(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115221553 A
(43)申请公布日 2022.10.21

(21)申请号 202210801641.1

(22)申请日 2022.07.07

(71)申请人 嘉兴职业技术学院
地址 314500 浙江省嘉兴市桐乡大道547号

(72)发明人 谢升余 潘赟 隋龙飞

(74)专利代理机构 嘉兴启帆专利代理事务所(普通合伙) 33253
专利代理师 林鸳

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)
G06Q 40/04(2012.01)
G06F 16/27(2019.01)
G06F 16/2458(2019.01)
G06K 9/62(2022.01)

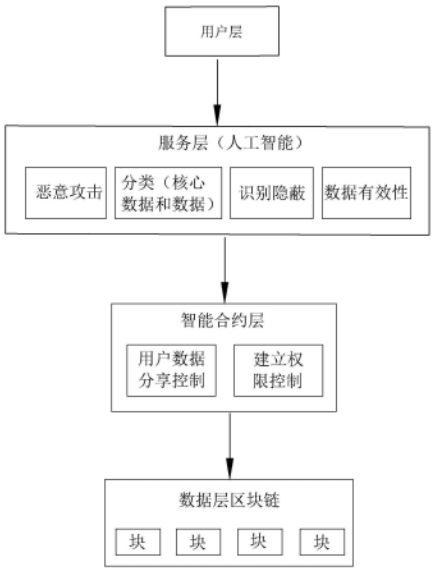
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种基于人工智能与区块链智能合约分区的数据防护系统

(57)摘要

本发明公开了一种基于人工智能与区块链智能合约分区的数据防护系统，包括用户层、服务层、智能合约层和数据层区块链；用户层用于上传数据，服务层用于对数据进行分类、隐私保护、有效性处理，智能合约层依据数据标识确定数据在区块链上的存储访问策略，数据层区块链用于并行处理数据。本发明通过整合区块链、智能合约以及人工智能技术，对数据进行分类识别、有效性验证和重要数据隐蔽保护处理，再通过智能合约控制用户数据分享和权限，对数据进行分布式存储，从而极大地提高了云端数据的安全性，有效性和处理效率。



CN 115221553 A

1.一种基于人工智能与区块链智能合约分区的数据防护系统，其特征在于：包括用户层、服务层、智能合约层和数据层区块链；

用户层用于上传数据，数据包括头部和数据的内容；

服务层用于对数据进行分类、隐私保护、有效性处理；对数据进行标识，得到数据的类型信息x_j、数据的重要性m_k和数据选择分区所有其它影响因素p(Y)；

智能合约层依据数据标识确定数据在区块链上的存储访问策略；根据所述数据标识计算数据的权重W和用户属性U，数据的权重采用如下计算公式如下：

$$W = a \times \int_0^N f(x_j)dx_j + b \times \int_0^M f(m_k)dm_k + p(Y)$$

其中：a、b为常系数；

N为数据分类后的x_j个数，$\{x_j \mid j=1,2,\ldots,N\}$；

$M = \frac{m_k}{\sum m_k}$，$\{m_k \mid k = 1,2,\ldots,N\}$，M即所选数据类型的重要性在所有重要性的占比；

$p(Y) = \sum_{i=0}^{n=i} y_i^n L_i$，其中L是常系数，$y_0=1$；

比较所选数据权重W与用户属性U之间的大小关系，根据用户属性U对应的权限，来判断数据所属的分区；不同的数据分区制定不同的规则，不同属性的用户设置不同的访问权限；

数据层区块链用于并行处理数据；部署T个云服务器，$S=\{s_i \mid i=1,2,\ldots,T\}$，其中$s_i$为第i个云服务器，T≥N*2，且T为N的倍数，N为数据分类后的x个数；区块链全网节点的总个数为T，分成N组，则每组节点个数$t = \frac{T}{N}(t \geq 2)$；将不同类型的数据分发到各个组所在区的节点，每一组至少有2个节点保存着相同的数据，实现并行处理。

2.如权利要求1所述的一种基于人工智能与区块链智能合约分区的数据防护系统，其特征在于：所述服务层对数据的初步处理为安全识别处理，根据预设的黑名单、白名单、敏感字样来识别数据，判断数据是否存在恶意攻击。

3.如权利要求1所述的一种基于人工智能与区块链智能合约分区的数据防护系统，其特征在于：所述服务层将数据分为四类，四类数据按照重要性程度由低到高依次为：非核心数据、核心非有效数据、核心非保护数据、核心隐蔽保护数据；类型信息分别为x1、x2、x3、x4，数据的重要性分别为m1、m2、m3、m4；且用户属性按照权限由低到高分别为U_1、U_2、U_3；

数据权重W与用户属性U之间的大小关系如下：

当$W \leq U_1$时，数据选择存放于非核心区；

当$U_1 < W \leq U_2$时，数据选择存放于核心非有效区；

当$U_2 < W \leq U_3$时，数据选择存放于核心非保护区；

当$U_3 < W$时，数据选择存放于核心保护隐藏区。

4.如权利要求3所述的一种基于人工智能与区块链智能合约分区的数据防护系统，其特征在于：所述服务层进行数据分类的具体步骤如下：

1)对数据进行是否恶意攻击识别，在通过安全识别处理后继续下一步；

2)对数据进行分类识别，根据数据重要性等级进行分析，判断数据为核心数据或非核心数据；

3)对于核心数据，对其进行是否有效性识别操作；且对有效数据继续进行下一步的识别掩蔽动作；

4)对于核心有效数据,对其进行是否受信息保护识别;对受保护数据,进行掩蔽操作。

5.如权利要求3所述的一种基于人工智能与区块链智能合约分区的数据防护系统,其特征在于:所述智能合约层内写入不同组的用户信息、访问权限和相对应的规则,并加载到每个节点上;相对应的加密文件通过智能合约层的调整使用进行创建,并将信息录入到区块链里;用户先通过智能合约层查询访问权限,在满足预先设定的规则时,实现访问不同分区的加密文件:

①对非核心数据区,采用开放式的权限规则;

②对核心数据区,依照用户所在组的级别属性U,分别授予指定的权限来访问不同核心数据区域。

一种基于人工智能与区块链智能合约分区的数据防护系统

技术领域

[0001] 本发明属于数据安全技术领域，具体地涉及一种基于人工智能与区块链智能合约分区的数据防护系统。

背景技术

[0002] 随着近年来数字监控和网络安全漏洞的增加，在大数据时代改善隐私和信息安全越来越重要，特别是在用户的个人数据方面。同时，网络安全和个人信息保护立法的加强也对数据的存储安全的改善提出更高的要求。然而现有多数云存储服务主要以中心化的方式对用户数据进行集中管理，一旦中心节点出现问题，用户数据将面临极大数据访问或者丢失风险。此外，中心化的服务商可以监视，审查和泄露数据给第三方，也会给用户带来泄露隐私等安全问题。而不同的数据其安全等级和安全隐私的程度是不同的，如果所有数据均同等加密保护，会影响系统运行速率，且有些数据本身就是需要共享，加密会影响数据的分享。因此，数据保护需要分区处理。

[0003] 区块链和分布式账本技术为通过去中心化身份和其他隐私机制为保护用户数据提供了新的机会。而人工智能技术为增强系统和用户安全、数据分类和支持改进的分析模型提供了进一步的可能性。因此，本发明基于区块链与人工智能技术，提供了一种数据防护系统。

发明内容

[0004] 为了解决上述问题，本发明提供了一种基于人工智能与区块链智能合约分区的数据防护系统，通过整合区块链、智能合约以及人工智能技术，对数据进行分类识别、有效性验证和重要数据隐蔽保护处理，再通过智能合约进行用户数据分享和权限控制，对数据进行分布式存储，从而极大地提高了云端数据的安全性，有效性和处理效率。

[0005] 为此，本发明的技术方案是：一种基于人工智能与区块链智能合约分区的数据防护系统，包括用户层、服务层、智能合约层和数据层区块链；

[0006] 用户层用于上传数据，数据包括头部和数据的内容；

[0007] 服务层用于对数据进行分类、隐私保护、有效性处理；对数据进行标识，得到数据的类型信息x_j、数据的重要性m_k和数据选择分区所有其它影响因素p(Y)；

[0008] 智能合约层依据数据标识确定数据在区块链上的存储访问策略；根据所述数据标识计算数据的权重W和用户属性U，数据的权重采用如下计算公式如下：

[0009] $$W = a \times \int_0^N f(x_j)dx_j + b \times \int_0^M f(m_k)dm_k + p(Y)$$

[0010] 其中：a、b为常系数；

[0011] N为数据分类后的x_j个数，$\{x_j \mid j=1,2,\cdots,N\}$；

[0012] $M = \frac{m_k}{\sum m_k}$，$\{m_k \mid k = 1,2,\ldots,N\}$，M即所选数据类型的重要性在所有重要性的占比；

[0013] $p(Y)=\sum_{i=0}^{n=i} y_i^n L_i$,其中L是常系数,$y_0=1$;

[0014] 比较所选数据权重W与用户属性U之间的大小关系,根据用户属性U对应的权限,来判断数据所属的分区;不同的数据分区制定不同的规则,不同属性的用户设置不同的访问权限;

[0015] 数据层区块链用于并行处理数据;部署T个云服务器,$S=\{s_i \mid i=1,2,\cdots,T\}$,其中$s_i$为第i个云服务器,T≥N*2,且T为N的倍数,N为数据分类后的x个数;区块链全网节点的总个数为T,分成N组,则每组节点个数$t=\frac{T}{N}(t\geq 2)$;将不同类型的数据分发到各个组所在区的节点,每一组至少有2个节点保存着相同的数据,实现并行处理。

[0016] 优选地,所述服务层对数据的初步处理为安全识别处理,根据预设的黑名单、白名单、敏感字样来识别数据,判断数据是否存在恶意攻击。

[0017] 优选地,所述服务层将数据分为四类,四类数据按照重要性程度由低到高依次为:非核心数据、核心非有效数据、核心非保护数据、核心隐蔽保护数据;类型信息分别为x1、x2、x3、x4,数据的重要性分别为m1、m2、m3、m4;且用户属性按照权限由低到高分别为U_1、U_2、U_3;

[0018] 数据权重W与用户属性U之间的大小关系如下:

[0019] 当$W\leq U_1$时,数据选择存放于非核心区;

[0020] 当$U_1<W\leq U_2$时,数据选择存放于核心非有效区;

[0021] 当$U_2<W\leq U_3$时,数据选择存放于核心非保护区;

[0022] 当$U_3<W$时,数据选择存放于核心保护隐藏区。

[0023] 优选地,所述服务层进行数据分类的具体步骤如下:

[0024] 1)对数据进行是否恶意攻击识别,在通过安全识别处理后继续下一步;

[0025] 2)对数据进行分类识别,根据数据重要性等级进行分析,判断数据为核心数据或非核心数据;

[0026] 3)对于核心数据,对其进行是否有效性识别操作;且对有效数据继续进行下一步的识别掩蔽动作;

[0027] 4)对于核心有效数据,对其进行是否受信息保护识别;对受保护数据,进行掩蔽操作。

[0028] 优选地,所述智能合约层内写入不同组的用户信息、访问权限和相对应的规则,并加载到每个节点上;相对应的加密文件通过智能合约层的调整使用进行创建,并将信息录入到区块链里;用户先通过智能合约层查询访问权限,在满足预先设定的规则时,实现访问不同分区的加密文件:

[0029] ①对非核心数据区,采用开放式的权限规则;

[0030] ②对核心数据区,依照用户所在组的级别属性U,分别授予指定的权限来访问不同核心数据区域。

[0031] 与现有技术相比,本发明的有益效果是:利用人工智能对用户上传的数据进行恶意攻击分析、拦阻,对数据进行分类,对不同重要性的数据进行有效性验证以及对受保护数据进行识别隐藏处理;数据依照重要性和受保护程度不同的属性加密后,按照特定规则在区块链上分区存储;当用户使用数据时,系统通过智能合约层控制用户数据分享的权限,当

识别的用户属性和访问的数据属性一致时，才可以将隐藏处理的数据进行解密重组，恢复为原始信息，从而极大地提高了云端数据访问的安全性、有效性和处理效率。

附图说明

[0032] 以下结合附图和本发明的实施方式来作进一步详细说明

[0033] 图1为本发明的系统框图；

[0034] 图2为本发明的数据处理流程图。

具体实施方式

[0035] 参见附图。本实施例所述数据防护系统，包括用户层、服务层、智能合约层和数据层区块链；用户层用于上传数据，数据包括头部和数据的内容。

[0036] 服务层用于对数据进行分类、隐私保护、有效性处理；对数据进行分类，具体步骤如下：

[0037] 1)对数据进行是否恶意攻击识别，在通过安全识别处理后继续下一步；恶意攻击识别根据现有指标来判别，例如：IP、黑名单、白名单、敏感字样等；

[0038] 2)对数据进行分类识别，根据数据重要性等级进行分析，判断数据为核心数据或非核心数据；

[0039] 3)对于核心数据，对其进行是否有效性识别操作；且对有效数据继续进行下一步的识别掩蔽动作；

[0040] 4)对于核心有效数据，对其进行是否受信息保护识别；对受保护数据，进行掩蔽操作。

[0041] 当用户上传数据经系统进行上述处理完后，产生了四类数据，按照重要性程度由低到高依次为：非核心数据，核心非有效数据，核心非保护数据，核心隐蔽保护数据。四类数据对应的类型信息分别为x_1、x_2、x_3、x_4，四类数据的重要性分别为m_1、m_2、m_3、m_4，类型信息、数据重要性等级采用量化后的信息；根据各个类型性质进行量化，x_1、x_2、x_3、x_4分别量化为不同的值，例如1、2、3、4；根据数据的重要性程度，m_1、m_2、m_3、m_4由低到高依次量化为不同的值，例如1、2、3、4等；数据选择分区还有其它影响因素p(Y)，影响因素包括数据大小、网络节点、带宽、分区节点等，系统对每一个因素自定义赋值。具体的赋值规则，可以通过处理经验进行一一关联。

[0042] 智能合约层依据数据标识确定数据在区块链上的存储访问策略，具体如下；根据所述数据标识计算数据的权重W和用户属性U，用户的权重值依照群组级别属性计算，如经理U_3、员工U_2或其他用户U_1等，从而将数据在区块链上进行分区存储，分为非核心区、核心非有效区、核心非保护数据区、核心保护隐藏数据区；其中，数据的权重采用如下计算公式如下：

[0043] $$W = a \times \int_0^N f(x_j)dx_j + b \times \int_0^M f(m_k)dm_k + p(Y)$$

[0044] 其中：a、b为常系数；

[0045] N为数据分类后的x_j个数，$\{x_j \mid j=1,2,\ldots,N\}$，N＝4；

[0046] $M = \frac{m_k}{\sum m_k}$，$\{m_k \mid k = 1,2,\ldots,N\}$，M即所选数据类型的重要性在所有重要性的占

比；

[0047] $p(Y)=\sum_{i=0}^{n=i} y_i^n L_i$ ，其中L是常系数，y0＝1；系统对每一个影响因素自定义赋值。得到y_1、y_2、y_3等的值，L_1、L_2、L_3等由计算机赋值，不同系统选择不同的影响因素，得到p(Y)，计算时p(Y)相当于不变量。

[0048] 比较所选数据权重W与用户属性U之间的大小关系，根据用户属性U对应的权限，来判断数据所属的分区；用户属性按照权限由低到高分别为U_1、U_2、U_3，用户可对U_1、U_2、U_3自定义赋值，可多次调整数值，满足分类合理性即可。

[0049] 数据权重W与用户属性U之间的大小关系如下：

[0050] 当W≤U_1时，数据选择存放于非核心区；

[0051] 当U_1＜W≤U_2时，数据选择存放于核心非有效区；

[0052] 当U_2＜W≤U_3时，数据选择存放于核心非保护区；

[0053] 当U_3＜W时，数据选择存放于核心保护隐藏区。

[0054] 区块链分区时，部署T个云服务器，S＝{s_i|i＝1,2,...,T}，其中s_i为第i个云服务器，T≥N*2，且T为N的倍数，当数据分为四类，则N＝4，即T≥8；区块链全网节点的总个数为T，分成N组，则每组节点个数$t=\frac{T}{N}(t\geq 2)$；将不同类型的数据分发到各个组所在区的节点，每一组至少有2个节点保存着相同的数据，可以实现并行处理。相对于单链结构的区块链，因此有效提升了处理有效性。

[0055] 不同的数据分区制定不同的规则，不同属性的用户设置不同的访问权限；需将不同组的用户信息，访问权限和相对应的规则写进智能合约里，并加载到每个节点上。相对应的加密文件通过智能合约的调整使用进行创建，并将信息录入到区块链里。用户先通过智能合约查询自己的访问权限，在满足预先设定的规则时实现访问不同分区的加密文件。

[0056] ①对非核心数据区，采用开放式的权限规则从而提升用户数据分享的便利性和快捷性。

[0057] ②对核心数据区，依照用户所在组的级别属性，分别授予指定的权限来访问不同核心数据区域，从而确保数据的安全和隐私。

[0058] 以上所述仅是本发明的优选实施方式，本发明的保护范围并不仅局限于上述实施例，凡属于本发明思路下的技术方案均属于本发明的保护范围。应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理前提下的若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

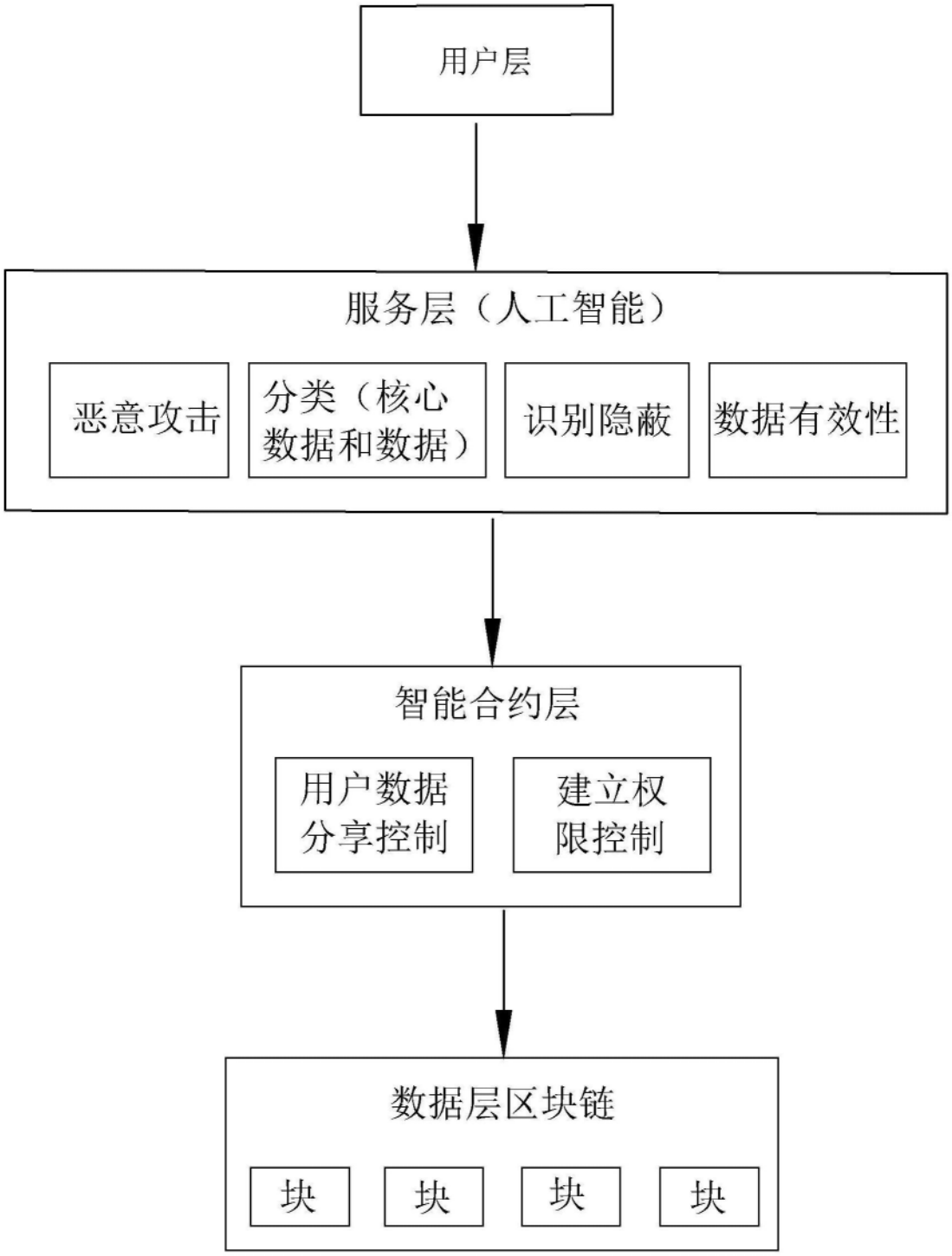

用户层
服务层（人工智能）
恶意攻击
分类（核心数据和数据）
识别隐蔽
数据有效性
智能合约层
用户数据分享控制
建立权限控制
数据层区块链
块
块
块
块

图1

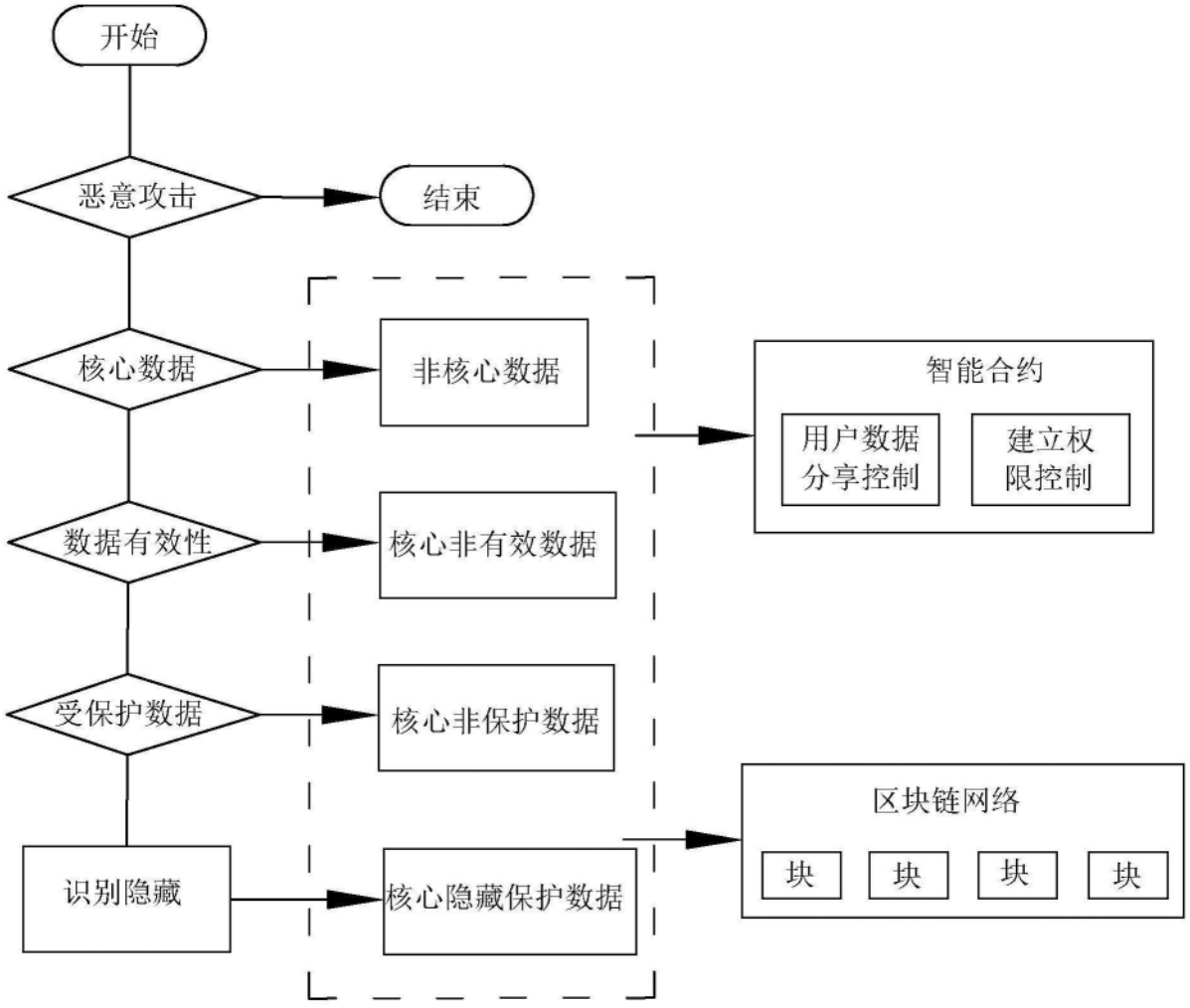

开始
恶意攻击
结束
核心数据
非核心数据
智能合约
用户数据分享控制
建立权限控制
数据有效性
核心非有效数据
受保护数据
核心非保护数据
区块链网络
块
块
块
块
识别隐藏
核心隐藏保护数据

图2