CN 106209847 A

1.一种电力数据传输方法，其特征在于：包括如下步骤：

在不同等级的安全工作区中设置缓存服务器，所述安全工作区中的各个服务器连接对应的缓存服务器，服务器与缓存服务器之间经虚拟专用网VPN连接；所述服务器的USB端口连接内置的安全加密芯片加密，设置BIOS，使系统只能从指定USB端口的安全加密芯片启动；系统开机，判断安全加密芯片是否正常工作，如不能正常工作，则系统自动关机；

所述服务器根据用户类型为用户终端设置授权权限；

所述服务器检测到用户的接入请求时，进行用户认证；

认证成功后，根据用户终端发送的指令进行数据的存取、搜索和更改；并将该数据存储到缓存服务器中，在所述缓存服务器中根据被寻址次数进行排序。

2.根据权利要求1所述的一种电力数据传输方法，其特征在于：所述服务器根据用户类型为用户终端设置授权权限，包括：

服务器为用户分配信用值，根据所述信用值确定访问授权权限；

服务器检测到用户发送的访问授权请求，所述访问授权请求包括：用户ID、登陆密码和访问事项；

服务器将授权请求转化为多个访问授权子查询任务，分别对所述多个访问授权子查询任务进行验证，若通过验证，则通过所述访问授权请求，用户认证成功；若未通过验证，则拒绝所述访问授权请求，并将反馈结果发送给用户。

3.根据权利要求2所述的一种电力数据传输方法，其特征在于：所述服务器检测到用户的接入请求时，进行用户认证，包括：

服务器检测到用户的接入请求时，首先进行用户认证，用户认证成功后，隔离到隔离网络区域，进行安全检测和风险评估，根据安全检测和风险评估结果确定是否同意用户的接入请求，并将结果反馈给用户；所述安全检测包括恶意攻击检测、脆弱点检测、网络数据包捕获和网络拓扑检测；用户认证未成功，则拒绝接入请求。

4.根据权利要求3所述的一种电力数据传输方法，其特征在于：还包括：所述服务器定期检测用户终端发送的终端安全信息、授权权限的使用状态，根据所述终端安全信息和授权权限的使用状态确定新的信用值。

5.根据权利要求4所述的一种电力数据传输方法，其特征在于：还包括：若安全检测和风险评估未通过时，根据服务器反馈的结果，提示用户终端进行升级和病毒库更新。

6.一种电力数据传输装置，其特征在于：包括：

设置模块，用于不同等级的安全工作区中设置缓存服务器，所述安全工作区中的各个服务器连接对应的缓存服务器，服务器与缓存服务器之间经虚拟专用网VPN连接；所述服务器的USB端口连接内置的安全加密芯片加密，设置BIOS，使系统只能从指定USB端口的安全加密芯片启动；系统开机，判断安全加密芯片是否正常工作，如不能正常工作，则系统自动关机；

授权模块，用于所述服务器根据用户类型为用户终端设置授权权限；

认证模块，用于所述服务器检测到用户的接入请求时，进行用户认证；

执行模块，用于认证成功后，根据用户终端发送的指令进行数据的存取、搜索和更改；并将该数据存储到缓存服务器中，在所述缓存服务器中根据被寻址次数进行排序。

7.根据权利要求6所述的一种电力数据传输装置，其特征在于：所述授权模块，包括：

分配子模块，用于服务器为用户分配信用值，根据所述信用值确定访问授权权限；

检测子模块，用于服务器检测到用户发送的访问授权请求，所述访问授权请求包括：用户ID、登陆密码和访问事项；

验证子模块，用于服务器将授权请求转化为多个访问授权子查询任务，分别对所述多个访问授权子查询任务进行验证，若通过验证，则通过所述访问授权请求，用户认证成功；若未通过验证，则拒绝所述访问授权请求，并将反馈结果发送给用户。

8.根据权利要求7所述的一种电力数据传输装置，其特征在于：所述认证模块，包括：

认证子模块，用于服务器检测到用户的接入请求时，首先进行用户认证，用户认证成功后，隔离到隔离网络区域，进行安全检测和风险评估，根据安全检测和风险评估结果确定是否同意用户的接入请求，并将结果反馈给用户；所述安全检测包括恶意攻击检测、脆弱点检测、网络数据包捕获和网络拓扑检测；用户认证未成功，则拒绝接入请求。

9.根据权利要求8所述的一种电力数据传输装置，其特征在于：还包括：更新模块，用于所述服务器定期检测用户终端发送的终端安全信息、授权权限的使用状态，根据所述终端安全信息和授权权限的使用状态确定新的信用值。

10.根据权利要求9所述的一种电力数据传输装置，其特征在于：还包括：反馈模块，用于若安全检测和风险评估未通过时，根据服务器反馈的结果，提示用户终端进行升级和病毒库更新。

电力数据传输方法及装置

技术领域

[0001] 本发明涉及计算机信息安全领域，尤其是涉及一种电力数据传输方法及装置。

背景技术

[0002] 传统实现计算机信息安全的技术方案主要分为两大类：一类是软件技术方案。这是目前应用最多的技术，利用安全保护软件实现计算机信息安全，这种技术方案成本低、开发灵活等优点，但也存在一些不足：(1) 系统重装后，需要重新安装软件；(2) 软件容易被卸载，导致计算机处于未保护状态；(3) 软件存在漏洞，木马、病毒会攻击安全防护软件，停掉保护进程，使得安全防护失效。另一类是硬件技术方案，如带加密芯片的硬盘、安全U 盘，这种解决方案具有安全性高、破解难等优点，但也存在一些不足：硬件成本高、 兼容性差、通用性差。

[0003] 公告号为CN101901197的发明专利公开了一种信息安全设备、控制方法及系统，信息安全设备与主机连接上电后，接收主机的状态查询，并返回多次状态不满足指令；接收主机发送的中断信号，中断返回状态满足指令给主机，以中断运行AUTORUN 程序；或者，回状态满足指令给主机，运行AUTORUN 程序。该信息安全设备及控制系统，通过主机发送中断信号给信息安全设备，中断AUTORUN程序的运行，使得信息安全设备在主机的Windows 操作系统下的使用，可不受用户权限的限制。

[0004] 公告号为CN102546620的发明专利公开了一种信息安全控制方法、信息安全控制装置以及客户端，客户端启动操作系统时，其信息安全控制装置发送连接请求给服务器，如果收到所述服务器的响应，则关闭客户端部分或全部数据输出应用；客户端进入操作系统后，发送访问许可的请求给所述服务器，如果收到允许访问服务器的响应，则允许客户端访问所述服务器，否则禁止客户端访问所述服务器。该方法能够使服务器的信息不被客户端随意下载并传播，从而提高了服务器数据的安全性。

[0005] 上述两种方法均需采用专门的信息安全设备进行信息的安全控制，其硬件成本较高，且兼容性及通用性较差。

发明内容

[0006] 有鉴于此，本发明的目的是针对现有技术的不足，提供一种电力数据传输方法及装置，用以实现电力领域的数据传输安全。

[0007] 为达到上述目的，本发明采用以下技术方案：

一种电力数据传输方法，其中，包括如下步骤：

在不同等级的安全工作区中设置缓存服务器，所述安全工作区中的各个服务器连接对应的缓存服务器，服务器与缓存服务器之间经虚拟专用网VPN连接；所述服务器的USB端口连接内置的安全加密芯片加密，设置BIOS，使系统只能从指定USB端口的安全加密芯片启动；系统开机，判断安全加密芯片是否正常工作，如不能正常工作，则系统自动关机；

所述服务器根据用户类型为用户终端设置授权权限；

所述服务器检测到用户的接入请求时，进行用户认证；

认证成功后，根据用户终端发送的指令进行数据的存取、搜索和更改；并将该数据存储到缓存服务器中，在所述缓存服务器中根据被寻址次数进行排序。

[0008] 优选的，所述服务器根据用户类型为用户终端设置授权权限，包括：

服务器为用户分配信用值，根据所述信用值确定访问授权权限；

服务器检测到用户发送的访问授权请求，所述访问授权请求包括：用户ID、登陆密码和访问事项；

服务器将授权请求转化为多个访问授权子查询任务，分别对所述多个访问授权子查询任务进行验证，若通过验证，则通过所述访问授权请求，用户认证成功；若未通过验证，则拒绝所述访问授权请求，并将反馈结果发送给用户。

[0009] 优选的，所述服务器检测到用户的接入请求时，进行用户认证，包括：

服务器检测到用户的接入请求时，首先进行用户认证，用户认证成功后，隔离到隔离网络区域，进行安全检测和风险评估，根据安全检测和风险评估结果确定是否同意用户的接入请求，并将结果反馈给用户；所述安全检测包括恶意攻击检测、脆弱点检测、网络数据包捕获和网络拓扑检测；用户认证未成功，则拒绝接入请求。

[0010] 优选的，还包括：所述服务器定期检测用户终端发送的终端安全信息、授权权限的使用状态，根据所述终端安全信息和授权权限的使用状态确定新的信用值。

[0011] 优选的，还包括：若安全检测和风险评估未通过时，根据服务器反馈的结果，提示用户终端进行升级和病毒库更新。

[0012] 一种电力数据传输装置，其中，包括：

设置模块，用于不同等级的安全工作区中设置缓存服务器，所述安全工作区中的各个服务器连接对应的缓存服务器，服务器与缓存服务器之间经虚拟专用网VPN连接；所述服务器的USB端口连接内置的安全加密芯片加密，设置BIOS，使系统只能从指定USB端口的安全加密芯片启动；系统开机，判断安全加密芯片是否正常工作，如不能正常工作，则系统自动关机；

授权模块，用于所述服务器根据用户类型为用户终端设置授权权限；

认证模块，用于所述服务器检测到用户的接入请求时，进行用户认证；

执行模块，用于认证成功后，根据用户终端发送的指令进行数据的存取、搜索和更改；并将该数据存储到缓存服务器中，在所述缓存服务器中根据被寻址次数进行排序。

[0013] 优选的，所述授权模块，包括：

分配子模块，用于服务器为用户分配信用值，根据所述信用值确定访问授权权限；

检测子模块，用于服务器检测到用户发送的访问授权请求，所述访问授权请求包括：用户ID、登陆密码和访问事项；

验证子模块，用于服务器将授权请求转化为多个访问授权子查询任务，分别对所述多个访问授权子查询任务进行验证，若通过验证，则通过所述访问授权请求，用户认证成功；若未通过验证，则拒绝所述访问授权请求，并将反馈结果发送给用户。

[0014] 优选的，所述认证模块，包括：

认证子模块，用于服务器检测到用户的接入请求时，首先进行用户认证，用户认证成功后，隔离到隔离网络区域，进行安全检测和风险评估，根据安全检测和风险评估结果确定是

否同意用户的接入请求，并将结果反馈给用户；所述安全检测包括恶意攻击检测、脆弱点检测、网络数据包捕获和网络拓扑检测；用户认证未成功，则拒绝接入请求。

[0015] 优选的，更新模块，用于所述服务器定期检测用户终端发送的终端安全信息、授权权限的使用状态，根据所述终端安全信息和授权权限的使用状态确定新的信用值。

[0016] 优选的，还包括反馈模块，用于若安全检测和风险评估未通过时，根据服务器反馈的结果，提示用户终端进行升级和病毒库更新。

[0017] 本发明的有益效果是：

随着计算机的普及和网络的发展，互联网的信息安全问题也越来越重要，尤其是对数据安全要求较多的部门，为了避免信息泄露等风险，内网计算机禁止连接互联网。本发明通过设置用户信用值和授权权限，进行用户认证，针对不同的用户类型和信用值，分配不同的授权权限，并对用户发起的访问授权请求，服务器将授权请求转化为多个访问授权子查询任务，分别对所述多个访问授权子查询任务进行验证，这种分布式查询的方式增加了验证的过程，进一步保证了信息安全。

[0018] 本发明在不同等级的安全工作区中设置缓存服务器，安全工作区中的各个服务器连接对应的缓存服务器，服务器与缓存服务器之间经虚拟专用网VPN连接，解决了现有电力二次系统中通信成本较高的问题，在外网访问服务器中的数据时，对于访问频率较高的数据，可在缓存服务器中快速查到，节约了时间成本。

[0019] 本发明服务器在接受用户终端的接入请求时，进行安全检测和风险评估，通过安全检测的结果进行风险评估，若风险评估后认为无风险或风险较小，则同意接入请求，若风险评估后认为风险较大，则不同意接入请求，同时将该结果反馈给用户终端。这种方式在身份认证的基础上进一步对网络安全进行判断，最大程度上避免了信息泄露的风险，且若判断出风险较大时，将该安全检测结果和风险评估结果反馈给用户终端，使用户终端能够及时发现自身存在的安全风险，通过升级、病毒库更新等方式确保终端的信息安全。

[0020] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0021] 图1为本发明一种电力数据传输方法的方法流程图。

[0022] 图2为本发明一种电力数据传输方法步骤S102的方法流程图。

[0023] 图3为本发明一种电力数据传输装置的原理框图。

[0024] 图4为本发明一种电力数据传输装置授权模块的原理框图。

具体实施方式

[0025] 下面结合附图和实施例对本发明作进一步描述。

[0026] 如图1所示，一种电力数据传输方法，包括如下步骤：

步骤S101，在不同等级的安全工作区中设置缓存服务器，所述安全工作区中的各个服务器连接对应的缓存服务器，服务器与缓存服务器之间经虚拟专用网VPN连接；所述服务器的USB端口连接内置的安全加密芯片加密，设置BIOS，使系统只能从指定USB端口的安全加

密芯片启动；系统开机，判断安全加密芯片是否正常工作，如不能正常工作，则系统自动关机；

步骤S102，所述服务器根据用户类型为用户终端设置授权权限；

步骤S103，所述服务器检测到用户的接入请求时，进行用户认证；

步骤S104，认证成功后，根据用户终端发送的指令进行数据的存取、搜索和更改；并将该数据存储到缓存服务器中，在所述缓存服务器中根据被寻址次数进行排序。

[0027] 该实施例中，按照被寻址的次数、频率、时标信息将数据进行排序，综合被寻址次数和频率进行排序，被寻址次数越多以及频率越高其排序的优先级越高，排序结果是一个动态变化的过程，根据被寻址次数及频率不断地更新。排序后增加排序索引，这里的排序索引可以是指针或链表。将经常被访问的数据存储在缓存服务器中，并根据被寻址次数(即访问次数)进行排序，在外网访问服务器中的数据时，对于访问频率较高的数据，可在缓存服务器中快速查到，节约了时间成本。

[0028] 所述服务器的USB端口连接内置的安全加密芯片加密，设置BIOS，使系统只能从指定USB端口的安全加密芯片启动；系统开机，判断安全加密芯片是否正常工作，如不能正常工作，则系统自动关机。如果安全加密芯片正常工作，系统从硬盘启动，保留一个VGA接口和内置的USB接口，关闭其它端口。

[0029] 本发明通过给服务器设置安全加密芯片，通过该加密芯片对系统进行加密管理，分别实现系统通讯数据加密，系统网络连接加密。有效防止了服务器外接互联网而导致信息泄露，感染病毒及木马等具有安全威胁的黑客软件。同时取消相应的外部硬件设备通讯及连接端口，以保证用户硬盘的信息数据不泄漏，保证服务器硬件系统信息的保密安全。

[0030] 在一个实施例中，如图2所示，步骤S102可实施为以下步骤：

步骤S201，服务器为用户分配信用值，根据所述信用值确定访问授权权限。

[0031] 步骤S202，服务器检测到用户发送的访问授权请求，所述访问授权请求包括：用户ID、登陆密码和访问事项。

[0032] 步骤S203，服务器将访问授权请求转化为多个访问授权子查询任务，分别对所述多个访问授权子查询任务进行验证，若通过验证，则通过所述访问授权请求，用户认证成功；若未通过验证，则拒绝所述访问授权请求，并将反馈结果发送给用户。

[0033] 根据授权规则将访问授权请求分解为多个子查询任务，再把这些子查询任务发送给不同的授权服务器进行验证，最终的授权结果是对多个子查询任务的综合判断。服务器包括存储数据的服务器和授权服务器，存储数据的服务器用于数据查询、调用、更改等操作，授权服务器根据授权规则对用户ID、登陆密码和访问事项进行授权，例如，根据用户类别对不同用户ID分配的访问事项权限不同，对一个用户进行访问授权时，需要登陆后获取信用值，再进行授权访问。如果是匿名用户或未知设备，需要分配相应的初始信用值。如果某一用户接入服务器引起信息泄露，则将该用户的信用值降低，并将该用户ID列为重点观察对象。

[0034] 在一个实施例中，步骤S103可实施为以下步骤：

服务器检测到用户的接入请求时，首先进行用户认证，用户认证成功后，隔离到隔离网络区域，进行安全检测和风险评估，根据安全检测和风险评估结果确定是否同意用户的接入请求，并将结果反馈给用户；所述安全检测包括恶意攻击检测、脆弱点检测、网络数据包

捕获和网络拓扑检测;用户认证未成功,则拒绝接入请求。

[0035] 服务器检测到用户接入请求时,进行网络安全检测,安全检测包括恶意攻击检测、脆弱点检测、网络数据包捕获和网络拓扑检测。脆弱点检测,指利用脆弱点扫描器找出网络各主机节点可能存在的脆弱点。根据安全检测结果进行风险识别、分析、评估,根据脆弱点存在的可信度和被利用的难易程序计算攻击成功发生的可能性,以得到最终的风险评估值。

[0036] 随着计算机的普及和网络的发展,互联网的信息安全问题也越来越重要,尤其是对数据安全要求较多的部门,为了避免信息泄露等风险,内网计算机禁止连接互联网。本发明通过设置用户信用值和授权权限,进行用户认证,针对不同的用户类型和信用值,分配不同的授权权限,并对用户发起的访问授权请求,服务器将授权请求转化为多个访问授权子查询任务,分别对所述多个访问授权子查询任务进行验证,这种分布式查询的方式增加了验证的过程,进一步保证了信息安全。

[0037] 本发明服务器在接受用户终端的接入请求时,进行安全检测和风险评估,通过安全检测的结果进行风险评估,若风险评估后认为无风险或风险较小,则同意接入请求,若风险评估后认为风险较大,则不同意接入请求,同时将该结果反馈给用户终端。这种方式在身份认证的基础上进一步对网络安全进行判断,最大程度上避免了信息泄露的风险,且若判断出风险较大时,将该安全检测结果和风险评估结果反馈给用户终端,使用户终端能够及时发现自身存在的安全风险,通过升级、病毒库更新等方式确保终端的信息安全。

[0038] 在一个实施例中,该实施例步骤S102还包括步骤S204,所述服务器定期检测用户终端发送的终端安全信息、授权权限的使用状态,根据所述终端安全信息和授权权限的使用状态确定新的信用值。

[0039] 在一个实施例中,该实施例步骤S102还包括步骤S205,若安全检测和风险评估未通过时,根据服务器反馈的结果,提示用户终端进行升级和病毒库更新。

[0040] 如图3所示,一种电力数据传输装置,包括:

设置模块101,用于不同等级的安全工作区中设置缓存服务器,所述安全工作区中的各个服务器连接对应的缓存服务器,服务器与缓存服务器之间经虚拟专用网VPN连接;所述服务器的USB端口连接内置的安全加密芯片加密,设置BIOS,使系统只能从指定USB端口的安全加密芯片启动;系统开机,判断安全加密芯片是否正常工作,如不能正常工作,则系统自动关机;

授权模块102,用于所述服务器根据用户类型为用户终端设置授权权限;

认证模块103,用于所述服务器检测到用户的接入请求时,进行用户认证;

执行模块104,用于认证成功后,根据用户终端发送的指令进行数据的存取、搜索和更改;并将该数据存储到缓存服务器中,在所述缓存服务器中根据被寻址次数进行排序。

[0041] 在一个实施例中,如图4所示,所述授权模块102,包括:

分配子模块201,用于服务器为用户分配信用值,根据所述信用值确定访问授权权限;

检测子模块202,用于服务器检测到用户发送的访问授权请求,所述访问授权请求包括:用户ID、登陆密码和访问事项;

验证子模块203,用于服务器将授权请求转化为多个访问授权子查询任务,分别对所述多个访问授权子查询任务进行验证,若通过验证,则通过所述访问授权请求,用户认证成

功;若未通过验证,则拒绝所述访问授权请求,并将反馈结果发送给用户。

[0042] 在一个实施例中,所述认证模块103,包括:

认证子模块,用于服务器检测到用户的接入请求时,首先进行用户认证,用户认证成功后,隔离到隔离网络区域,进行安全检测和风险评估,根据安全检测和风险评估结果确定是否同意用户的接入请求,并将结果反馈给用户;所述安全检测包括恶意攻击检测、脆弱点检测、网络数据包捕获和网络拓扑检测;用户认证未成功,则拒绝接入请求。

[0043] 在一个实施例中,所述授权模块102还包括:更新子模块,用于所述服务器定期检测用户终端发送的终端安全信息、授权权限的使用状态,根据所述终端安全信息和授权权限的使用状态确定新的信用值。

[0044] 在一个实施例中,所述授权模块102还包括:反馈子模块,用于若安全检测和风险评估未通过时,根据服务器反馈的结果,提示用户终端进行升级和病毒库更新。

[0045] 说明的是,以上实施例仅用以说明本发明的技术方案而非限制,本领域普通技术人员对本发明的技术方案所做的其他修改或者等同替换,只要不脱离本发明技术方案的精神和范围,均应涵盖在本发明的权利要求范围当中。

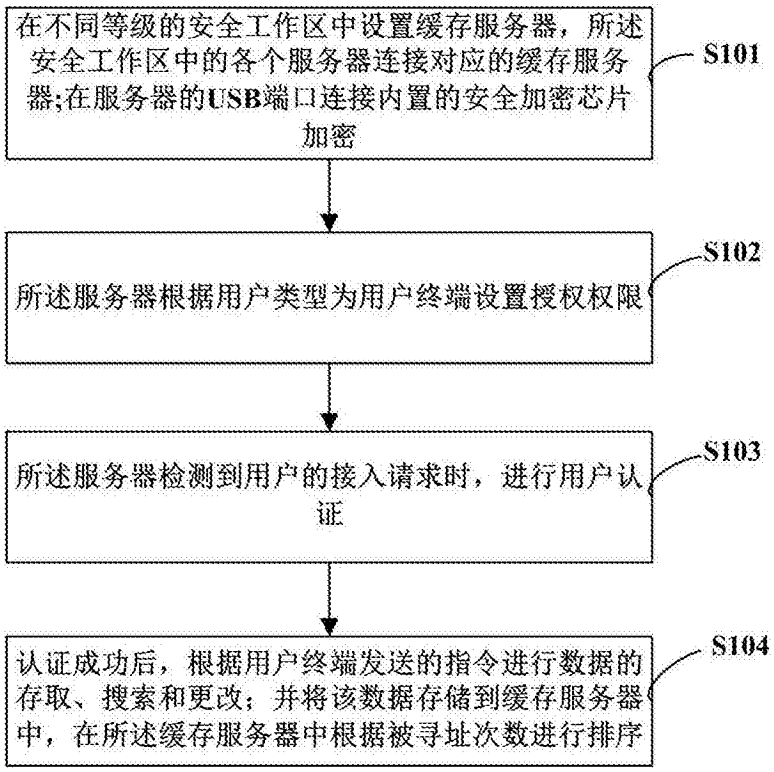

在不同等级的安全工作区中设置缓存服务器，所述安全工作区中的各个服务器连接对应的缓存服务器;在服务器的USB端口连接内置的安全加密芯片加密
S101
所述服务器根据用户类型为用户终端设置授权权限
S102
所述服务器检测到用户的接入请求时，进行用户认证
S103
认证成功后，根据用户终端发送的指令进行数据的存取、搜索和更改；并将该数据存储到缓存服务器中，在所述缓存服务器中根据被寻址次数进行排序
S104

图1

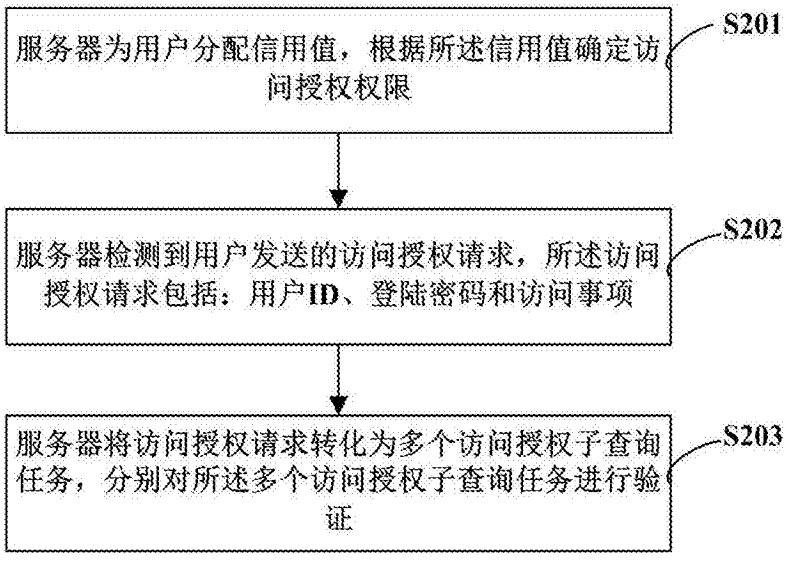

服务器为用户分配信用值，根据所述信用值确定访问授权权限
S201
服务器检测到用户发送的访问授权请求，所述访问授权请求包括：用户ID、登陆密码和访问事项
S202
服务器将访问授权请求转化为多个访问授权子查询任务，分别对所述多个访问授权子查询任务进行验证
S203

图2

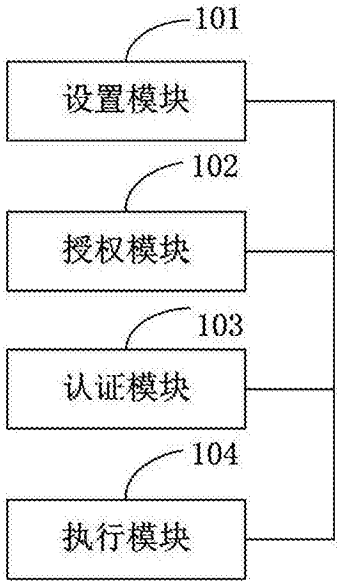

101
设置模块
102
授权模块
103
认证模块
104
执行模块

图3

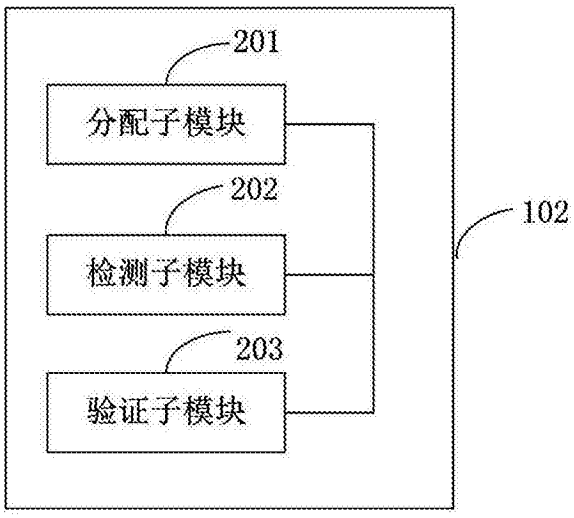


图4