(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 112769782 A
(43)申请公布日 2021.05.07

(21)申请号 202011602730.0

(22)申请日 2020.12.29

(71)申请人 上海联蔚盘云科技有限公司
地址 200231 上海市徐汇区平福路188号2号楼五楼

(72)发明人 徐正昊 高海峰 赵平

(74)专利代理机构 上海剑秋知识产权代理有限公司 31382
代理人 杨飞

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 17/18(2006.01)

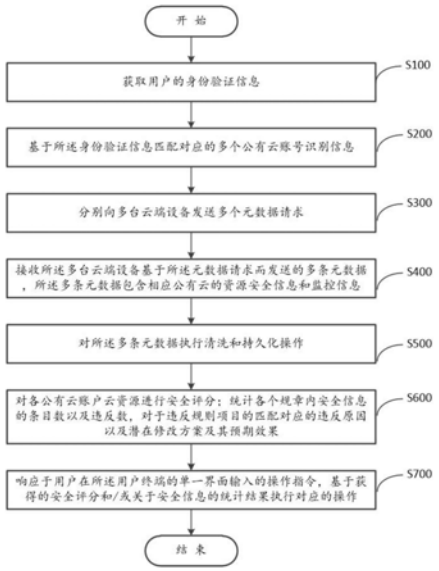
权利要求书2页 说明书16页 附图3页

(54)发明名称

多云安全基线管理的方法与设备

(57)摘要

本发明提供了一种多云安全基线管理的方法,应用于一用户终端,所述方法包括:获取用户的身份验证信息,所述身份验证信息匹配对应的多个公有云账号识别信息;基于所述多个公有云账号识别信息分别向多台云端设备发送多个元数据请求;接收所述多台云端设备基于所述元数据请求而发送的多条元数据,所述多条元数据包含相应公有云的资源安全信息和监控信息;对所述多条元数据执行清洗和持久化操作;根据获取的所述安全信息和所述监控信息,对各公有云账户云资源进行安全评分;统计各个规章内安全信息的条目数以及违反数,对于违反规则项目的匹配对应的违反原因以及潜在修改方案及其预期效果。



CN 112769782 A

1.一种多云安全基线管理的方法,其特征在于,应用于一用户终端,所述方法包括:

获取用户的身份验证信息,所述身份验证信息匹配对应的多个公有云账号识别信息;

基于所述多个公有云账号识别信息分别向多台云端设备发送多个元数据请求;

接收所述多台云端设备基于所述元数据请求而发送的多条元数据,所述多条元数据包含相应公有云的资源安全信息和监控信息;

对所述多条元数据执行清洗和持久化操作;

根据获取的所述安全信息和所述监控信息,对各公有云账户云资源进行安全评分;统计各个规章内安全信息的条目数以及违反数,对于违反规则项目的匹配对应的违反原因以及潜在修改方案及其预期效果;

响应于用户在所述用户终端的单一界面输入的操作指令,基于获得的安全评分和/或关于安全信息的统计结果执行对应的操作。

2.根据权利要求1所述的方法,其特征在于,所述分别向多台云端设备发送多个元数据请求的步骤,包括:

基于预设的时间间隔分别向多台云端设备发送多个元数据请求。

3.根据权利要求1所述的方法,其特征在于,针对任一公有云账户云资源进行安全评分的步骤,包括:

计算所述公有云账户云资源的总得分;

计算所述公有云账户云资源的总失分;

所述总得分减去所述总失分获得最终的安全评分。

4.根据权利要求3所述的方法,其特征在于,所述计算所述公有云账户云资源的总得分的步骤,包括:

计算单个实例中所有监控指标的得分总和,获得单个实例的得分;

计算单类资源中所有单个实例的得分总和,获得单类资源的得分;

根据单类资源的得分及其包括的实例数量,计算获得单类资源的平均得分;

将各单类资源的平均得分加权后相加,获得所述公有云账户云资源的总得分。

5.根据权利要求4所述的方法,其特征在于,单项监控指标的得分为其加分值与预设得分系数的乘积,其中所述单项监控指标的加分值由相应公有云的资源安全信息所限定。

6.根据权利要求3所述的方法,其特征在于,所述计算所述公有云账户云资源的总失分的步骤,包括:

计算单个实例中所有监控指标的失分总和,获得单个实例的失分;

计算单类资源中所有单个实例的失分总和,获得单类资源的失分;

根据单类资源的失分及其包括的实例数量,计算单类资源的平均失分;

将各单类资源的平均失分加权后相加,获得所述公有云账户云资源的总失分。

7.根据权利要求6所述的方法,其特征在于,单项监控指标的失分为其减分值、预设失分系数及风险影响系数的乘积,其中所述单项监控指标的减分值由相应公有云的资源安全信息所限定,所述风险影响系数由预设的时间风险系数与检测失效距今的天数所限定。

8.根据权利要求1所述的方法,其特征在于,针对任一公有云账户云资源进行安全评分的计算公式如下:

$$Sum = \sum_{m=1}^{m=max} \varepsilon_m \frac{\sum_{n=1}^{n=max} \phi_n(A,k)}{S_m} - \sum_{m=1}^{m=max} \varepsilon_m \frac{\sum_{n=1}^{n=max} \left(\sum_{i=1}^{i=max} |0 - A_i| * j_i * \omega(t,u) \right)_n}{S_m}$$

$$\phi(\mathrm{A},\mathrm{k}) = \sum_{i=1}^{i=max} (\mathrm{A}_i - 0) * \mathrm{k}_i$$

$\omega(t,u) = ut^2$

其中，(A_i-0)表示单项监控指标的得分值，$|0-A_i|$表示单项监控指标的失分值，i为单个实例中监控指标的编号，k为得分系数，j为失分系数，u为时间风险系数，t为检测失效距今的天数，n为单类资源中实例的编号，m为资源类的编号，S表示单类资源中实例的总数，ε表示单类资源的安全分数系数。

9.一种多云安全基线管理的设备，其特征在于，所述设备包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行根据权利要求1至8中任一项所述方法的操作。

10.一种存储指令的计算机可读介质，其特征在于，所述指令在被执行时使得系统执行根据权利要求1至8中任一项所述方法的操作。

多云安全基线管理的方法与设备

技术领域

[0001] 本发明涉及云计算领域，尤其涉及一种多云安全基线管理的方法及系统与设备。

背景技术

[0002] 经过多年的发展历程，公有云已成为众多领域内各大企业计算和存储的首选。云计算和云存储也正处于高速发展期，而多云资源安全管理是企业发展的必经阶段。

[0003] 1)企业提倡信息化、数字化、敏捷化，公有云资源随取随用特性被重视。

[0004] 2)企业减轻财务负担，公有云具有共享资源服务的核心属性。

[0005] 3)着眼于不同公有云所各自具有的特色，越来越多的企业会选择以多云形式使用。

[0006] 4)企业使用大量的多公有云资源，需要加强对资源的信息管理和安全管理。

[0007] 由于公有云资源都是虚拟化并处于供应商之处，企业对于敏感信息的保护以及服务高可用性的要求将会十分重视，尤其是一些有竞争力的行业，对于用户数据以及商业机密的信息的管理就会十分严格。如何统一管理和判断多公有云的资源是否拥有强大的保密性和高可用性就至关重要。

发明内容

[0008] 鉴于现有技术中的问题，本发明提供了一种多云安全基线管理的方法，应用于一用户终端，所述方法包括：

[0009] 获取用户的身份验证信息，所述身份验证信息匹配对应的多个公有云账号识别信息；

[0010] 基于所述多个公有云账号识别信息分别向多台云端设备发送多个元数据请求；

[0011] 接收所述多台云端设备基于所述元数据请求而发送的多条元数据，所述多条元数据包含相应公有云的资源安全信息和监控信息；

[0012] 对所述多条元数据执行清洗和持久化操作；

[0013] 根据获取的所述安全信息和所述监控信息，对各公有云账户云资源进行安全评分；统计各个规章内安全信息的条目数以及违反数，对于违反规则项目的匹配对应的违反原因以及潜在修改方案及其预期效果；

[0014] 响应于用户在所述用户终端的单一界面输入的操作指令，基于获得的安全评分和/或关于安全信息的统计结果执行对应的操作。

[0015] 进一步地，所述分别向多台云端设备发送多个元数据请求的步骤，包括：

[0016] 基于预设的时间间隔分别向多台云端设备发送多个元数据请求。

[0017] 进一步地，针对任一公有云账户云资源进行安全评分的步骤，包括：

[0018] 计算所述公有云账户云资源的总得分；

[0019] 计算所述公有云账户云资源的总失分；

[0020] 所述总得分减去所述总失分获得最终的安全评分。

[0021] 进一步地,所述计算所述公有云账户云资源的总得分的步骤,包括:

[0022] 计算单个实例中所有监控指标的得分总和,获得单个实例的得分;

[0023] 计算单类资源中所有单个实例的得分总和,获得单类资源的得分;

[0024] 根据单类资源的得分及其包括的实例数量,计算获得单类资源的平均得分;

[0025] 将各单类资源的平均得分加权后相加,获得所述公有云账户云资源的总得分。

[0026] 进一步地,单项监控指标的得分为其加分值与预设得分系数的乘积,其中所述单项监控指标的加分值由相应公有云的资源安全信息所限定。

[0027] 进一步地,所述计算所述公有云账户云资源的总失分的步骤,包括:

[0028] 计算单个实例中所有监控指标的失分总和,获得单个实例的失分;

[0029] 计算单类资源中所有单个实例的失分总和,获得单类资源的失分;

[0030] 根据单类资源的失分及其包括的实例数量,计算单类资源的平均失分;

[0031] 将各单类资源的平均失分加权后相加,获得所述公有云账户云资源的总失分。

[0032] 进一步地,单项监控指标的失分为其减分值、预设失分系数及风险影响系数的乘积,其中所述单项监控指标的减分值由相应公有云的资源安全信息所限定,所述风险影响系数由预设的时间风险系数与检测失效距今的天数所限定。

[0033] 进一步地,针对任一公有云账户云资源进行安全评分的计算公式如下:

[0034] $$Sum=\sum_{m=1}^{m=max}\varepsilon_m\frac{\sum_{n=1}^{n=max}\phi_n(A,k)}{S_m}-\sum_{m=1}^{m=max}\varepsilon_m\frac{\sum_{n=1}^{n=max}\left(\sum_{i=1}^{i=max}|0-A_i|*j_i*\omega(t,u)\right)_n}{S_m}$$

[0035] $$\phi(\mathrm{A},\mathrm{k})=\sum_{i=1}^{i=max}(\mathrm{A}_i-0)*\mathrm{k}_i$$

[0036] $\omega(t,u)=ut^2$

[0037] 其中,(A_i-0)表示单项监控指标的得分值,$|0-A_i|$表示单项监控指标的失分值,i为单个实例中监控指标的编号,k为得分系数,j为失分系数,u为时间风险系数,t为检测失效距今的天数,n为单类资源中实例的编号,m为资源类的编号,S表示单类资源中实例的总数,ε表示单类资源的安全分数系数。

[0038] 本发明还提供了一种多云安全基线管理的设备,所述设备包括:

[0039] 处理器;以及

[0040] 被安排成存储计算机可执行指令的存储器,所述可执行指令在被执行时使所述处理器执行上述方法的操作。

[0041] 本发明还提供了一种存储指令的计算机可读介质,所述指令在被执行时使得系统执行上述方法的操作。

[0042] 与现有技术相比,本发明的多云安全基线管理的方法与设备将多云中获取到的资源安全和监控信息,通过统一终端集中管理,以安全基线为标准帮助企业IT人员在多云多账号的环境下,维护资源安全,保证信息私有化。采用本发明的方法与设备可以帮助用户实现威胁检测、响应、溯源的自动化安全运营闭环,保护云上资产和信息安全并满足监管合规要求,帮助用户了解云资源的漏洞以及不合规的地方,通过评分预警和分析以改善用户在云上使用的不合规设置。

附图说明

[0043] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述,本发明的其它特征、目的和优点将会变得更明显:

[0044] 图1示出本发明一个实施例的一种多云安全基线管理的方法的流程;

[0045] 图2是本发明一个实施例中同步任务执行的流程示意图;

[0046] 图3示出可用于本发明各实施例的一种示例性系统的功能模块。

[0047] 附图中相同或相似的附图标记代表相同或相似的部件。

具体实施方式

[0048] 下面结合附图对本发明作进一步详细描述。

[0049] 在本发明的一个典型的配置中,终端、服务网络的设备和可信方均包括一个或多个处理器(例如,中央处理器(Central Processing Unit,CPU))、输入/输出接口、网络接口和内存。

[0050] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(Random Access Memory,RAM)和/或非易失性内存等形式,如只读存储器(Read Only Memory,ROM)或闪存(Flash Memory)。内存是计算机可读介质的示例。

[0051] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(Phase-Change Memory,PCM)、可编程随机存取存储器(Programmable Random Access Memory,PRAM)、静态随机存取存储器(Static Random-Access Memory,SRAM)、动态随机存取存储器(Dynamic Random Access Memory,DRAM)、其他类型的随机存取存储器(Random Access Memory,RAM)、只读存储器(Read-Only Memory,ROM)、电可擦除可编程只读存储器(Electrically-Erasable Programmable Read-Only Memory,EEPROM)、快闪记忆体(Flash Memory)或其他内存技术、只读光盘只读存储器(Compact Disc Read-Only Memory,CD-ROM)、数字多功能光盘(Digital Versatile Disc,DVD)或其他光学存储、磁盒式磁带,磁带磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。

[0052] 本发明所指设备包括但不限于用户设备、网络设备、或用户设备与网络设备通过网络相集成所构成的设备。所述用户设备包括但不限于任何一种可与用户进行人机交互(例如通过触摸板进行人机交互)的移动电子产品,例如智能手机、平板电脑等,所述移动电子产品可以采用任意操作系统,如Android操作系统、iOS操作系统等。其中,所述网络设备包括一种能够按照事先设定或存储的指令,自动进行数值计算和信息处理的电子设备,其硬件包括但不限于微处理器、专用集成电路(Application Specific Integrated Circuit,ASIC)、可编程逻辑器件(Programmable Logic Device,PLD)、现场可编程门阵列(Field Programmable Gate Array,FPGA)、数字信号处理器(Digital Signal Processor,DSP)、嵌入式设备等。所述网络设备包括但不限于计算机、网络主机、单个网络服务器、多个网络服务器集或多个服务器构成的云;在此,云由基于云计算(Cloud Computing)的大量计算机或网络服务器构成,其中,云计算是分布式计算的一种,由一群松散耦合的计算机集组成的一个虚拟超级计算机。所述网络包括但不限于互联网、广域网、城域网、局域网、VPN网

络、无线自组织网络(Ad Hoc Network)等。优选地,所述设备还可以是运行于所述用户设备、网络设备、或用户设备与网络设备、网络设备、触摸终端或网络设备与触摸终端通过网络相集成所构成的设备上的程序。

[0053] 当然,本领域技术人员应能理解上述设备仅为举例,其他现有的或今后可能出现的设备如可适用于本发明,也应包含在本发明保护范围以内,并在此以引用方式包含于此。

[0054] 在本发明的实施方式的描述中,“多个”的含义是两个或者更多,除非另有明确具体的限定。

[0055] 本实施例首先提供了一种多云安全基线管理的系统架构,该系统采用B/S模式和微服务架构,服务端选用微服务架构设计,整体结构设计分为用户层、网关层、业务层、数据层和云层五层结构,其中:

[0056] -用户层:用户通过PC电脑或Laptop访问本系统。

[0057] -网关层:用户使用专属账户登入系统,网关层进行身份识别与访问管理,并对前端和后端服务进行分布式部署,前端页面进行单独部署到Web服务器。

[0058] -业务层:应用服务可构建集群提供服务,包括数据分析、数据统计、查询服务、数据库访问服务、配置服务、定时任务服务等,用户通过网关层的Webservices或者Restful与业务层进行数据请求交互。

[0059] -数据层:数据库服务器的运行方式分为两种:双机热备、主从同步。增加单独的缓存服务器,对页面和常用数据进行缓存,用以减轻数据库的压力,解决数据库读写瓶颈,保证数据库的正常运行。

[0060] -云层:根据不同云账号信息,自定义定时任务,请求API或者SDK定时从云(阿里云、Azure、AWS、腾讯云)中同步资源数据,从云中同步元数据,通过数据清洗服务,根据定义的规则完成安全数据的分析告警或存储分析。

[0061] 基于上述架构,具体而言,本实施例提供了一种多云资源报警管控的方法。该方法应用于一用户终端,并由相应的网络设备(例如云端服务器)提供支撑。参考图1,该方法包括步骤S100、步骤S200、步骤S300、步骤S400、步骤S500、步骤S600和步骤S700。以下以一用户终端为例描述本实施例的具体实施方式。

[0062] 具体地,在步骤S100中,用户终端获取用户的身份验证信息。例如,用户在用户终端输入自己的用户标识(例如系统账号名称)及认证信息(例如账号密码)。

[0063] 在步骤S200中,用户终端基于所述身份验证信息匹配对应的多个公有云账号识别信息,其中每个公有云账号识别信息分别对应一公有云账号。例如,管理员所登录的用户账号对应于其所管理的若干个公有云账号;在一些情形下,对于同一套系统而言,不同的管理员可能管理不同的公有云账号。

[0064] 在步骤S300中,用户终端分别向多台云端设备发送多个元数据请求,其中每个元数据请求包括一公有云账号识别信息,所述公有云账号识别信息用于确定用户对相应公有云账号的访问权限。例如,多台云端设备分别对应于多个不同的云平台。用户对某个云账号的访问权限,在一些实施例中由用户提供的相关账号信息确定,例如阿里云需要获取录入accessKeyId、accessSecret字段,而Azure(微软所提供的云服务平台)需要获取录入subscriptionId、clientSecret字段。录入成功以后验证录入账号是否可用。

[0065] 在步骤S400中,接收所述多台云端设备基于所述元数据请求而发送的多条元数

据,所述多条元数据包含相应公有云的资源安全信息和监控信息。

[0066] 在步骤S500中,用户终端根据各云平台不同的数据清洗规则,将元数据的内容清洗至相应的数据结构中,包括检查数据一致性,处理无效值和缺失值等;再将已清洗的数据做持久化操作,以便于后续安全基线管理的利用。

[0067] 在步骤S600中,用户终端根据获取的所述安全信息和所述监控信息,对各公有云账户云资源进行安全评分;统计各个规章内安全信息的条目数以及违反数,对于违反规则项目的匹配对应的违反原因以及潜在修改方案及其预期效果。

[0068] 在步骤S700中,用户终端响应于用户在所述用户终端的单一界面输入的操作指令,基于获得的安全评分和/或关于安全信息的统计结果执行对应的操作。

[0069] 从而,用户仅在一个单一的用户界面中,即可实现对多个云账号的云资源报警进行管控,无需分别进入各个云账号进行监控管理。

[0070] 其中在一些实施例中,在上述步骤S300中,用户终端基于预设的时间间隔分别向多台网络设备发送多个元数据请求。例如,在获取用户的身份验证信息后,系统自行地每隔一定时间执行前述操作,以减轻用户的操作负担和提高本地数据的实时性。

[0071] 在一些实施例中,上述步骤S300包括子步骤S310、子步骤S320、子步骤S330和子步骤S340(图中未示出)。在子步骤S310中,用户终端创建任务队列,所述任务队列包括对应于所述多个公有云账号识别信息的多个元数据请求任务;在子步骤S320中,用户终端获取所述任务队列中的当前任务,并确定所述当前任务的可执行状态;在子步骤S330中,用户终端若所述当前任务的可执行状态为不可执行,将所述当前任务移至所述任务队列的队尾;在子步骤S340中,若所述当前任务的可执行状态为可以执行,用户终端执行所述当前任务以向相应的网络设备发送相应的元数据请求,并在所述当前任务执行完毕后移除所述当前任务。其中,为自动执行某些任务而减轻管理员负担,一些任务设置有循环状态,该循环状态用于表征该任务是否在本次执行后仍需再次自动执行。相应地在一些实施例中,在子步骤S340中,若所述当前任务的可执行状态为可以执行,用户终端执行所述当前任务以向相应的网络设备发送相应的元数据请求;若所述当前任务的循环状态为真,在所述当前任务执行完毕后将所述当前任务移至所述任务队列的队尾;否则在所述当前任务执行完毕后移除所述当前任务。

[0072] 例如,系统对各个云账号资源(基础资源、安全信息等)信息同步的管理,同步任务创建成功后,其执行状态的变化如图2所示。系统首先读取账户访问信息,判断账户信息是否可用,如不可用,则任务状态为不可执行,任务状态码设置为-1,等待下一次访问;如可用,则开始执行同步任务,任务状态码设置为0。在任务执行过程中,任务状态码设置为2。判断任务执行是否成功,执行成功,任务状态码设置为3,任务结束;执行失败,任务状态码设置为1,等待下一次访问。

[0073] 在一些实施例中,在步骤S400中,用户终端接收的多条元数据包含相应公有云的资源安全信息和监控信息,以Azure为例,可包括Azure规章遵从标准数据、Azure规章遵从性控件数据、Azure合规性评估数据、Azure评估元数据、Azure个评估数据、Azure安全分数数据、Azure安全计分控制数据等,表1至表7示出了请求上述数据的返回参数。

[0074] 表1 Azure规章遵从标准数据的返回参数

[0075]

Name	Type	descripition
Other Status Codes	CloudError	描述操作失败原因的错误响应。
nextLink	string	要获取下一页的 URI。
value	RegulatoryComplianceStandard[]	法规合规性标准详细信息和状态
id	string	资源 ID
name	string	资源名称
properties.failedControls	integer	具有失败状态的给定标准受支持的法规遵从性控制的数量
properties.passedControls	integer	给定标准受支持的法规遵从性控制的数量，并带有传递状态
properties.skippedControls	integer	具有跳过状态的给定标准受支持的法规遵从性控制的数量
properties.state	state	基于标准支持的控件状态的聚合状态
properties.unsupportedControls	integer	未得到自动评估支持的给定标准的法规合规性控制数量
type	string	资源类型

[0076] 表2 Azure规章遵从性控件数据的返回参数

[0077]

Name	Type	descripition
Other Status Codes	CloudError	描述操作失败原因的错误响应。
nextLink	string	要获取下一页的 URI。
value	RegulatoryComplianceAssessment[]	法规遵从性评估详细信息和状态
id	string	资源 ID
name	string	资源名称
properties.description	string	法规遵从性控制的描述
properties.failedAssessments	integer	具有失败状态的给定控件的支持法规合规性评估的数量
properties.passedAssessments	integer	具有已通过状态的给定控件的支持法规合规性评估的数量
properties.skippedAssessments	integer	具有跳过状态的给定控件的支持法规合规性评估的数量
properties.state	state	基于控件支持的评估状态的聚合状态
type	string	资源类型

[0078] 表3 Azure合规性评估数据的返回参数

[0079]

Name	Type	descripition

[0080]

Other Status Codes	CloudError	描述操作失败原因的错误响应。
nextLink	string	要获取下一页的 URI
value	RegulatoryComplianceAssessment[]	法规遵从性评估详细信息和状态
id	string	资源 ID
name	string	资源名称
properties.assessmentDetailsLink	string	链接到更详细的评估结果数据。 响应类型将根据评估类型字段
properties.assessmentType	string	评估详细信息链接中包含的预期评估类型
properties.description	string	法规遵从性评估的描述
properties.failedResources	integer	给定评估的相关资源计数失败状态。
properties.passedResources	integer	给定评估的相关资源计数与传递状态。
properties.skippedResources	integer	给定评估的相关资源计数与跳过状态。
properties.state	state	基于评估扫描资源状态的聚合状态
properties.unsupportedResources	integer	给定评估的相关资源计数与不受支持的状态。
Type	string	资源类型

[0081] 表4 Azure评估元数据的返回参数

[0082]

Name	Type	descripition
Other Status Codes	CloudError	描述操作失败原因的错误响应。
nextLink	string	要获取下一页的 URI
id	string	资源 ID
name	string	资源名称
properties.assessmentType	assessmentType	生成 在基于内置 Azure 策略定义的评估中，自定义基于自定义 Azure 策略定义的评估
properties.category	string[]	评估不正常时处于风险中的资源类别
properties.description	string	评估的人类可读描述
properties.displayName	string	评估的用户友好显示名称
properties.implementationEffort	implementationEffort	修复此评估所需的实施工作
properties.partnerData	SecurityAssessmentMetadataPartnerData	描述创建评估的合作伙伴
properties.policyDefinitionId	string	将此评估计算打开的策略定义的 Azure 资源 ID
properties.preview	boolean	如果此评估处于预览发布状态，则为 True
properties.remediationDescription	string	人工可读描述您应该采取哪些操作来缓解此安全问题
properties.severity	severity	评估的严重性级别

[0083]

properties.threats	string[]	评估对威胁的影响
properties.userImpact	userImpact	评估的用户影响
type	string	资源类型

[0084] 表5 Azure个评估数据的返回参数

[0085]

Name	Type	descripition
Other Status Codes	CloudError	描述操作失败原因的错误响应。
nextLink	string	要获取下一页的 URI
id	string	资源 Id
name	string	资源名称
properties.additionalData	object	有关评估的其他数据
properties.displayName	string	用户友好的评估显示名称
properties.links	AssessmentLinks	与评估相关的链接
properties.metadata	SecurityAssessmentMetadataProperties	描述评估元数据的属性。
properties.partnersData	SecurityAssessmentPartnerData	与第三方合作伙伴集成相关的数据
properties.resourceDetails	ResourceDetails:	已评估的资源的详细信息
	AzureResourceDetails	
	OnPremiseResourceDetails	
	OnPremiseSqlResourceDetails	
properties.status	AssessmentStatus	评估结果
type	string	资源类型

[0086] 表6 Azure安全分数数据的返回参数

[0087]

Name	Type	descripition
Other Status Codes	CloudError	描述操作失败原因的错误响应。
nextLink	string	要获取下一页的 URI
id	string	资源 Id
name	string	资源名称
properties.displayName	string	计划的名称
properties.score.current	number	当前分数
properties.score.max	integer	最大可用分数
properties.score.percentage	number	当前分数的比率除以最大值。 舍入到小数点后 4 位
properties.weight	integer	每个订阅的相对权重。 计算多个订阅的聚合安全分数时使用。
type	string	资源类型

[0088] 表7 Azure安全计分控制数据的返回参数

[0089]

Name	Type	descripition
Other Status Codes	CloudError	描述操作失败原因的错误响应。
nextLink	string	要获取下一页的 URI
id	string	资源 Id
name	string	资源名称
properties.definition	SecureScoreControlDefinitionItem	有关安全控件的信息。
properties.displayName	string	控件的用户友好显示名称
properties.healthyResourceCount	integer	控件中正常运行的资源数
properties.notApplicableResourceCount	integer	控件中不适用的资源数
properties.score.current	number	当前分数
properties.score.max	integer	最大可用分数
properties.score.percentage	number	当前分数的比率除以最大值。 舍入到小数点后 4 位
properties.unhealthyResourceCount	integer	控件中不正常的资源数
properties.weight	integer	此特定控件在每个订阅中的相对权重。在所有订阅中计算此控件的聚合分数时使用。
type	string	资源类型

[0090] 在一些实施例中，在步骤S600中，针对任一公有云账户云资源进行安全评分的计算公式如下：

[0091] $$Sum=\sum_{m=1}^{m=max}\varepsilon_m\frac{\sum_{n=1}^{n=max}\phi_n(A,k)}{S_m}-\sum_{m=1}^{m=max}\varepsilon_m\frac{\sum_{n=1}^{n=max}\left(\sum_{i=1}^{i=max}|0-A_i|*j_i*\omega(t,u)\right)_n}{S_m} \quad (1)$$

[0092] $$\phi(A,k)=\sum_{i=1}^{i=max}(A_i-0)*k_i \quad (2)$$

[0093] $$\omega(t,u)=ut^2 \quad (3)$$

[0094] 公式(1)中，等号左边的Sum表示公有云账户云资源的安全评分；等号右边分为两部分，减号左边是公有云账户云资源的总得分，减号右边是公有云账户云资源的总失分。

[0095] 首先对于上述公式中的参数进行统一说明，详见以下表8。

[0096] 表8

[0097]

参数	说明
A	单类单例单项监控指标
i	单类单例的监控指标编号
A_i	单类单例单项监控指标分值
(A_i-0)	表示单项监控指标的得分值
$\|0-A_i\|$	表示单项监控指标的失分值
k	单类单例单项监控指标的得分系数

S	单类资源中实例的总数
m	资源类的编号
n	单类资源中实例的编号
ε	单类资源的安全分数系数
j	单类单例单项监控指标的失分系数
u	时间风险系数
t	检测失效距今的天数

[0098] 以下对于模型中的各个单元以及含义做进一步的说明。

[0099] 单例总得分：

[0100] 公式(2)中，$(A_i-0)*k_i$为单个实例中第i项监控指标的得分，其是单项监控指标的得分值(A_i-0)与单项监控指标的得分系数k_i的乘积，从而Φ(A,k)代表了单个实例中所有不同的监控指标的得分的总和，即该单例的总得分。

[0101] 单类资源总得分和平均得分：

[0102] 公式(1)中的

[0103] $$\frac{\sum_{n=1}^{n=max}\phi_n(A,k)}{S_m}$$

[0104] 该式分子部分表示单类资源中所有单例的得分之和，即单类资源的总得分；分母为该单类资源中实例的总数，从而该式表示单类资源的平均得分。

[0105] 公有云账户云资源总得分：

[0106] 公式(1)中的

[0107] $$\sum_{m=1}^{m=max}\varepsilon_m\frac{\sum_{n=1}^{n=max}\phi_n(A,k)}{S_m}$$

[0108] 该式是将所有单类资源的平均得分分别乘以其相应的安全分数系数ε后再求和，从而获得公有云账户云资源的总得分。安全分数系数ε实际就是单类资源的分数权重，公有云账户云资源的总得分即是将所有单类资源的平均得分加权后的总和。

[0109] 风险影响系数：

[0110] 公式(3)中ω表示风险影响系数，其是时间风险系数u与时间t平方的乘积，此处t采用检测失效距今的天数。可见，时间风险系数越高，检测失效距今时间越久，则风险影响系数会越高。

[0111] 单例总失分：

[0112] 公式(1)中，$|0-A_i|*j_i*\omega(t,u)$为单个实例中第i项监控指标的失分，其是单项监控指标的失分值$|0-A_i|$与单项监控指标的失分系数j_i以及风险影响系数ω的乘积，从而

[0113] $$\sum_{i=1}^{i=max}|0-A_i|*j_i*\omega(t,u)$$

[0114] 该式代表了单个实例中所有不同的监控指标的失分的总和，即该单例的总失分。

[0115] 单类资源总失分和平均失分：

[0116] 公式(1)中的

[0117] $$\frac{\sum_{n=1}^{n=max}\left(\sum_{i=1}^{i=max}|0-A_i|*j_i*\omega(t,\mu)\right)_n}{S_m}$$

[0118] 该式分子部分表示单类资源中所有单例的失分之和,即单类资源的总失分;分母为该单类资源中实例的总数,从而该式表示单类资源的平均失分。

[0119] 公有云账户云资源总失分:

[0120] 公式(1)中的

[0121] $$\sum_{m=1}^{m=max}\varepsilon_m\frac{\sum_{n=1}^{n=max}\left(\sum_{i=1}^{i=max}|0-A_i|*j_i*\omega(t,\mu)\right)_n}{S_m}$$

[0122] 该式是将所有单类资源的平均失分分别乘以其相应的安全分数系数ε后再求和,从而获得公有云账户云资源的总失。如前所述,安全分数系数ε实际就是单类资源的分数权重,公有云账户云资源的总失分即是将所有单类资源的平均失分加权后的总和。

[0123] 公有云账户云资源的安全评分:

[0124] 将上述计算获得的公有云账户云资源总得分减去其总失分,从而获得公有云账户云资源的安全评分,即公式(1)。

[0125] 以下以一个阿里云的安全基线项目对公有云账户云资源的安全评分计算做进一步说明,表9示出了安全基线项目的配置规则。

[0126] 表9

[0127]

名称	详情	监控项 A	得分系数 k	失分系数 j	时间风险系数 u
云防火墙规则扫描	阿里云防火墙，防火墙（安全组）规则从 0.0.0.0/0 进入的端口为不合规	10	0.8	0.8	0.06
安全组规则扫描	安全组进出包含拒绝入站 IP 地址段：0.0.0.0/0 端口：-1-1 和出站 0.0.0.0/0 端口：-1-1 流量规则为不合规	10	0.8	0.8	0.04
VPC 路由规则扫描	VPC 包含 0.0.0.0/0 的访问公网的默认路由为不合规	20	1.2	0.8	0.04
RDS 白名单扫描	RDS 数据库的防火墙白名单中包含0.0.0.0/0的网段访问为不合规	10	0.4	0.4	0.02
OSS 合规扫描	扫描有公开读写的 OSS 为不合规	5	0.1	0.1	0.01

[0128] 根据同步的公有云资源安全和监控信息，汇总得到如表10的分值和时间数据，其中X、V、R、O表示不同的资源类，X1、X2为资源类X中的两个实例，V1、V2为资源类V中的两个实例，R1为资源类R中的一个实例，O1、O2为资源类O中的两个实例。各资源类的安全分数系数ε均设置为1。

[0129] 表10

[0130]

检控规则	项目	得分值	失分值	检测失效至今天数
云防火墙规则扫描	X1	6	4	10
	X2	10	0	0
安全组规则扫描	X1	2	8	2
	X2	10	0	0
VPC 路由规则扫描	V1	20	0	0
	V2	12	8	3
RDS 白名单扫描	R1	8	2	2
OSS 合规扫描	O1	0	5	2
	O2	5	0	0

[0131] 计算该公有云账户云资源的总得分，算式如下：

[0132]
$$1\times\frac{6\times0.8+2\times0.8+10\times0.8+10\times0.8}{2}+1\times\frac{20\times1.2+12\times1.2}{2}+1\times\frac{8\times0.4}{1}+1\times\frac{5\times0.1}{2}=33.85$$

[0133] 即该公有云账户云资源的总得分为33.85。

[0134] 计算该公有云账户云资源的总失分，算式如下：

[0135]
$$1\times\frac{4\times0.8\times0.06\times10^2+8\times0.8\times0.04\times2^2}{2}+1\times\frac{8\times0.8\times0.04\times3^2}{2}+1\times\frac{2\times0.4\times0.02\times2^2}{1}+1\times\frac{5\times0.1\times0.01\times2^2}{2}=11.338$$

[0136] 即该公有云账户云资源的总失分为11.338。

[0137] 从而该公有云账户云资源的安全评分为33.85-11.338＝22.512。

[0138] 在一些实施例中，在步骤S700中，用户终端检测用户在所述用户终端的浏览器应用中的单一界面输入的操作指令；响应于所述操作指令，用户终端基于获得的安全评分和/或关于安全信息的统计结果执行对应的操作。在此，上述相应的操作包括但不限于安全评分及统计信息的筛选、展示、图形化、汇总、输出等。具体地，显示内容可以是一个云账户的安全评分、各个规章内统计安全信息的条目数以及违反数、基于违反规则项目所罗列出的详细原因和对应的潜在修改方案及其效果、多云安全基线扫描后的数据图表、配合云账号设置的安全基线内容以及结合其数据和标准数据对比(得出相应的分数或曲线)等等。

[0139] 本实施例还提供了一种计算机程序产品，当所述计算机程序产品被计算机设备执行时，如前任一项所述的方法被执行。

[0140] 本实施例还提供了一种计算机设备，所述计算机设备包括：

[0141] 一个或多个处理器；

[0142] 存储器，用于存储一个或多个计算机程序；

[0143] 当所述一个或多个计算机程序被所述一个或多个处理器执行时，使得所述一个或

多个处理器实现如前任一项所述的方法。

[0144] 图3示出了可被用于实施本发明中所述的各个实施例的示例性系统。

[0145] 如图3所示，在一些实施例中，系统1000能够作为各所述实施例中的任意一个用户终端设备。在一些实施例中，系统1000可包括具有指令的一个或多个计算机可读介质(例如，系统存储器或NVM/存储设备1020)以及与该一个或多个计算机可读介质耦合并被配置为执行指令以实现模块从而执行本发明中所述的动作的一个或多个处理器(例如，(一个或多个)处理器1005)。

[0146] 对于一个实施例，系统控制模块1010可包括任意适当的接口控制器，以向(一个或多个)处理器1005中的至少一个和/或与系统控制模块1010通信的任意适当的设备或组件提供任意适当的接口。

[0147] 系统控制模块1010可包括存储器控制器模块1030，以向系统存储器1015提供接口。存储器控制器模块1030可以是硬件模块、软件模块和/或固件模块。

[0148] 系统存储器1015可被用于例如为系统1000加载和存储数据和/或指令。对于一个实施例，系统存储器1015可包括任意适当的易失性存储器，例如，适当的DRAM。在一些实施例中，系统存储器1015可包括双倍数据速率类型四同步动态随机存取存储器(DDR4 SDRAM)。

[0149] 对于一个实施例，系统控制模块1010可包括一个或多个输入/输出(I/O)控制器，以向NVM/存储设备1020及(一个或多个)通信接口1025提供接口。

[0150] 例如，NVM/存储设备1020可被用于存储数据和/或指令。NVM/存储设备1020可包括任意适当的非易失性存储器(例如，闪存)和/或可包括任意适当的(一个或多个)非易失性存储设备(例如，一个或多个硬盘驱动器(Hard Disk,HDD)、一个或多个光盘(CD)驱动器和/或一个或多个数字通用光盘(DVD)驱动器)。

[0151] NVM/存储设备1020可包括在物理上作为系统1000被安装在其上的设备的一部分的存储资源，或者其可被该设备访问而不必作为该设备的一部分。例如，NVM/存储设备1020可通过网络经由(一个或多个)通信接口1025进行访问。

[0152] (一个或多个)通信接口1025可为系统1000提供接口以通过一个或多个网络和/或与任意其他适当的设备通信。系统1000可根据一个或多个无线网络标准和/或协议中的任意标准和/或协议来与无线网络的一个或多个组件进行无线通信。

[0153] 对于一个实施例，(一个或多个)处理器1005中的至少一个可与系统控制模块1010的一个或多个控制器(例如，存储器控制器模块1030)的逻辑封装在一起。对于一个实施例，(一个或多个)处理器1005中的至少一个可与系统控制模块1010的一个或多个控制器的逻辑封装在一起以形成系统级封装(SiP)。对于一个实施例，(一个或多个)处理器1005中的至少一个可与系统控制模块1010的一个或多个控制器的逻辑集成在同一模具上。对于一个实施例，(一个或多个)处理器1005中的至少一个可与系统控制模块1010的一个或多个控制器的逻辑集成在同一模具上以形成片上系统(SoC)。

[0154] 在各个实施例中，系统1000可以但不限于是：服务器、工作站、台式计算设备或移动计算设备(例如，膝上型计算设备、手持计算设备、平板电脑、上网本等)。在各个实施例中，系统1000可具有更多或更少的组件和/或不同的架构。例如，在一些实施例中，系统1000包括一个或多个摄像机、键盘、液晶显示器(LCD)屏幕(包括触屏显示器)、非易失性存储器

端口、多个天线、图形芯片、专用集成电路(ASIC)和扬声器。

[0155] 需要注意的是,本发明可在软件和/或软件与硬件的组合体中被实施,例如,可采用专用集成电路(ASIC)、通用目的计算机或任何其他类似硬件设备来实现。在一个实施例中,本发明的软件程序可以通过处理器执行以实现上文所述步骤或功能。同样地,本发明的软件程序(包括相关的数据结构)可以被存储到计算机可读记录介质中,例如,RAM存储器,磁或光驱动器或软磁盘及类似设备。另外,本发明的一些步骤或功能可采用硬件来实现,例如,作为与处理器配合从而执行各个步骤或功能的电路。

[0156] 另外,本发明的一部分可被应用为计算机程序产品,例如计算机程序指令,当其被计算机执行时,通过该计算机的操作,可以调用或提供根据本发明的方法和/或技术方案。本领域技术人员应能理解,计算机程序指令在计算机可读介质中的存在形式包括但不限于源文件、可执行文件、安装包文件等,相应地,计算机程序指令被计算机执行的方式包括但不限于:该计算机直接执行该指令,或者该计算机编译该指令后再执行对应的编译后程序,或者该计算机读取并执行该指令,或者该计算机读取并安装该指令后再执行对应的安装后程序。在此,计算机可读介质可以是可供计算机访问的任意可用的计算机可读存储介质或通信介质。

[0157] 通信介质包括藉此包含例如计算机可读指令、数据结构、程序模块或其他数据的通信信号被从一个系统传送到另一系统的介质。通信介质可包括有导的传输介质(诸如电缆和线(例如,光纤、同轴等))和能传播能量波的无线(未有导的传输)介质,诸如声音、电磁、RF、微波和红外。计算机可读指令、数据结构、程序模块或其他数据可被体现为例如无线介质(诸如载波或诸如被体现为扩展频谱技术的一部分的类似机制)中的已调制数据信号。术语“已调制数据信号”指的是其一个或多个特征以在信号中编码信息的方式被更改或设定的信号。调制可以是模拟的、数字的或混合调制技术。

[0158] 作为示例而非限制,计算机可读存储介质可包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据的信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动的介质。例如,计算机可读存储介质包括,但不限于,易失性存储器,诸如随机存储器(RAM,DRAM,SRAM);以及非易失性存储器,诸如闪存、各种只读存储器(ROM,PROM,EPROM,EEPROM)、磁性和铁磁/铁电存储器(MRAM,FeRAM);以及磁性和光学存储设备(硬盘、磁带、CD、DVD);或其它现在已知的介质或今后开发的能够存储供计算机系统使用的计算机可读信息/数据。

[0159] 在此,根据本发明的一个实施例包括一个装置,该装置包括用于存储计算机程序指令的存储器和用于执行程序指令的处理器,其中,当该计算机程序指令被该处理器执行时,触发该装置运行基于前述根据本发明的多个实施例的方法和/或技术方案。

[0160] 对于本领域技术人员而言,显然本发明不限于上述示范性实施例的细节,而且在不背离本发明的精神或基本特征的情况下,能够以其他的具体形式实现本发明。因此,无论从哪一点来看,均应将实施例看作是示范性的,而且是非限制性的,本发明的范围由所附权利要求而不是上述说明限定,因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本发明内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。此外,显然“包括”一词不排除其他单元或步骤,单数不排除复数。装置权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第一,第二等词语用来表

示名称,而并不表示任何特定的顺序。

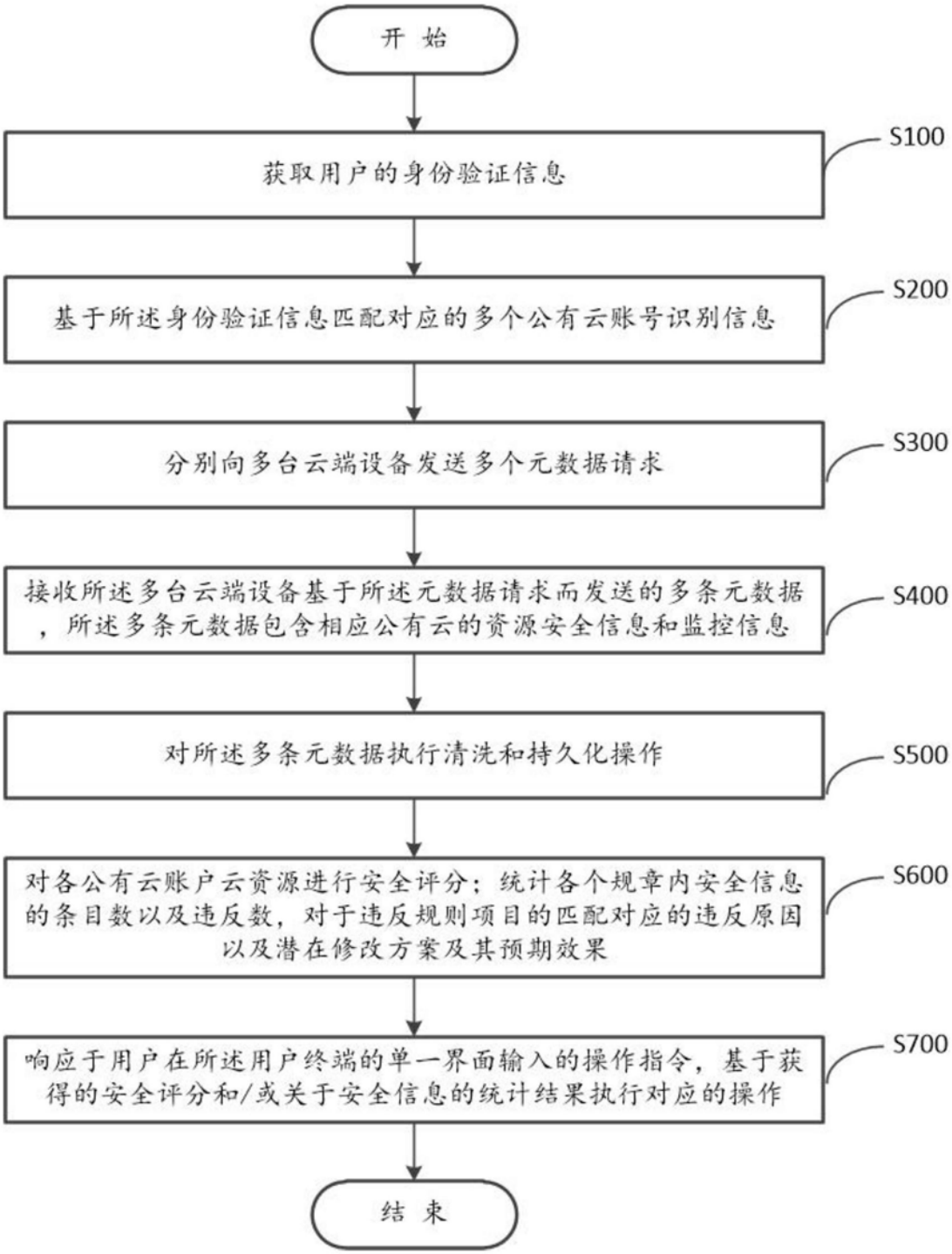

开 始
获取用户的身份验证信息
S100
基于所述身份验证信息匹配对应的多个公有云账号识别信息
S200
分别向多台云端设备发送多个元数据请求
S300
接收所述多台云端设备基于所述元数据请求而发送的多条元数据，所述多条元数据包含相应公有云的资源安全信息和监控信息
S400
对所述多条元数据执行清洗和持久化操作
S500
对各公有云账户云资源进行安全评分；统计各个规章内安全信息的条目数以及违反数，对于违反规则项目的匹配对应的违反原因以及潜在修改方案及其预期效果
S600
响应于用户在所述用户终端的单一界面输入的操作指令，基于获得的安全评分和/或关于安全信息的统计结果执行对应的操作
S700
结 束

图1

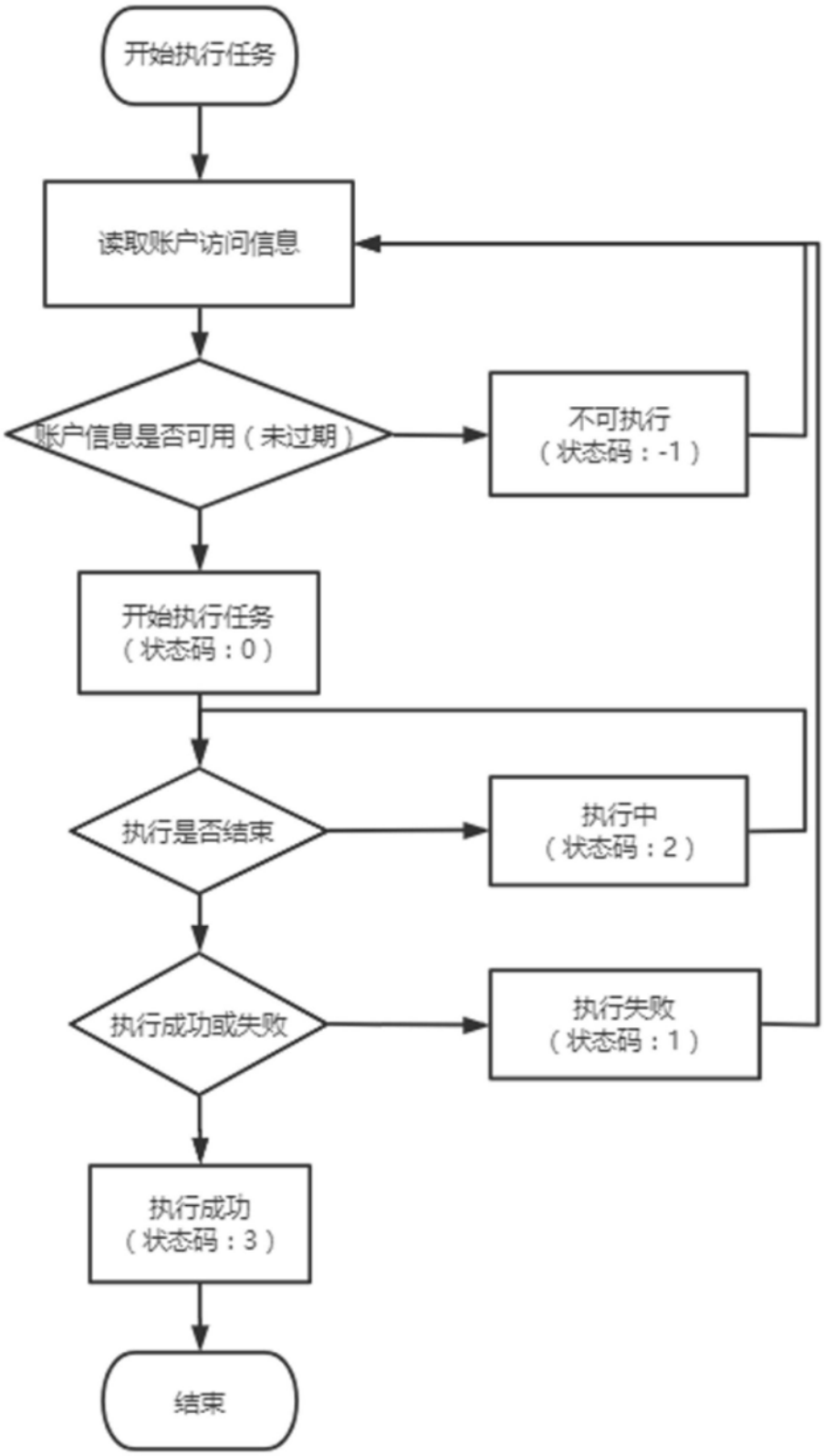

开始执行任务
读取账户访问信息
账户信息是否可用（未过期）
不可执行
（状态码：-1）
开始执行任务
（状态码：0）
执行是否结束
执行中
（状态码：2）
执行成功或失败
执行失败
（状态码：1）
执行成功
（状态码：3）
结束

图2

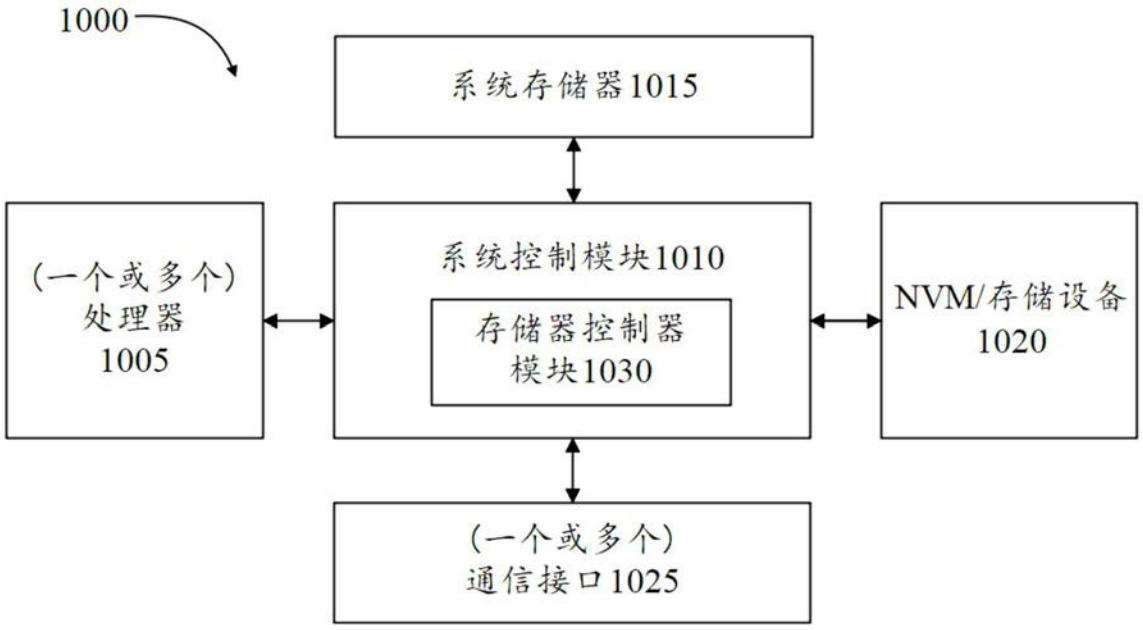

1000
系统存储器1015
(一个或多个)
处理器
1005
系统控制模块1010
存储器控制器
模块1030
NVM/存储设备
1020
(一个或多个)
通信接口1025

图3