(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 109815717 A
(43)申请公布日 2019.05.28

(21)申请号 201910042526.9

(22)申请日 2019.01.17

(71)申请人 平安科技(深圳)有限公司
地址 518000 广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼

(72)发明人 曾维刚

(74)专利代理机构 深圳众鼎专利商标代理事务所(普通合伙) 44325
代理人 黄章辉

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)

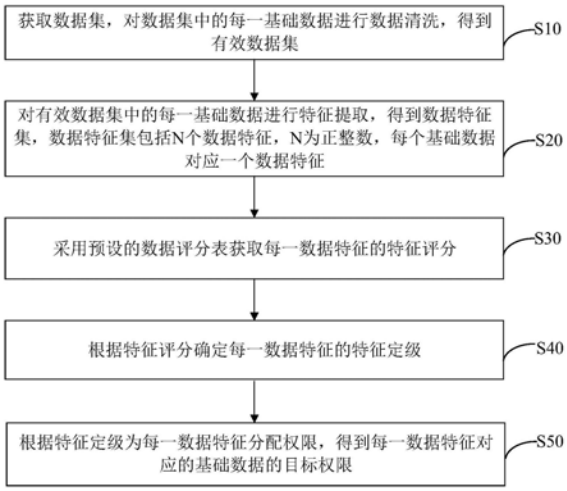
权利要求书2页 说明书11页 附图4页

(54)发明名称

数据权限管理方法、数据访问方法、装置、设备及介质

(57)摘要

本发明公开了一种数据权限管理方法、数据访问方法、装置、设备及介质，所述数据权限管理方法包括：获取数据集，对所述数据集中的每一基础数据进行数据清洗，得到有效数据集；对所述有效数据集中的每一所述基础数据进行特征提取，得到数据特征集，每个所述基础数据对应一个所述数据特征；采用预设的数据评分表获取每一所述数据特征的特征评分；根据所述特征评分确定每一所述数据特征的特征定级；根据所述特征定级为每一所述数据特征分配权限，得到每一所述数据特征对应的所述基础数据的目标权限。上述权限管理方法通过对提取的数据特征进行处理，提高了数据管理效率，并保证了数据访问安全性。



CN 109815717 A

1.一种数据权限管理方法,其特征在于,所述数据权限管理方法包括:

获取数据集,对所述数据集中的每一基础数据进行数据清洗,得到有效数据集;

对所述有效数据集中的每一所述基础数据进行特征提取,得到数据特征集,所述数据特征集包括N个数据特征,N为正整数,每个所述基础数据对应一个所述数据特征;

采用预设的数据评分表获取每一所述数据特征的特征评分;

根据所述特征评分确定每一所述数据特征的特征定级;

根据所述特征定级为每一所述数据特征分配权限,得到每一所述数据特征对应的所述基础数据的目标权限。

2.如权利要求1所述的数据权限管理方法,其特征在于,所述对所述有效数据集进行特征提取,得到数据特征集,包括:

若所述有效数据集的数据类型为文本型,则对所述有效数据集采用分词技术进行分词,得到词组作为所述数据特征集。

3.如权利要求1所述的数据权限管理方法,其特征在于,所述对所述有效数据集进行特征提取,得到数据特征集,包括:

若所述有效数据集的数据类型为二进制数据类型,则采用Brief算法对所述二进制数据类型进行特征提取,得到二进制串作为所述数据特征集。

4.如权利要求1所述的数据权限管理方法,其特征在于,所述对所述有效数据集进行特征提取,得到数据特征集,包括:

若所述有效数据集的数据类型为结构化数据类型,则采用数据库查询语句对所述结构化数据进行查询,得到数据维度作为所述数据特征集。

5.一种数据访问方法,其特征在于,所述数据访问方法包括:

获取数据访问请求,所述数据访问请求包括当前账户信息和待访问数据的数据标识;

从预设数据库中,获取所述当前账户信息对应的访问权限,作为当前访问权限,并获取所述待访问数据的数据标识对应的基础数据的目标权限,作为目标访问权限,其中,所述目标权限是采用如权利要求1至4任一项所述的数据权限管理方法得到的;

验证所述目标访问权限是否超出所述当前访问权限,得到验证结果;

若所述验证结果为所述目标访问权限未超出所述当前访问权限,则从所述预设的数据库中,获取所述数据标识对应的基础数据,作为待显示数据;

按照所述数据标识对应的预设数据转换方式,对所述待显示数据进行数据转换,得到目标显示数据。

6.如权利要求5所述的数据访问方法,其特征在于,所述对所述待显示数据进行数据转换,得到目标显示数据,包括:

对所述待显示数据以数据变形的转换方式进行转换,或者,对所述待显示数据以数据隐藏的转换方式进行转换,得到所述目标显示数据。

7.一种数据权限管理方法装置,其特征在于,所述数据权限管理装置包括:

有效数据集获取模块,用于获取数据集,对所述数据集中的每一基础数据进行数据清洗,得到有效数据集;

数据特征集获取模块,用于对所述有效数据集中的每一所述基础数据进行特征提取,得到数据特征集,所述数据特征集包括N个数据特征,N为正整数,每个所述基础数据对应一

个所述数据特征；

特征评分获取模块，用于采用预设的数据评分表获取每一所述数据特征的特征评分；

特征定级确定模块，用于根据所述特征评分确定每一所述数据特征的特征定级；

目标权限获取模块，用于根据所述特征定级为每一所述数据特征分配权限，得到每一所述数据特征对应的所述基础数据的目标权限。

8.一种数据访问装置，其特征在于，所述数据数据访问装置包括：

数据访问请求获取模块，用于获取数据访问请求，所述数据访问请求包括当前账户信息和待访问数据的数据标识；

访问权限获取模块，用于从预设数据库中，获取所述当前账户信息对应的访问权限，作为当前访问权限，并获取所述待访问数据的数据标识对应的基础数据的目标权限，作为目标访问权限，其中，所述目标权限是采用如权利要求1至4任一项所述的数据权限管理方法得到的；

权限验证模块，用于验证所述目标访问权限是否超出所述当前访问权限，得到验证结果；

待显示数据获取模块，用于在所述验证结果为所述目标访问权限未超出所述当前访问权限时，则从所述预设的数据库中，获取所述数据标识对应的基础数据，作为待显示数据；

目标显示数据获取模块，用于按照所述数据标识对应的预设数据转换方式，对所述待显示数据进行数据转换，得到目标显示数据。

9.一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现如权利要求1至4任一项所述数据权限管理方法，或者所述处理器执行所述计算机程序时实现如权利要求5-6所述的数据访问方法。

10.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至4任一项所述数据权限管理方法，或者所述处理器执行所述计算机程序时实现如权利要求5-6所述的数据访问方法。

数据权限管理方法、数据访问方法、装置、设备及介质

技术领域

[0001] 本发明涉及数据处理领域，尤其涉及一种数据权限管理方法、数据访问方法、装置、设备及介质。

背景技术

[0002] 企业的生产、技术、客户、成本和战略规划等数据，一直以来都是企业赖以生存的核心机密数据，这些数据的丢失或泄露，往往会给企业造成巨大的损失，在系统运行过程中会输出很多日志数据包括很多敏感信息。例如：用户密码、用户银行卡号、家庭住址或者系统通信密钥等，这些数据如果不经过处理就暴露给日志查看人员，泄露风险很高，并且业务生产系统积累了大量包含账户等敏感信息的数据，如果这些数据被泄露和损坏，不仅会给企业带来经济上的损失，而且会给企业的声誉带来负面影响。因此，如何对这些数据进行有效的安全防护已经成为大多数企业关注的重点。

[0003] 传统地，通过人工制定安全规则，完全依赖于人的经验，容易敏感数据的泄露，同时对数据一刀切，数据安全难以保障。

发明内容

[0004] 本发明实施例提供一种数据权限管理方法、装置、设备及介质，以解决数据安全性较低的问题。

[0005] 此外，本发明实施例提供一种数据访问方法、装置、设备及介质，以解决数据访问的安全性较低的问题。

[0006] 一种数据权限管理方法，包括：

[0007] 获取数据集，对所述数据集中的每一基础数据进行数据清洗，得到有效数据集；

[0008] 对所述有效数据集中的每一所述基础数据进行特征提取，得到数据特征集，所述数据特征集包括N个数据特征，N为正整数，每个所述基础数据对应一个所述数据特征；

[0009] 采用预设的数据评分表获取每一所述数据特征的特征评分；

[0010] 根据所述特征评分确定每一所述数据特征的特征定级；

[0011] 根据所述特征定级为每一所述数据特征分配权限，得到每一所述数据特征对应的所述基础数据的目标权限。

[0012] 一种数据权限管理装置，包括：

[0013] 有效数据集获取模块，用于获取数据集，对所述数据集中的每一基础数据进行数据清洗，得到有效数据集；

[0014] 数据特征集获取模块，用于对所述有效数据集中的每一所述基础数据进行特征提取，得到数据特征集，所述数据特征集包括N个数据特征，N为正整数，每个所述基础数据对应一个所述数据特征；

[0015] 特征评分获取模块，用于采用预设的数据评分表获取每一所述数据特征的特征评分；

[0016] 特征定级确定模块，用于根据所述特征评分确定每一所述数据特征的特征定级；

[0017] 目标权限获取模块，用于根据所述特征定级为每一所述数据特征分配权限，得到每一所述数据特征对应的所述基础数据的目标权限。

[0018] 一种数据访问方法，包括：

[0019] 获取数据访问请求，所述数据访问请求包括当前账户信息和待访问数据的数据标识；

[0020] 从预设数据库中，获取所述当前账户信息对应的访问权限，作为当前访问权限，并获取所述待访问数据的数据标识对应的基础数据的目标权限，作为目标访问权限，其中，所述目标权限是采用如权利要求1至4任一项所述的数据权限管理方法得到的；

[0021] 验证所述目标访问权限是否超出所述当前访问权限，得到验证结果；

[0022] 若所述验证结果为所述目标访问权限未超出所述当前访问权限，则从所述预设的数据库中，获取所述数据标识对应的基础数据，作为待显示数据；

[0023] 按照所述数据标识对应的预设数据转换方式，对所述待显示数据进行数据转换，得到目标显示数据。

[0024] 一种数据访问装置，包括：

[0025] 数据访问请求获取模块，用于获取数据访问请求，所述数据访问请求包括当前账户信息和待访问数据的数据标识；

[0026] 访问权限获取模块，用于从预设数据库中，获取所述当前账户信息对应的访问权限，作为当前访问权限，并获取所述待访问数据的数据标识对应的基础数据的目标权限，作为目标访问权限，其中，所述目标权限是采用数据权限管理方法得到的；

[0027] 权限验证模块，用于验证所述目标访问权限是否超出所述当前访问权限，得到验证结果；

[0028] 待显示数据获取模块，用于在所述验证结果为所述目标访问权限未超出所述当前访问权限时，则从所述预设的数据库中，获取所述数据标识对应的基础数据，作为待显示数据；

[0029] 目标显示数据获取模块，用于按照所述数据标识对应的预设数据转换方式，对所述待显示数据进行数据转换，得到目标显示数据。

[0030] 一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现上述数据权限管理方法的步骤，或者，所述处理器执行所述计算机程序时实现上述数据访问方法的步骤。

[0031] 一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述数据权限管理方法的步骤，或者，所述处理器执行所述计算机程序时实现上述数据访问方法的步骤。

[0032] 上述数据权限管理方法、装置、设备及介质中，首先，获取数据集，对数据集中的每一基础数据进行数据清洗，得到有效数据集，避免了后续对数据进行进一步处理产生干扰，提高数据处理效率；然后，对有效数据集中的每一基础数据进行特征提取，得到数据特征集，通过对每一基础数据进行特征提取，从而简化了基础数据，以便后续更加方便快速地对数据进行进一步处理；接着，采用预设的数据评分表获取每一数据特征的特征评分，实现了对数据特征的量化，从而更加直观地反映了数据特征的敏感程度和数据本身的安全性；再

接着，根据特征评分确定每一数据特征的特征定级，减少了对数据特征的冗余操作，以便后续使得数据特征得以高效分类管理；最后，根据特征定级为每一数据特征分配权限，得到每一数据特征对应的基础数据的目标权限，实现了数据集的安全规则的自我进化和数据集中的数据安全访问的个性化。并且有效避免了对数据进行一刀切产生的高风险，提高了数据管理的效率，保证了数据的安全性。

[0033] 上述数据访问方法、装置、设备及介质中，首先，获取数据访问请求；然后，从预设数据库中，获取当前账户信息对应的访问权限，作为当前访问权限，并获取待访问数据的数据标识对应的基础数据的目标权限，作为目标访问权限，使得基础数据的目标权限更为准确；接着，验证目标访问权限是否超出当前访问权限，得到验证结果，以便后续基于该验证结果对数据进行安全访问接下来，若验证结果为目标访问权限未超出当前访问权限，则从预设的数据库中，获取数据标识对应的基础数据，作为待显示数据；最后，按照数据标识对应的预设数据转换方式，对待显示数据进行数据转换，得到目标显示数据，从而保证了目标显示数据的安全性。

附图说明

[0034] 为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例的描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0035] 图1是本发明实施例提供的数据权限管理方法、数据访问方法的应用环境示意图；

[0036] 图2是本发明实施例提供的数据权限管理方法一示例图；

[0037] 图3是本发明实施例提供的数据权限管理装置的一原理框图；

[0038] 图4是本发明实施例提供的数据访问方法的一示例图；

[0039] 图5是本发明实施例提供的数据访问装置的一原理框图；

[0040] 图6是本发明实施例提供的计算机设备的一示意图。

具体实施方式

[0041] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0042] 本申请提供的数据权限管理方法，可应用在如图1的应用环境中，其中，客户端通过网络与服务端进行通信，服务端接收客户端发送的数据集，对数据集中的每一基础数据进行数据清洗，得到有效数据集；然后对有效数据集中的每一基础数据进行特征提取，得到数据特征集；接着，采用预设的数据评分表获取每一数据特征的特征评分；进而根据特征评分确定每一数据特征的特征定级；最后，根据特征定级为每一数据特征分配权限，得到每一数据特征对应的基础数据的目标权限。其中，客户端可以但不限于是各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备。服务端可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

[0043] 在一个实施例中，如图2所示，以该方法应用于图1中的服务端为例进行说明，包括如下步骤：

[0044] S10：获取数据集，对数据集中的每一基础数据进行数据清洗，得到有效数据集。

[0045] 其中，数据集是指不同类型的数据的集合，示例性地，数据集可以包括结构化数据、二进制数据或文本数据等。具体地，数据集可以是服务端从客户端的系统运行的日志数据库中获取得到，也可以是通过客户端的系统数据库中直接获取到数据集，还可以是通过客户端的第三方数据采集工具，从系统数据接口获取数据集，该第三方数据采集工具可以是八爪鱼采集器，也可以是爬山虎采集器等。

[0046] 其中，数据清洗是指对特定的数据进行过滤，用于减少对数据分析的干扰。具体地，数据清洗可以包括对数据集中指定的不需要的基础数据进行清洗、对数据集中的异常基础数据进行清洗、对数据集中的重复基础数据进行清洗和对数据集进行基础数据关联性校验进而对不存在关联的数据进行清洗。

[0047] 示例性地，若去除指定的不需要数据，则可以通过查询数据集中的基础数据，当该数据集中存在与预设关键字库中相同的基础数据时，去除对应的基础数据，其中的关键字库是指包含有指定的数据以及具有指定数据特征的数据。若去除异常的基础数据，则可以通过字符串比较方法进行数据校验，得到数据格式不符合预设格式或者数据内容不符合预设内容的异常基础数据。比如，中国人姓名出现数字和字母、身份证号码出现文字字符或年龄超过200岁的异常基础数据等。若对基础数据进行关联性校验，则可以通过正则表达式进行关联性校验，比如身份证号码和出生年月不一致或者身份证号和性别不一致等情形。可以理解地，通过每一基础数据进行数据清洗，清除了错误异常的基础数据，避免了后续对数据进行进一步处理产生干扰，提高数据处理效率。

[0048] S20：对有效数据集中的每一基础数据进行特征提取，得到数据特征集，数据特征集包括N个数据特征，N为正整数，每个基础数据对应一个数据特征。

[0049] 其中，特征提取是一种对数据进行关键信息提取的操作。用于获取基础数据的关键信息。数据特征是指能够体现数据属性的关键数据，用于对表征数据的特性。特征提取的具体实现过程为：先对基础数据进行分割，形成一个或者多个基础数据词汇，然后对每个基础数据词汇使用词性标注工具(如ictclas)进行词性标注，得到词性数据特征。最后通过词频统计工具对每一词性数据特征对应的基础数据进行词频统计，根据词频得到数据特征。例如，一基础数据为“我的身份证号是534232323232323，我的密码是754312，我家地址是广东省深圳市”，通过对该基础数据进行特征提取，得到的数据特征为{“身份证”、“密码”、“地址”}。本步骤中的特征提取方法可以是分词的特征提取方法，也可以是基于Brief算法的特征提取方法，还可以是结构化语言查询的特征提取方法。

[0050] 可以理解地，通过对每一基础数据进行特征提取，从而简化了基础数据，以便后续更加方便快速地对数据进行进一步处理。需要说明的是，一个数据特征包含一个或者多个子数据特征，继续以本步骤中的数据特征{“身份证”、“密码”、“地址”}为例，该数据特征包含3个子数据特征，分别为“身份证”子数据特征、“密码”子数据特征和“地址”子数据特征。

[0051] S30：采用预设的数据评分表获取每一数据特征的特征评分。

[0052] 其中，预设的数据评分表是指预先设置的对数据进行打分的表格。用于映射数据的敏感程度。在数据评分表中，分值越高，代表数据敏感程度越高。特征评分是根据数据的

敏感程度进行评价得到的分值，用于反映数据的敏感程度。示例性地，在一企业资源计划(Enterprise Resource Planning,ERP)系统中，该数据评分表用于对ERP系统数据库中的数据进行评分，以便后续对数据进行管理。例如，数据特征为{“地址”}，其特征评分为3分，数据特征为{“电话号码”}，其特征评分为4分，数据特征为{“密码”}，其特征评分为10分。具体地，可以在预设的数据评分中，以数据特征作为查询条件，查询与数据特征对应的分值，即为该数据特征的数据评分。可以理解地，通过对数据特征进行评分，实现了对数据特征的量化，从而更加直观地反映了数据特征的敏感程度和数据本身的安全性。

[0053] 需要说明的是，当数据特征包含多个子数据特征时，可以采用预设的数据评分表对每一子数据特征进行评分，然后对评分进行汇总，即可得到数据特征评分。其中的汇总方式可以是将每一子数据特征的评分进行叠加后求取平均值的汇总方式，也可以是对每一子数据特征赋予相应的权值，进行加权求和的汇总方式。具体的权值设置可根据实际需要进行选择，此处不作限制。

[0054] S40:根据特征评分确定每一数据特征的特征定级。

[0055] 其中，特征定级是用于表征数据特征的级别，每一特征定级对应一个特征评分区间。其中，特征定级与特征评分区间的对应关系可以根据实际需求进行设定。具体地，通过判断特征评分落在的评分区间，进而根据评分区间与特征关系的对照表格确定数据特征的特征定级。例如，特征定级位1级对应的评分区间为[0,1.5]，特征定级位2级对应的评分区间为[1.6,3]，特征定级位2级对应的评分区间为[3.1,4.5]...特征定级位10级对应的评分区间为[13.6,15]。当某一数据特征评分为1.4时，该数据特征的特征定级即为1级。可以理解地，不同的数据特征其特征评分也不同，由于有效数据集中的数据特征数量繁多，其特征评分的数量也会很多，不便于后续的处理，因此，根据特征评分确定每一数据特征的特征定级，减少了对数据特征的冗余操作，以便后续使得数据特征得以高效分类管理。

[0056] S50:根据特征定级为每一数据特征分配权限，得到每一数据特征对应的基础数据的目标权限。

[0057] 其中，该步骤中的权限是指访问权限，用于根据在各种预定义的组中用户的身份标识及其成员身份来限制访问数据的机制，防止数据一刀切，即完全暴露给用户或者完全限制用户访问。具体地，根据特征定级，对数据特征对应的基础数据进行权限分配，容易理解地，特征评分与特征定级之间的关系为正相关，特征定级与目标权限的之间也是呈正相关，因此，特征定级越高，分配的目标权限越大，即该基础数据需要的访问权限越大。进一步地，可以预先设定一个权限分配表，根据特征定级和目标权限的对应关系，对每个数据特征分配权限，得到目标权限。该权限分配表可以通过数据规则领域专家依据经验来设定，也可以根据实际需要进行设定。

[0058] 可以理解地，客户端访问数据时，只能访问到小于或者等于自身目标权限级别的数据。例如，某一数据特征对应的基础数据的目标权限级别最低，则该基础数据访问方式即为最低目标权限对应的访问方式。

[0059] 该步骤中，通过根据特征定级为每一数据特征分配权限，得到每一数据特征对应的基础数据的目标权限，实现了数据集的安全规则的自我进化和数据集中的数据安全访问的个性化。并且有效避免了对数据进行一刀切产生的高风险，提高了数据管理的效率，保证了数据的安全性。

[0060] 本实施例中，首先，获取数据集，对数据集中的每一基础数据进行数据清洗，得到有效数据集，避免了后续对数据进行进一步处理产生干扰，提高数据处理效率；然后，对有效数据集中的每一基础数据进行特征提取，得到数据特征集，通过对每一基础数据进行特征提取，从而简化了基础数据，以便后续更加方便快速地对数据进行进一步处理；接着，采用预设的数据评分表获取每一数据特征的特征评分，实现了对数据特征的量化，从而更加直观地反映了数据特征的敏感程度和数据本身的安全性；再接着，根据特征评分确定每一数据特征的特征定级，减少了对数据特征的冗余操作，以便后续使得数据特征得以高效分类管理；最后，根据特征定级为每一数据特征分配权限，得到每一数据特征对应的基础数据的目标权限，实现了数据集的安全规则的自我进化和数据集中的数据安全访问的个性化。并且有效避免了对数据进行一刀切产生的高风险，提高了数据管理的效率，保证了数据的安全性。

[0061] 在一实施例中，步骤S30中，对有效数据集进行特征提取，得到数据特征集，具体为：

[0062] S31：若有效数据集的数据类型为文本型，则对有效数据集采用分词技术进行分词，得到词组作为数据特征集。

[0063] 其中，文本型的有效数据集是指文本格式的数据组成的数据集，如文本“中华人民共和国”。词组是指文本类型的数据集中的数据进行分词处理后得到且计算机能够自动识别语义的文本的单元文本数据。例如，“中华人民共和国”通过分词技术得到“中华”、“人民”和“共和国”三个词组。又如：例如“我的身份证”“张三的身份证”，这两个文本型的数据的共同特征“身份证”，因此，将“身份证”这一词组作为数据特征。

[0064] 其中，分词是指将文本类型的数据集中文本序列切分成计算机能够自动识别语义的词组。而分词技术是搜索引擎针对用户提交查询的关键词串进行的查询处理后根据用户的关键词串用各种匹配方法进行的一种技术。该分词技术可以是基于字符串的分词方法，也可以是基于理解地分词方法，还可以是基于统计的分词方法。优选地，本实施例中采用基于字符串匹配的分词算法进行分词处理。具体地，首先将有效数据集中的基础数据进行分割后，得到多个字符串，然后将该多个字符串与预设的关键字符库中的关键字符串匹配，将与关键字符串匹配的字符串作为词组，即得到数据特征。

[0065] 本实施例中，通过分词技术对有效数据集进行特征提取，从而实现对有效数据集中的基础数据的优化，获取更加准确的有数据特征。

[0066] 在一实施例中，步骤S30中，对有效数据集进行特征提取，得到数据特征集，具体为：

[0067] S31’：若有效数据集的数据类型为二进制数据类型，则采用Brief算法对二进制数据类型进行特征提取，得到二进制串作为数据特征集。

[0068] 其中，二进制数据类型是指数值型数据，用于标识数据集中数值类型的数据，例如：手机号码，身份证号码或者图像、视频等的二进制文中包含的二进制数据等。Brief算法(Binary Robust Independent Elementary Features)是在特征点附近随机选取若干点对，将这些点对的灰度值的大小，组合成一个二进制串，并将这个二进制串作为该特征点的特征描述子的算法，用于提取二进制串的数据特征。具体地，将二进制数据类型的数据具有关联特征的二进制数据作为数据特征集。例如，身份证号码的18位数字，有八位数字表示出

生年月日，能够体现身份证的特征，因此，采用Brief算法将其中的8为数字作为数据集特征，例如，当有一个八位二进制数据时，将其作为身份证号码的二进制串。

[0069] 可以理解地，例如，一数据集包含有10000个人的身份证信息，其中，身份证号码是一个18位的浮点数，企业管理系统的数据库中身份证信息较多，势必占用大量的内存空间并且意味着越长的匹配时间。为此，通过Brief算法对二进制数据类型的有效数据集进行特征提取，减少信息存储空间。有利于后续对特征数据特征的进一步处理。

[0070] 在一实施例中，步骤S30中，对有效数据集进行特征提取，得到数据特征集，具体为：

[0071] S31”：若有效数据集的数据类型为结构化数据类型，则采用数据库查询语句对结构化数据进行查询，得到数据维度作为数据特征集。

[0072] 其中，结构化数据是指数据库范畴的数据表中的数据，如数据表中的字段和属性等。例如，如用户表t_user里面的字段用户名username，密码password等即为结构化的数据。其中，数据维度是指结构化数据的数据属性。例如，密码password体现了该结构化数据的数据特征为{“密码”}。

[0073] 具体地，数据库查询语句是指结构化查询语言(SQL)指令，提取出结构化数据的数据维度，进而得到结构化数据的数据特征集。

[0074] 本实施例中，采用数据库查询语句对结构化数据进行查询，得到数据维度作为数据特征集，能够快速准确地提取数据特征，提高了数据特征的获取效率。

[0075] 可以理解地，特征提取在提高数据安全性中起着非常关键的作用。对有效数据集的特征提取的方法进行归纳分类，将有利于提高有效数据特征集的准确性和完整性。步骤S31、步骤S31’和步骤S31”中，特征提取方法可以是分词的特征提取方法，也可以是基于Brief算法的特征提取方法，还可以是结构化语言查询的特征提取方法。通过对有效数据集中的数据类型进行判断，对每一数据类型的数据采用对应的方法进行特征提取，高效得获取了数据集的数据特征，从而高效地得到有效数据特征集，以便后续对数据进行安全防护。

[0076] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0077] 在一实施例中，提供一种数据权限管理装置，该数据权限管理装置与上述实施例中数据权限管理方法一一对应。如图3所示，该基于深度学习的文本分析装置包括有效数据集获取模块10、数据特征集获取模块20、特征评分获取模块30、特征定级确定模块40和目标权限获取模块50。各功能模块详细说明如下：

[0078] 有效数据集获取模块10，用于获取数据集，对数据集中的每一基础数据进行数据清洗，得到有效数据集；

[0079] 数据特征集获取模块20，用于对有效数据集中的每一基础数据进行特征提取，得到数据特征集，数据特征集包括N个数据特征，N为正整数，每个基础数据对应一个数据特征；

[0080] 特征评分获取模块30，用于采用预设的数据评分表获取每一数据特征的特征评分；

[0081] 特征定级确定模块40，用于根据特征评分确定每一数据特征的特征定级；

[0082] 目标权限获取模块50，用于根据特征定级为每一数据特征分配权限，得到每一数据特征对应的基础数据的目标权限。

[0083] 优选地，数据特征集获取模块包括第一数据特征获取单元，用于在有效数据集的数据类型为文本型时，则对有效数据集采用分词技术进行分词，得到词组作为数据特征集。

[0084] 优选地，数据特征集获取模块还包括第二数据特征获取单元，用于在有效数据集的数据类型为二进制数据类型时，则采用Brief算法对二进制数据类型进行特征提取，得到二进制串作为数据特征集。

[0085] 优选地，数据特征集获取模块还包括第三数据特征获取单元，用于在有效数据集的数据类型为结构化数据类型时，则采用数据库查询语句对结构化数据进行查询，得到数据维度作为数据特征集。

[0086] 在一实施例中，提供一数据访问方法，该数据访问方法也可以应用在如图1的应用环境中，其中，客户端通过网络与服务端进行通信。服务端接收客户端发送的数据访问请求；然后，从预设数据库中，获取当前账户信息对应的访问权限，作为当前访问权限，并获取待访问数据的数据标识对应的基础数据的目标权限，作为目标访问权限；接着，若验证结果为目标访问权限未超出当前访问权限，则从预设的数据库中，获取数据标识对应的基础数据，作为待显示数据；最后，按照数据标识对应的预设数据转换方式，对待显示数据进行数据转换，得到目标显示数据。其中，客户端可以但不限于是各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备。服务端可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

[0087] 在一个实施例中，如图4所示，以该方法应用于图1中的服务端为例进行说明，包括如下步骤：

[0088] S60：获取数据访问请求，数据访问请求包括当前账户信息和待访问数据的数据标识。

[0089] 其中，数据访问请求为客户端发起的对数据进行访问的请求。具体地，用户通过客户端输入对应的指令或信息来触发该数据访问请求。客户端将该数据访问请求请求发送至服务端，服务端即获取到数据访问请求。当前账户信息是指访问数据的账户信息，如账号和密码。待访问数据的数据标识是用于唯一标识出不同的数据特征。在一个实施方式中，数据标识可以为数据库名称或者数据日志名称等。

[0090] S70：从预设数据库中，获取当前账户信息对应的访问权限，作为当前访问权限，并获取待访问数据的数据标识对应的基础数据的目标权限，作为目标访问权限，其中，目标权限是采用数据权限管理方法得到的。

[0091] 其中，预设数据库是指预先设定的用于存储账户信息与访问权限映射关系的数据库。当前访问权限是指与当前账户信息对应的访问权限。例如：账户信息为“管理员”时，当前访问权限为最高级别的权限，账户信息为“普通用户”时，当前访问权限为较低级别的权限。目标访问权限是指待访问数据的数据标识对应的基础数据的目标权限，由于该目标权限是采用数据权限管理方法得到的，使得基础数据的目标权限更为准确。

[0092] S80：验证目标访问权限是否超出当前访问权限，得到验证结果。

[0093] 具体地，比较目标访问权限和当前访问权限的级别关系，得到二者之间的大小关系，作为验证结果。可选地，目标访问权限和当前访问权限均可以通过数值进行反映，继而

比较各自对应的数字大小，若目标访问权限对应的数值大于当前访问权限对应的数值，验证结果为目标访问权限超出当前访问权限，当目标访问权限对应的数值小于或者等于当前访问权限对应的数值，验证结果为目标访问权限未超出当前访问权限，以便后续基于该验证结果对数据进行安全访问。

[0094] S90：若验证结果为目标访问权限未超出当前访问权限，则从预设的数据库中，获取数据标识对应的基础数据，作为待显示数据。

[0095] 具体地，当目标访问权限未超出当前访问权限时，即当前访问权限的级别大于或者等于目标访问权限的级别，此时，能够获取到获取数据标识对应的基础数据，即从预设的数据库中，获取数据标识对应的基础数据，作为待显示数据。

[0096] S100：按照数据标识对应的预设数据转换方式，对待显示数据进行数据转换，得到目标显示数据。

[0097] 其中，预设数据转换方式是指预先设定的用于对数据形式进行转换处理方式，如对数据进行变形、马赛克处理或者隐藏处理等，保证数据的安全性。具体地，在获取到待显示数据后，服务端根据数据标识对应的预设数据转换方式，对待显示数据进行数据转换，得到目标显示数据，从而保证了目标显示数据的安全性。

[0098] 本实施例中，首先，获取数据访问请求；然后，从预设数据库中，获取当前账户信息对应的访问权限，作为当前访问权限，并获取待访问数据的数据标识对应的基础数据的目标权限，作为目标访问权限，使得基础数据的目标权限更为准确；接着，验证目标访问权限是否超出当前访问权限，得到验证结果，以便后续基于该验证结果对数据进行安全访问接下来，若验证结果为目标访问权限未超出当前访问权限，则从预设的数据库中，获取数据标识对应的基础数据，作为待显示数据；最后，按照数据标识对应的预设数据转换方式，对待显示数据进行数据转换，得到目标显示数据，从而保证了目标显示数据的安全性。

[0099] 在一实施例中，步骤S100中，对待显示数据进行数据转换，得到目标显示数据，具体为：

[0100] 对待显示数据以数据变形的转换方式进行转换，或者，对待显示数据以数据隐藏的转换方式进行转换，得到目标显示数据。

[0101] 其中，对目标数据进行变形是指对将数据以区别于自身的方式进行显示的转换方法。对数据进行隐藏是指对目标数据中一些数据去掉，不进行显示的转换方法。在一具体实施方式中，待显示数据为“我的身份证号是534232323232323，我的密码是754312，我家地址是广东省深圳市”，当对待显示数据进行变形时，得到的目标显示数据如下：“我的身份证号是534232323232323，我的密码是******，我家地址是广东省深圳市”。当对待显示数据进行隐藏时，目标显示数据如下：“我的身份证号是534232323232323，我的密码是，我家地址是广东省深圳市”。

[0102] 本实施例中，通过对待显示数据进行变形或者隐藏，不仅简单方便，而且使得访问用户能够更加直观的进行数据访问，同时也提高了数据访问的安全性。

[0103] 本在一实施例中，提供一种数据访问装置，该数据访问装置与上述实施例中数据权限管理方法一一对应。如图5所示，该数据访问装置包括数据访问请求获取模块60、访问权限获取模块70、权限验证模块80、待显示数据获取模块90和目标显示数据获取模块100。各功能模块详细说明如下：

[0104] 数据访问请求获取模块60，用于获取数据访问请求，数据访问请求包括当前账户信息和待访问数据的数据标识；

[0105] 访问权限获取模块70，用于从预设数据库中，获取当前账户信息对应的访问权限，作为当前访问权限，并获取待访问数据的数据标识对应的基础数据的目标权限，作为目标访问权限，其中，目标权限是采用数据权限管理方法得到的；

[0106] 权限验证模块80，用于验证目标访问权限是否超出当前访问权限，得到验证结果；

[0107] 待显示数据获取模块90，用于在验证结果为目标访问权限未超出当前访问权限时，则从预设的数据库中，获取数据标识对应的基础数据，作为待显示数据；

[0108] 目标显示数据获取模块100，用于按照数据标识对应的预设数据转换方式，对待显示数据进行数据转换，得到目标显示数据。

[0109] 优选地，目标显示数据获取模块包括目标显示数据转换单元，用于对待显示数据以数据变形的转换方式进行转换，或者，对待显示数据以数据隐藏的转换方式进行转换，得到目标显示数据。

[0110] 关于数据权限管理装置的具体限定可以参见上文中对于数据权限管理方法的限定，在此不再赘述。上述数据权限管理装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[0111] 在一个实施例中，提供了一种计算机设备，该计算机设备可以是服务器，其内部结构图可以如图6所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于数据权限管理方法中使用到的数据。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种数据权限管理方法。

[0112] 在一个实施例中，提供了一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行计算机程序时实现上述实施例中的数据权限管理方法，或者处理器执行计算机程序时实现上述实施例中的数据访问方法。

[0113] 在一个实施例中，提供了一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时实现上述实施例中的数据权限管理方法，或者处理器执行所述计算机程序时实现上述实施例中的数据访问方法。

[0114] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限，RAM以多种形式可得，

诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0115] 所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,仅以上述各功能单元、模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能单元、模块完成,即将所述装置的内部结构划分成不同的功能单元或模块,以完成以上描述的全部或者部分功能。

[0116] 以上所述实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围,均应包含在本发明的保护范围之内。

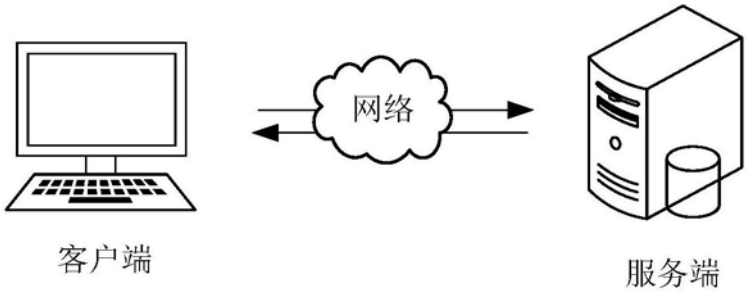

网络
客户端
服务端

图1

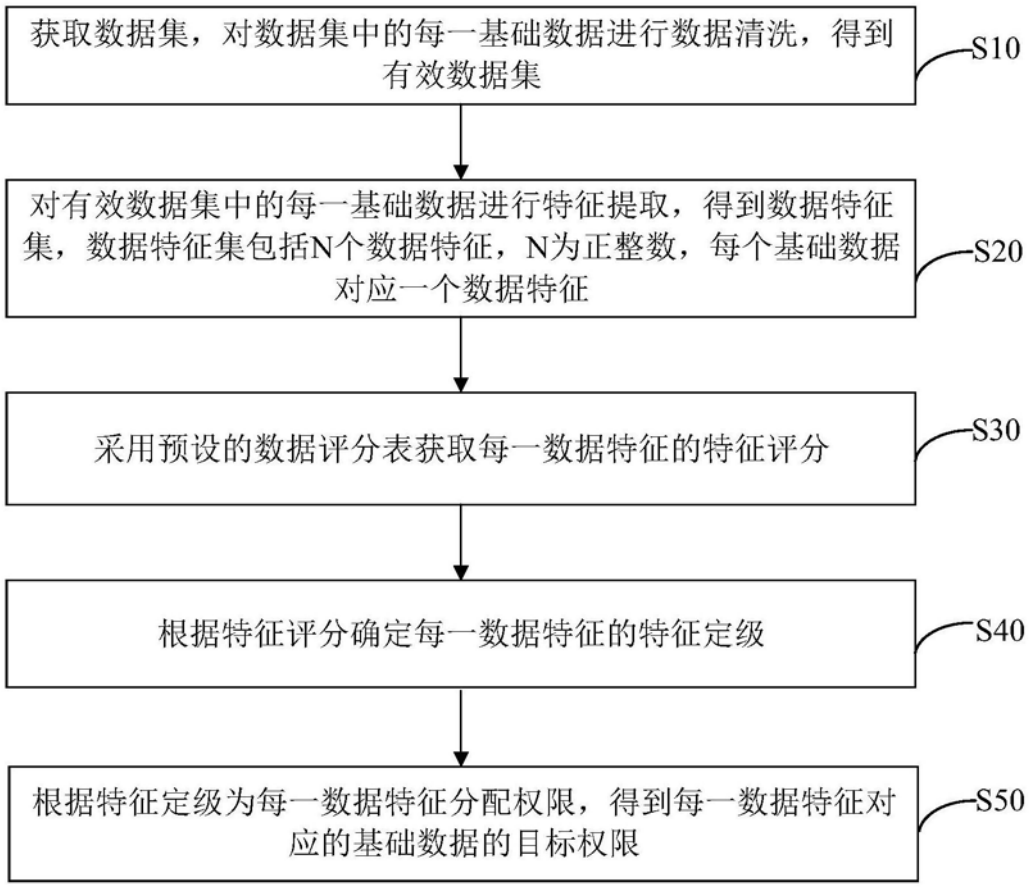

获取数据集，对数据集中的每一基础数据进行数据清洗，得到有效数据集
S10
对有效数据集中的每一基础数据进行特征提取，得到数据特征集，数据特征集包括N个数据特征，N为正整数，每个基础数据对应一个数据特征
S20
采用预设的数据评分表获取每一数据特征的特征评分
S30
根据特征评分确定每一数据特征的特征定级
S40
根据特征定级为每一数据特征分配权限，得到每一数据特征对应的基础数据的目标权限
S50

图2

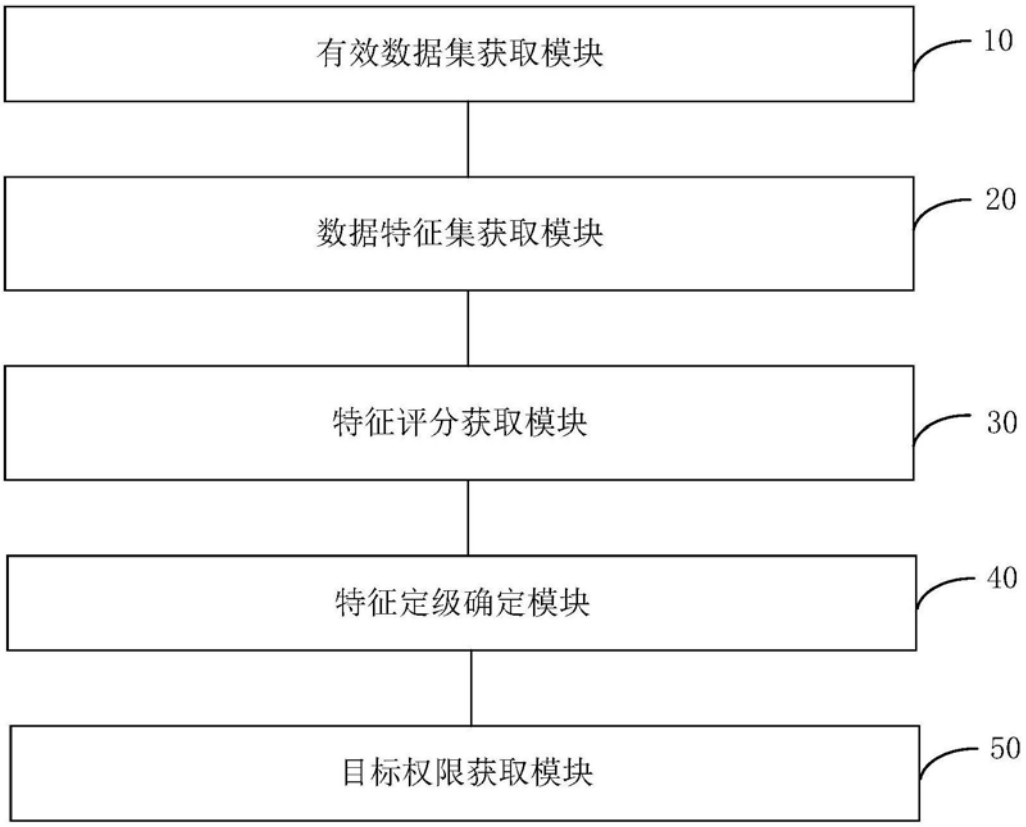

有效数据集获取模块
10
数据特征集获取模块
20
特征评分获取模块
30
特征定级确定模块
40
目标权限获取模块
50

图3

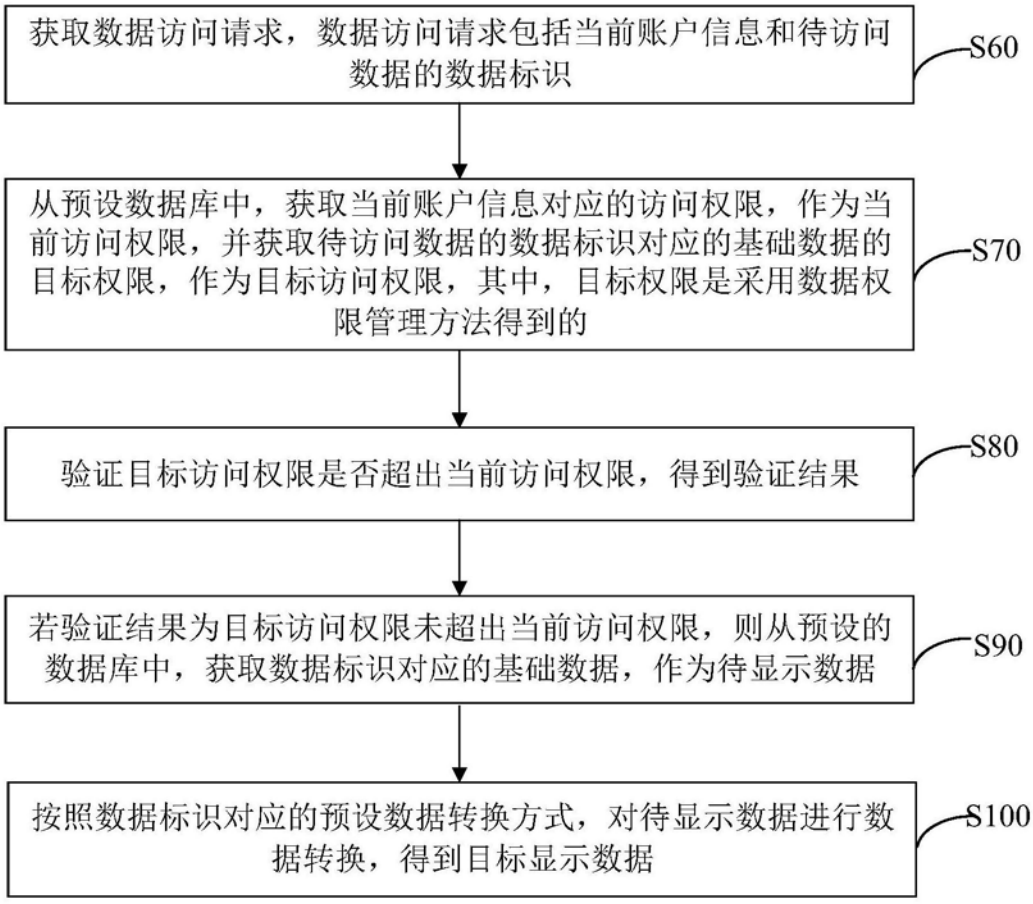

获取数据访问请求，数据访问请求包括当前账户信息和待访问数据的数据标识
S60
从预设数据库中，获取当前账户信息对应的访问权限，作为当前访问权限，并获取待访问数据的数据标识对应的基础数据的目标权限，作为目标访问权限，其中，目标权限是采用数据权限管理方法得到的
S70
验证目标访问权限是否超出当前访问权限，得到验证结果
S80
若验证结果为目标访问权限未超出当前访问权限，则从预设的数据库中，获取数据标识对应的基础数据，作为待显示数据
S90
按照数据标识对应的预设数据转换方式，对待显示数据进行数据转换，得到目标显示数据
S100

图4

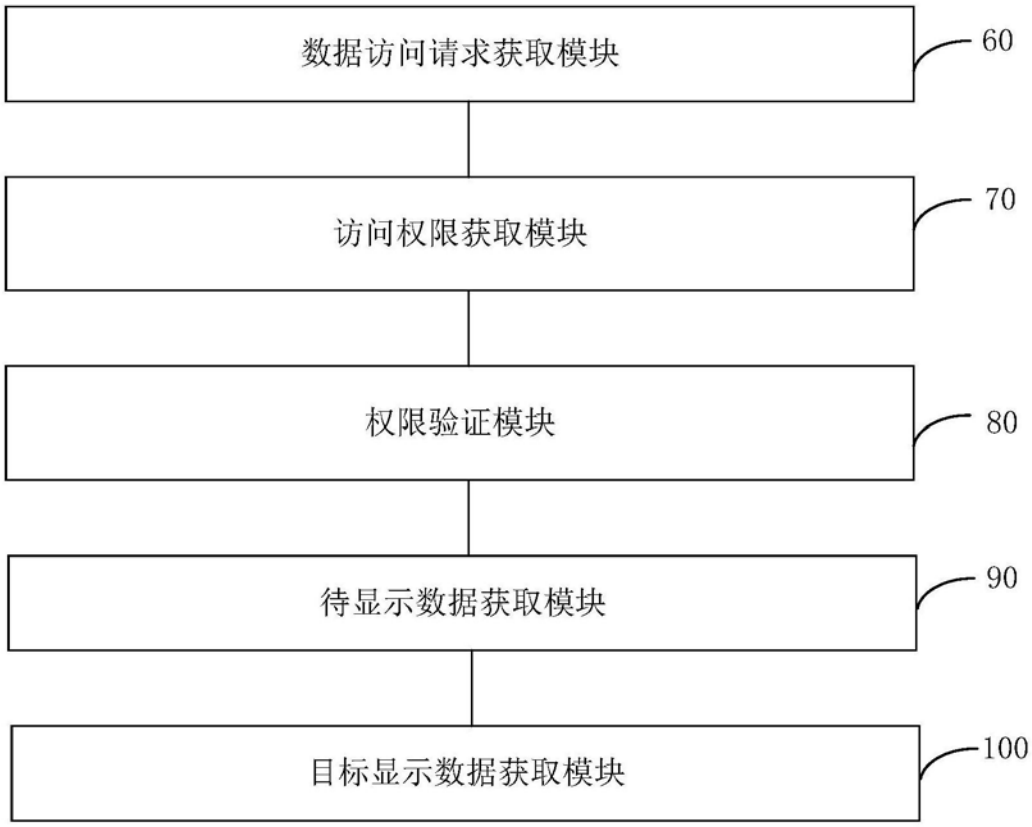

数据访问请求获取模块
60
访问权限获取模块
70
权限验证模块
80
待显示数据获取模块
90
目标显示数据获取模块
100

图5

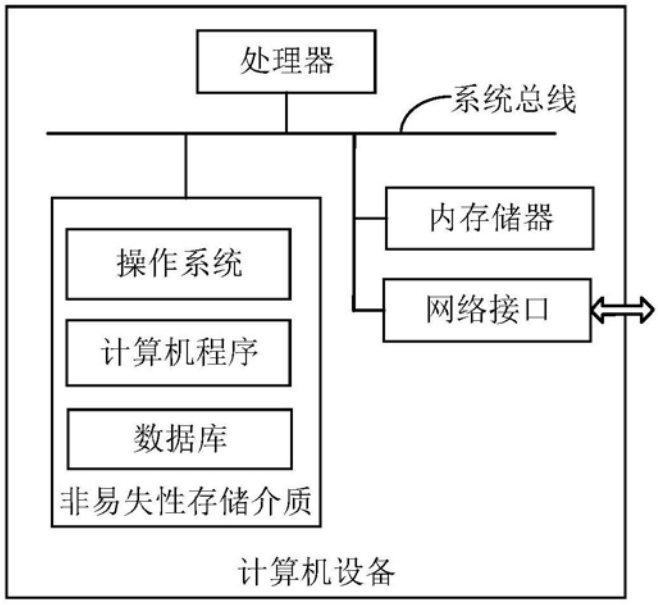

处理器
系统总线
内存储器
网络接口
操作系统
计算机程序
数据库
非易失性存储介质
计算机设备

图6