(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 103023886 B
(45)授权公告日 2015.11.25

(21)申请号 201210488724.6

(22)申请日 2012.11.26

(73)专利权人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
专利权人 奇智软件(北京)有限公司

(72)发明人 邓振波 张家柱 温铭 李宇 刘娇

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

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

(56)对比文件
CN 101299760 A,2008.11.05,说明书第4页第2行至第5页第11行,第6页第3行至第8行.
CN 101650768 A,2010.02.17,全文.
CN 101924761 A,2010.12.22,说明书第[0007]-[0023]段,第[0028]-[0053]段.
CN 102710588 A,2012.10.03,说明书第44段至第84段.
汪锋.白名单主动防御系统的设计与实现.《中国优秀硕士学位论文全文数据库信息科技辑》.2012,(第04期),正文第30页第2行至第33页第4行,图4.5.

审查员 薛乐梅

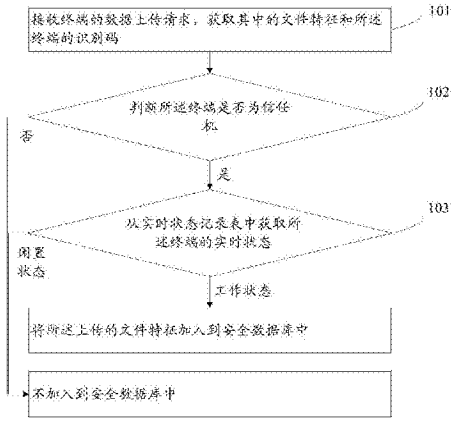
权利要求书2页 说明书7页 附图2页

(54)发明名称

安全数据处理方法及系统

(57)摘要

本申请提供了一种安全数据处理方法,包括以下步骤:安全控制服务器接收终端的数据上传请求,获取其中的文件特征和终端的识别码;安全控制服务器根据终端的识别码判断终端是否为信任机,信任机为其中的数据被认为是安全数据的终端;若终端为信任机,则安全控制服务器从实时状态记录表中获取终端的实时状态,若为工作状态,则将上传的文件特征加入到安全数据库中,若为闲置状态,则不加入到安全数据库中。本发明还提供一种实现前述方法的安全数据处理系统。本发明的安全数据处理方法及系统能够提高安全数据的更新效率。



CN 103023886 B

1. 一种安全数据处理方法，其特征在于，包括以下步骤：

安全控制服务器接收终端的数据上传请求，获取其中的文件特征和所述终端的识别码；

安全控制服务器根据所述终端的识别码判断所述终端是否为信任机，所述信任机为其中的数据被认为是安全数据的终端，其中，安全控制服务器预先对终端是否为信任机进行标识，所述标识存储在配置文件或关系表中，当安全控制服务器获取到终端的识别码，通过查询配置文件或关系表来判断该终端是否为信任机；

若所述终端被判断为信任机，则安全控制服务器从实时状态记录表中获取所述终端的实时状态，若为工作状态，则将所述上传的文件特征加入到安全数据库中，若为闲置状态，则不加入到安全数据库中；

所述安全数据处理方法在企业内网中实现。

2. 如权利要求 1 所述的安全数据处理方法，其特征在于，所述方法还包括：

变更所述终端的实时状态，所述终端的实时状态包括工作状态和闲置状态；

安全控制服务器根据变更后的实时状态对所述实时状态记录表中各终端的实时状态进行更新。

3. 如权利要求 2 所述的安全数据处理方法，其特征在于，变更所述终端的实时状态在终端中执行，所述方法还包括终端在实时状态变更后，将所述实时状态传输给安全控制服务器；

所述变更终端的实时状态包括：

监控终端上传文件特征后的时间，若超过第一预定时间，则将所述终端的工作状态变更为闲置状态；和 / 或

监控终端开机后的时间，若超过第二预定时间，则将所述终端的工作状态变更为闲置状态。

4. 如权利要求 3 所述的安全数据处理方法，其特征在于，所述监控终端上传文件特征后的时间包括：在监控到终端上传文件特征时，加载第一定时配置文件，所述第一定时配置文件的监测时长为第一预定时间；和 / 或

所述监控终端开机后的时间包括：在终端开机时，加载第二定时配置文件，所述第二定时配置文件的监测时长为第二预定时间。

5. 如权利要求 2 所述的安全数据处理方法，其特征在于，变更所述终端的实时状态在安全控制服务器中执行，所述变更终端的实时状态包括：

安全控制服务器监听外部输入的变更命令，根据所述变更命令将所述终端由工作状态变更为闲置状态或将所述终端由闲置状态变更为工作状态。

6. 如权利要求 5 所述的安全数据处理方法，其特征在于，所述安全控制服务器监听外部输入的变更命令，根据所述变更命令将所述终端由工作状态变更为闲置状态或将所述终端由闲置状态变更为工作状态包括：

获取外部输入的变更命令以及终端的识别码；

根据所述变更命令对具有所述识别码的终端进行实时状态变更。

7. 如权利要求 1 所述的安全数据处理方法，其特征在于，所述方法还包括：

采用加入到安全数据库中的文件特征识别其他终端的上传的文件特征信息的安全性。

8. 如权利要求 1 至 6 任一项所述的安全数据处理方法，其特征在于，所述实时状态记录表存储于所述安全控制服务器中，所述安全控制服务器根据实时获取的信息对其进行更新。

9. 一种安全数据处理系统，置于安全控制服务器中，其特征在于，包括 ：

信息接收模块，用于接收终端的数据上传请求，获取其中的文件特征和所述终端的识别码 ；

信任机判断模块，用于根据所述终端的识别码判断所述终端是否为信任机，若是，则触发实时状态获取模块，所述信任机为其中的数据被认为是安全数据的终端，其中，安全控制服务器预先对终端是否为信任机进行标识，所述标识存储在配置文件或关系表中，当安全控制服务器获取到终端的识别码，通过查询配置文件或关系表来判断该终端是否为信任机 ；

实时状态获取模块，用于从实时状态记录表中获取所述终端的实时状态，若为工作状态，则将所述上传的文件特征加入到安全数据库中，若为闲置状态，则不加入到安全数据库中，所述安全数据处理系统在企业内网中实现。

10. 如权利要求 9 所述的安全数据处理系统，其特征在于，所述系统还包括 ：

实时状态变更模块，用于变更所述终端的实时状态，所述终端的实时状态包括工作状态和闲置状态 ；和

更新模块，置于安全控制服务器中，用于根据实时状态变更模块的变更操作更新安全控制服务器的实时状态记录表中各终端的实时状态。

11. 如权利要求 10 所述的安全数据处理系统，其特征在于，所述实时状态变更模块置于终端中，所述系统还包括 ：

数据传输模块，置于终端中，用于终端在实时状态变更后，将所述实时状态传输给所述安全控制服务器中的更新模块 ；

所述实时状态变更模块包括 ：

时间监控子模块，用于监控终端上传文件特征后的时间，若超过第一预定时间，则将所述终端的工作状态变更为闲置状态 ；和 / 或监控终端开机后的时间，若超过第二预定时间，则将所述终端的工作状态变更为闲置状态。

12. 如权利要求 10 所述的安全数据处理系统，其特征在于，所述实时状态变更模块置于安全控制服务器中，包括 ：

命令接收子模块，用于安全控制服务器监听外部输入的变更命令，根据所述变更命令将所述终端由工作状态变更为闲置状态或将所述终端由闲置状态变更为工作状态。

13. 如权利要求 12 所述的安全数据处理系统，其特征在于，所述命令接收子模块包括 ：

信息获取单元，用于获取外部输入的变更命令以及终端的识别码 ；

变更单元，用于根据所述变更命令对具有所述识别码的终端进行实时状态变更。

14. 如权利要求 9 所述的安全数据处理系统，其特征在于，所述系统还包括 ：

识别对比模块，用于采用加入到安全数据库中的文件特征识别其他终端的上传的文件特征信息的安全性。

安全数据处理方法及系统

技术领域

[0001] 本发明涉及计算机安全技术领域，具体涉及一种安全数据处理方法及系统。

背景技术

[0002] 私有云是为企业单独部署的计算机安全系统，可以有效的保证内部数据的安全性。一般来说，在私有云系统中，终端将本地不能辨别安全的文件特征信息上传至安全控制服务器，安全控制服务器通过内部存储的安全信息数据库来对文件特征信息进行识别，将识别结果传输给终端，从而实现内部数据的安全管理。

[0003] 此种方式可以保证企业内部数据的安全，但是当终端上传给安全控制服务器的数据量较大，或者上传并发量较大时，安全控制服务器往往无法快速响应，降低了处理效率，在严重时，甚至可能导致安全控制服务器无法响应等问题。当安全控制服务器中没有相关文件特征信息时，便无法对终端上传的文件特征信息进行识别，因此，此种方式对于安全控制服务器中安全信息数据库中的数据的时效性要求较高。为了保证有效准确的对终端上传的文件特征信息进行识别，安全控制服务器需要实时并快速对安全信息数据进行更新，但是目前往往需要通过人工操作的方式来实现，或者通过文件特征逐一比对的方式来实现，更新花费的时间较长，效率较低。

发明内容

[0004] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的安全数据处理方法及系统。

[0005] 依据本发明的一个方面，提供了一种安全数据处理方法，包括以下步骤：

[0006] 安全控制服务器接收终端的数据上传请求，获取其中的文件特征和终端的识别码；

[0007] 安全控制服务器根据终端的识别码判断终端是否为信任机，信任机为其中的数据被认为是安全数据的终端；

[0008] 若终端被判断为信任机，则安全控制服务器从实时状态记录表中获取终端的实时状态，若为工作状态，则将上传的文件特征加入到安全数据库中，若为闲置状态，则不加入到安全数据库中。

[0009] 可选地，方法还包括：

[0010] 变更终端的实时状态，终端的实时状态包括工作状态和闲置状态；

[0011] 安全控制服务器根据变更后的实时状态对实时状态记录表中各终端的实时状态进行更新。

[0012] 可选地，变更终端的实时状态在终端中执行，方法还包括终端在实时状态变更后，将实时状态传输给安全控制服务器；

[0013] 变更终端的实时状态包括：

[0014] 监控终端上传文件特征后的时间，若超过第一预定时间，则将终端的工作状态变

更为闲置状态；和 / 或

[0015] 监控终端开机后的时间，若超过第二预定时间，则将终端的工作状态变更为闲置状态。

[0016] 可选地，监控终端上传文件特征后的时间包括：在监控到终端上传文件特征时，加载第一定时配置文件，第一定时配置文件的监测时长为第一预定时间；和 / 或

[0017] 监控终端开机后的时间包括：在终端开机时，加载第二定时配置文件，第二定时配置文件的监测时长为第二预定时间。

[0018] 可选地，变更终端的实时状态在安全控制服务器中执行，变更终端的实时状态包括：

[0019] 安全控制服务器监听外部输入的变更命令，根据变更命令将终端由工作状态变更为闲置状态或将终端由闲置状态变更为工作状态。

[0020] 可选地，安全控制服务器监听外部输入的变更命令，根据变更命令将终端由工作状态变更为闲置状态或将终端由闲置状态变更为工作状态包括：

[0021] 获取外部输入的变更命令以及终端的识别码；

[0022] 根据变更命令对具有识别码的终端进行实时状态变更。

[0023] 可选地，方法还包括：

[0024] 采用加入到安全数据库中的文件特征识别其他终端的上传的文件特征信息的安全性。

[0025] 可选地，安全数据处理方法在企业内网中实现。

[0026] 可选地，实时状态记录表存储于安全控制服务器中，安全控制服务器根据实时获取的信息对其进行更新。

[0027] 根据本发明的另一方面，提供了一种安全数据处理系统，置于安全控制服务器中，包括：

[0028] 信息接收模块，用于接收终端的数据上传请求，获取其中的文件特征和终端的识别码；

[0029] 信任机判断模块，用于根据终端的识别码判断终端是否为信任机，若是，则触发实时状态获取模块，信任机为其中的数据被认为是安全数据的终端；

[0030] 实时状态获取模块，用于从实时状态记录表中获取终端的实时状态，若为工作状态，则将上传的文件特征加入到安全数据库中，若为闲置状态，则不加入到安全数据库中。

[0031] 可选地，系统还包括：

[0032] 实时状态变更模块，用于变更终端的实时状态，终端的实时状态包括工作状态和闲置状态；和

[0033] 更新模块，置于安全控制服务器中，用于根据实时状态变更模块的变更操作更新安全控制服务器的实时状态记录表中各终端的实时状态。

[0034] 可选地，实时状态变更模块置于终端中，系统还包括：

[0035] 数据传输模块，置于终端中，用于终端在实时状态变更后，将实时状态传输给安全控制服务器中的更新模块；

[0036] 实时状态变更模块包括：

[0037] 时间监控子模块，用于监控终端上传文件特征后的时间，若超过第一预定时间，则

将终端的工作状态变更为闲置状态；和 / 或监控终端开机后的时间，若超过第二预定时间，则将终端的工作状态变更为闲置状态。

[0038] 可选地，实时状态变更模块置于安全控制服务器中，包括：

[0039] 命令接收子模块，用于安全控制服务器监听外部输入的变更命令，根据变更命令将终端由工作状态变更为闲置状态或将终端由闲置状态变更为工作状态。

[0040] 可选地，命令接收子模块包括：

[0041] 信息获取单元，用于获取外部输入的变更命令以及终端的识别码；

[0042] 变更单元，用于根据变更命令对具有识别码的终端进行实时状态变更。

[0043] 可选地，系统还包括：

[0044] 识别对比模块，用于采用加入到安全数据库中的文件特征识别其他终端的上传的文件特征信息的安全性。

[0045] 本发明的安全数据处理方法及系统通过前述的将设置为信任机的终端进行实时状态的区分以及转化，使处于工作状态的终端能够被安全控制服务器信任，而处于闲置状态的终端则需要对其进行安全验证，只有当其状态再次处于工作状态时，才会被安全控制服务器信任。即使处于闲置状态的信任机被仿造，但是安全控制服务器并不会信任其上传的信息，因此可以很好的保证安全控制服务器中数据的安全。在此过程中，只需要通过在安全控制服务器中维护实时状态记录表便可以实现信任机的安全监控，提高了安全数据更新的效率，且可以在保证安全的同时降低维护成本。

[0046] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0047] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0048] 图 1 示出了根据本发明实施例一的安全数据处理方法的流程图；

[0049] 图 2 示出了根据本发明实施例二的安全数据处理方法的流程图；

[0050] 图 3 示出了根据本发明实施例一的安全数据处理系统的结构图；以及

[0051] 图 4 示出了根据本发明实施例二的安全数据处理系统的结构图。

具体实施方式

[0052] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0053] 本发明的安全数据处理方法是对企业内网的数据安全进行处理，应用在企业内部的私有云系统中。由私有云系统中的安全控制服务器来实现识别和判断，完成对企业内网的安全数据库的更新，保证安全数据库更新的时效性和效率。其中，安全控制服务器是指在

私有云系统被设置为安全的服务端。一般来说，因为私有云系统中可能只有一个服务端，或者有多个服务端时，所有服务端都需要保证是安全的，此时，安全控制服务器也可以是所有的服务端。

[0054] 参照图 1，示出本发明的安全数据处理方法实施例一，包括以下步骤：

[0055] 步骤 101，安全控制服务器接收终端的数据上传请求，获取其中的文件特征和所述终端的识别码。

[0056] 在私有云系统的安全控制服务器中，预先存储与该安全控制服务器进行数据交互的所有终端的识别码。具体的，可以以配置文件、关系表等方式进行存储。其中，终端的识别码可以是终端的编号、特征码等能够唯一识别出该终端的标识。文件特征可以是文件的 MD5 值或者其他能够识别出文件的标识数据。

[0057] 当终端向安全控制服务器上传数据时，在数据上传请求中会包含终端的识别码以及需要上传的文件特征。安全控制服务器可以直接从终端的上传请求中获取这些信息。

[0058] 步骤 102，安全控制服务器根据所述终端的识别码判断所述终端是否为信任机，若是，则进行步骤 103；所述信任机为其中的数据被认为是安全数据的终端。

[0059] 其中，信任机可以通过人为设置和维护，即安全信息操作人员可以根据预定的规则和方式来将私有云系统中的某些终端的等级设置为安全，即将这些终端设置为信任机，并在安全控制服务器中存储相关的信息，安全控制服务器则可以信任这些终端，被设置为信任机的终端，其中的数据都会被认为是安全数据，对于其上传的文件或者文件特征信息都可以认为是安全的。

[0060] 具体的，安全控制服务器中会预先对终端是否为信任机进行标识，相关标识可以存储在配置文件或关系表中，当安全控制服务器获取到终端的识别码，并可以通过查询配置文件或关系表来判断该终端是否为信任机。若是，再进行下一步的判断。若不是，则不会将文件特征加入到安全数据库中，此时，可以根据实际情况对上传请求进行处理，若上传请求是请求将文件特征加入安全数据库，则安全控制服务器可以拒绝本次上传请求或不做相应，若上传请求是请求对文件特征进行识别，那么则可以将文件特征与安全数据库中已经存储的信息进行比较，然后将识别结果返回给终端。

[0061] 步骤 103，安全控制服务器从实时状态记录表中获取所述终端的实时状态，若为工作状态，则将所述上传的文件特征加入到安全数据库中，若为闲置状态，则不加入到安全数据库中。

[0062] 本发明中，被设置为信任机的终端的实时状态包括工作状态和闲置状态两种。对于被设置为信任机的终端，安全控制服务器只信任处于工作状态的终端，当其处于闲置状态时，安全控制服务器也不会信任其上传的文件。通过此种方式，可以保证上传数据的安全性。对于判断为闲置状态的终端的上传请求，可以根据实际情况处理，若上传请求是请求将文件特征加入安全数据库，则安全控制服务器可以拒绝本次上传请求或不做相应，若上传请求是请求对文件特征进行识别，那么则可以将文件特征与安全数据库中已经存储的信息进行比较，然后将识别结果返回给终端。

[0063] 可以理解，对于加入到安全数据库中的文件特征，安全控制服务器可以用于进行内网数据的安全管理，例如用于对其他终端上传的文件特征进行比对识别，例如判断后续上传的文件特征的安全性等等。

[0064] 在本发明的实际处理过程中，需要对被设置为信任机的终端的实时状态进行监控，并根据监控情况对终端的实时状态进行变更。安全控制服务器中维护有实时状态记录表，当作为信任机的终端的实时状态发生改变时，便需要在该实时状态记录表中进行对应修改，从而保证安全控制服务器中存储的是最新状态。为了保证数据读取的时效性和数据的安全性，实时状态记录表优选存储于安全控制服务器中。可以理解，实时状态记录表也可以存储在其他服务器或者数据库中，当需要时，安全控制服务器可以从存储的位置直接读取其中的信息。

[0065] 其中，监控以及变更终端的实时状态可以在安全控制服务器中执行，也可以在终端中执行。

[0066] 当在安全控制服务器中执行时，所述变更终端的实时状态包括：安全控制服务器监听外部输入的变更命令，根据所述变更命令将所述终端由工作状态变更为闲置状态或将所述终端由闲置状态变更为工作状态。具体的，前述过程可以通过如下方式来实现：获取外部输入的变更命令以及终端的识别码；根据所述变更命令对具有所述识别码的终端进行实时状态变更。另外，对于处于工作状态的终端来说，安全控制服务器还可以通过判断在预定时间内，终端与安全控制服务器是否有数据交互来执行。若超过预定时间，终端与安全控制服务器没有数据交互，则安全控制服务器可以将终端的工作状态变更为闲置状态。

[0067] 当在终端中执行时，终端还需要将变更后的实时状态实时传输给安全控制服务器，以供安全控制服务器对实时状态记录表进行更新。此时，变更终端的实时状态包括：监控终端上传文件特征后的时间，若超过第一预定时间，则将所述终端的工作状态变更为闲置状态；和/或监控终端开机后的时间，若超过第二预定时间，则将所述终端的工作状态变更为闲置状态。对于时间的监控，可以通过定时器也可以通过配置文件来实现。以配置文件为例，对于终端上传文件特征后的时间的监控，可以采用如下方式：在监控到终端上传文件特征时，加载第一定时配置文件，所述第一定时配置文件的监测时长为第一预定时间。对于终端开机后的时间的监控，可以采用如下方式：在终端开机时，加载第二定时配置文件，所述第二定时配置文件的监测时长为第二预定时间。

[0068] 可以理解，对于前述两种时间的监控，可以选择一种作为变更的触发条件，也可以两者相结合。即，可以仅监控终端上传文件特征后的时间，也可以仅监控终端开机后的时间，或者，二者同时监控，只要满足其中一个条件，便触发实时状态的变更。

[0069] 如前所述，为了保证信任机的安全，对于将工作状态变更为闲置状态可以通过前述的多种途径，只要满足其中一个条件，便可以出发变更。而对于将闲置状态变更为工作状态，则需要通过外部输入控制命令的方式。通过此种方式，可以避免信任机被仿造，保证数据安全。

[0070] 通过前述的将设置为信任机的终端进行实时状态的区分以及转化，使处于工作状态的终端能够被安全控制服务器信任，而处于闲置状态的终端则需要对其进行安全验证，只有当其状态再次处于工作状态时，才会被安全控制服务器信任。即使处于闲置状态的信任机被仿造，但是安全控制服务器并不会信任其上传的信息，因此可以很好的保证安全控制服务器中数据的安全。在此过程中，只需要通过在安全控制服务器中维护实时状态记录表便可以实现信任机的安全监控，提高了安全数据更新的效率，且可以在保证安全的同时降低维护成本。

[0071] 参照图 2，示出本发明的安全数据处理系统实施例一，置于安全控制服务器中，包括信息接收模块 10、信任机判断模块 20 和实时状态获取模块 30。

[0072] 信息接收模块 10，用于接收终端的数据上传请求，获取所述数据上传请求中包含的文件特征和所述终端的识别码。

[0073] 信任机判断模块 20，用于根据所述终端的识别码判断所述终端是否为信任机，若是，则触发实时状态获取模块，所述信任机为其中的数据被认为是安全数据的终端。

[0074] 实时状态获取模块 30，用于从实时状态记录表中获取所述终端的实时状态，若为工作状态，则将所述上传的文件特征加入到安全数据库中，若为闲置状态，则不加入到安全数据库中。

[0075] 优选地，该安全数据处理系统还包括实时状态变更模块 50 和更新模块 60（如图 3 和图 4 所示）。其中，该实时状态变更模块可以置于安全控制服务器中，也可以置于终端中，或者二者中同时都设置实时状态变更模块。

[0076] 实时状态变更模块，用于变更所述终端的实时状态，所述终端的实时状态包括工作状态和闲置状态。

[0077] 更新模块，置于安全控制服务器中，用于根据实时状态变更模块的变更操作更新安全控制服务器的实时状态记录表中各终端的实时状态。

[0078] 参照图 3，示出本申请的安全数据处理系统实施例二，当实时状态变更模块 50 置于终端中时，该系统还包括数据传输模块 52，置于终端中，用于终端在实时状态变更后，将所述实时状态传输给安全控制服务器中的更新模块 60。此时，实时状态变更模块包括时间监控子模块，用于监控终端上传文件特征后的时间，若超过第一预定时间，则将所述终端的工作状态变更为闲置状态；和 / 或监控终端开机后的时间，若超过第二预定时间，则将所述终端的工作状态变更为闲置状态。

[0079] 参照图 4，示出本申请的安全数据处理系统实施例三，实时状态变更模块 50 置于安全控制服务器中，此时，其包括命令接收子模块，用于安全控制服务器监听外部输入的变更命令，根据所述变更命令将所述终端由工作状态变更为闲置状态或将所述终端由闲置状态变更为工作状态。此时，实时状态变更模块 50 需要将变更操作传输给更新模块 60，从而使其更新安全控制服务器的实时状态记录表中各终端的实时状态。

[0080] 优选地，命令接收子模块包括信息获取单元和变更单元。信息获取单元，用于获取外部输入的变更命令以及终端的识别码。变更单元，用于根据所述变更命令对具有所述识别码的终端进行实时状态变更。

[0081] 可以理解，在前述实施例的基础上，该系统还包括识别对比模块，用于采用加入到安全数据库中的文件特征识别其他终端的上传的文件特征信息的安全性。

[0082] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0083] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构

和技术，以便不模糊对本说明书的理解。

[0084] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0085] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和／或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0086] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0087] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0088] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

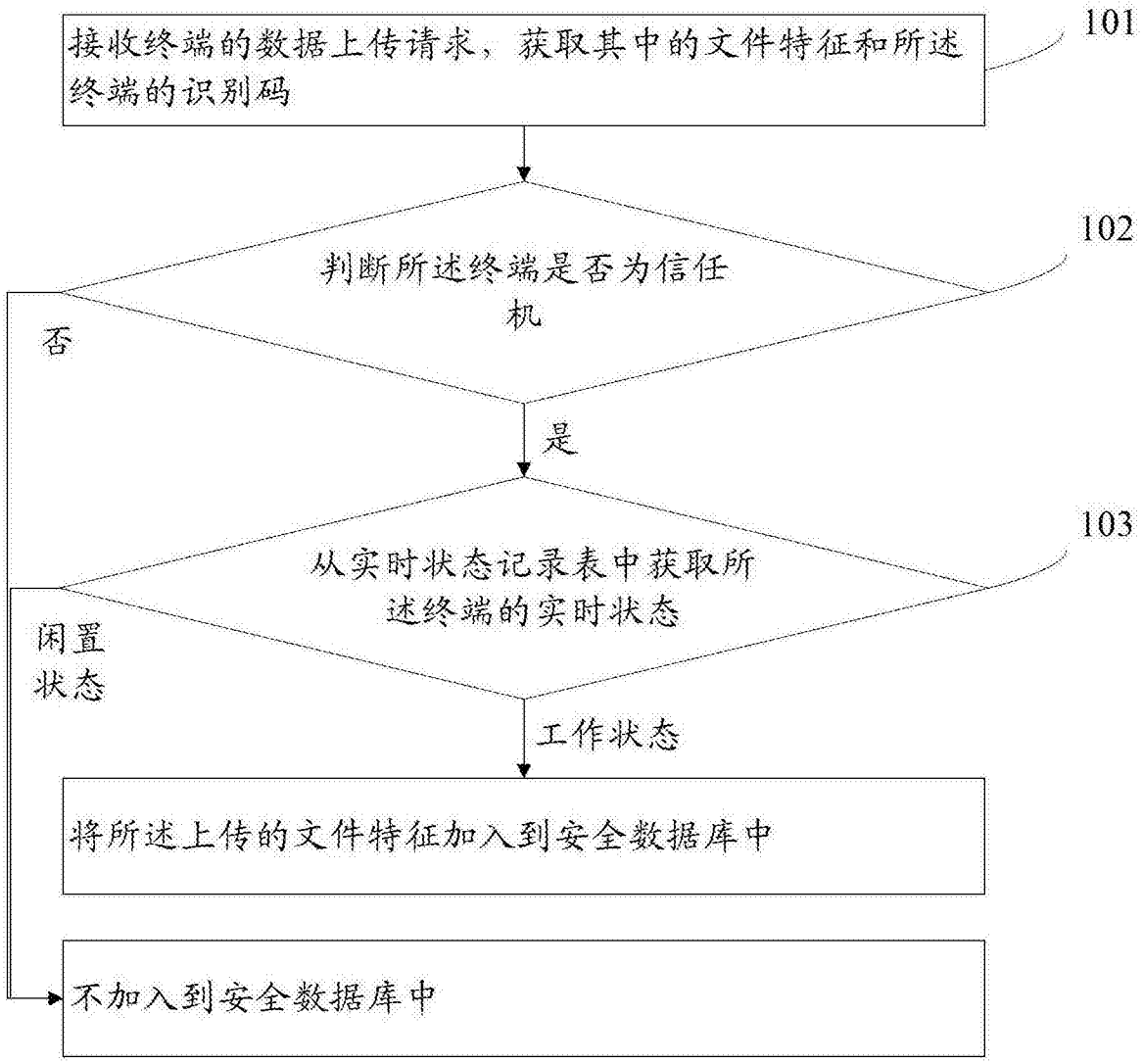

接收终端的数据上传请求，获取其中的文件特征和所述终端的识别码
101
判断所述终端是否为信任机
102
否
是
从实时状态记录表中获取所述终端的实时状态
103
闲置状态
工作状态
将所述上传的文件特征加入到安全数据库中
不加入到安全数据库中

图 1

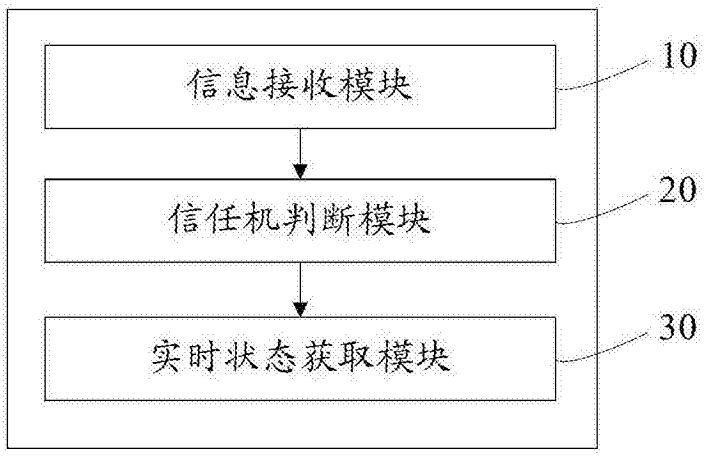

信息接收模块
10
信任机判断模块
20
实时状态获取模块
30

图 2

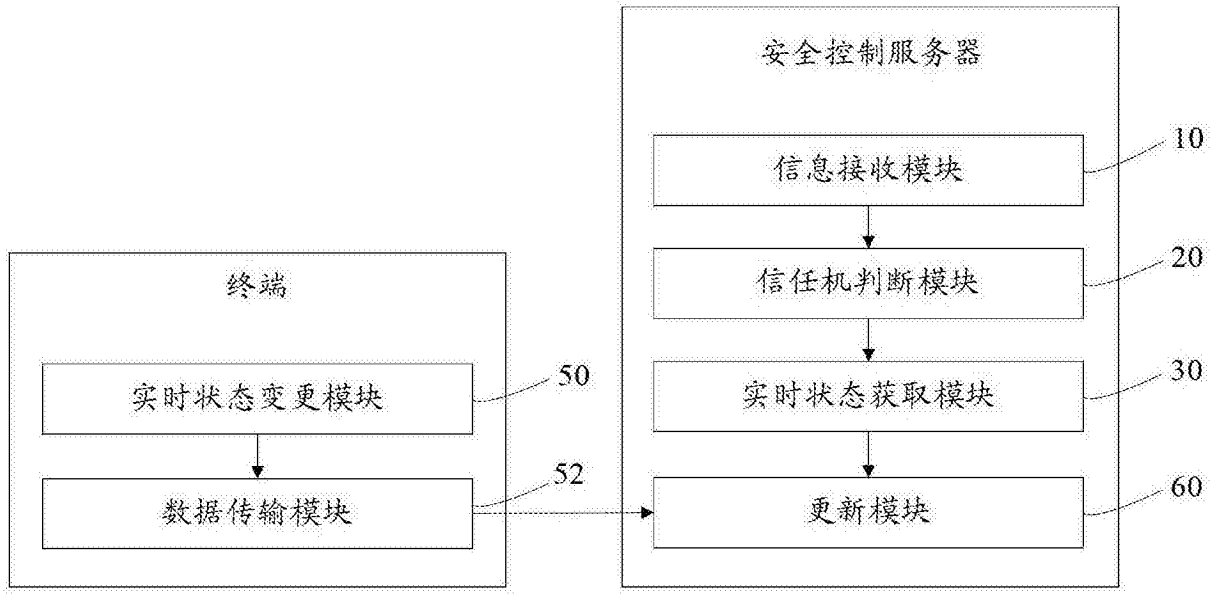

安全控制服务器
信息接收模块
10
信任机判断模块
20
实时状态获取模块
30
更新模块
60
终端
实时状态变更模块
50
数据传输模块
52

图 3

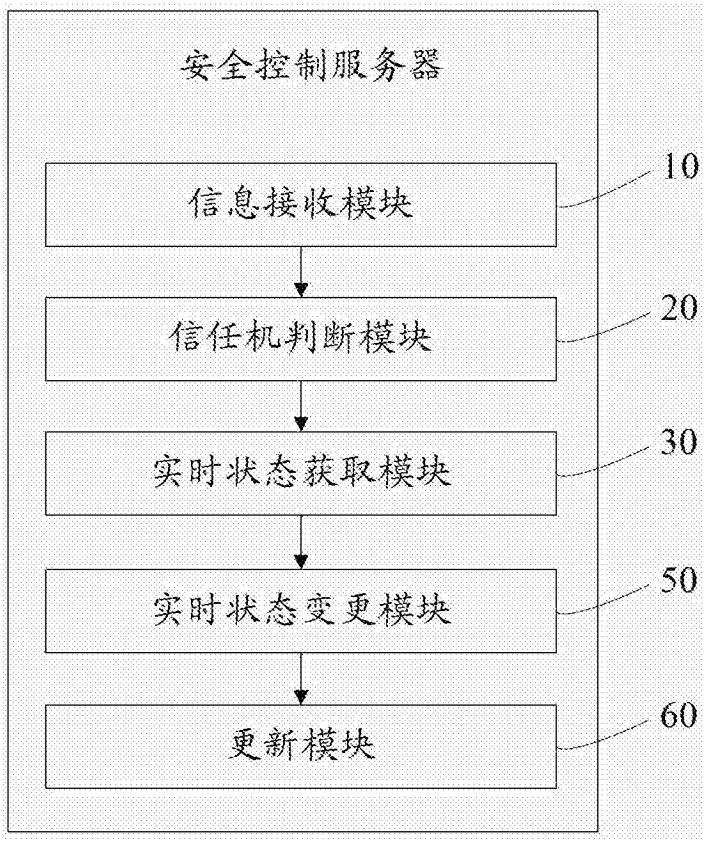

安全控制服务器
信息接收模块
10
信任机判断模块
20
实时状态获取模块
30
实时状态变更模块
50
更新模块
60

图 4