

说明书

一种规则检测方法、计算机系统及可读存储介质

技术领域

5 本说明书涉及计算机技术领域，尤其涉及一种规则检测方法、计算机系统及可读存储介质。

背景技术

目前，线上业务的执行往往需要配置相应的营销规则，以给用户带来丰富的业务体验。例如，对于一款商品 A 的线上营销活动来说，可以配置诸如“满 100，可 5 折购买商品 A”的营销规则，从而可以使得用户可以更为实惠的价格购买商品 A。

而为了保证用户的正常业务体验，在营销规则上线前，通常需要对其进行检测，以保证营销规则可以正常的使用。但是由于实际配置的营销规则众多，这就使得工作人员需要耗费大量的时间成本来完成营销规则的检测工作。并且，在实际应用中多个营销规则可以配合使用，这使得工作人员需要在准确梳理出各营销规则之间的逻辑关系的情况下，才能

15 对其进行检测，这不仅对工作人员的能力要求极高，也难免会出现检测错误。

所以，如何准确的对营销规则进行检测，则是一个亟待解决的问题。

发明内容

20 本说明书提供一种规则检测方法、计算机系统及可读存储介质，以部分的解决现有技术存在的上述问题。

本说明书提供了一种规则检测方法，包括：获取待检测规则，所述待检测规则中记录有若干子规则以及各子规则之间的组合方式；根据所述若干子规则以及所述组合方式，预测所述待检测规则应命中的流量，并从预设的历史流量数据中查询出所述待检测规则实际命中的历史流量数据；根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测。

25

本说明书提供了一种计算机系统，所述计算机系统包括存储器、处理器及存储在所述存储器上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程序时实现如下步骤：获取待检测规则，所述待检测规则中记录有若干子规则以及各子规则之间的组合方式；根据所述若干子规则以及所述组合方式，预测所述待检测规则应命中的流量，并从预设的历史流量数据中查询出所述待检测规则实际命中的历史流量数据；根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测。

30

本说明书提供了一种可读存储介质，所述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规则检测方法。

本说明书采用的上述至少一个技术方案能够达到以下有益效果：

在本说明书实施例提供的规则检测的方法中，在获取到待检测规则后，可以先通过历史流量数据，确定出待检测规则实际所能命中的历史流量数据，然后，通过待检测规则中所包含的各子规则之间的组合方式以及待检测规则实际所能命中的历史流量数据，来检测待检测规则是否存在错配的情况。通过这种方式，不仅可以极大的提高检测效率，降低规则检测的时间成本，并且，可以有效的提高规则检测的准确性。

附图说明

此处所说明的附图用来提供对本说明书的进一步理解，构成本说明书的一部分，本说明书的示意性实施例及其说明用于解释本说明书，并不构成对本说明书的不当限定。在附图中：

图 1 为本说明书实施例提供的一种规则检测的方法的流程示意图；

图 2 为本说明书实施例提供的一种规则检测的详细流程图；

图 3 为本说明书实施例提供的计算机系统的结构示意图。

具体实施方式

为使本说明书的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本说明书保护的范围。

以下结合附图，详细说明本说明书各实施例提供的技术方案。

图 1 为本说明书中提供的一种规则检测的方法的流程示意图，包括以下步骤：

S101：获取待检测规则，所述待检测规则中记录有若干子规则以及各子规则之间的组合方式。

在实际应用中，各项业务可以使用相应的营销规则，这些营销规则通常都是工作人员基于实际需求以及经验进行配置的，以为用户提供更好的业务体验。

而为了保证这些营销规则在实际使用中不会出现异常，为此，需要在这些营销规则实际上线前对其进行检测。那么，在本说明书实施例中，需要在线上进行检测的营销规则即可以称之为是待检测规则。

待检测规则中实际上可以包含有若干个子规则，这些子规则可以按照特定的组合方式进行组合，从而得到待检测规则。

这里提到的组合方式主要用于体现各子规则之间“或”或是“且”的逻辑运算关系，例如，假设待检测规则中包含有子规则 1 和子规则 2，子规则 1 为：商家 A、商家 B 或是商家 C 可以使用优惠券，子规则 2 为：当结算总价超过 200 时，可以使用 8 折的优惠券。子规则 1 和子规则 2 之间的组合方式为“且”的组合方式。那么，待检测规则应命中的流

量应该为在商家 A、商家 B 或是商家 C 结算总价超过 200 时，使用 8 折优惠券的流量。

在本说明书实施例中，可以通过多种方式来确定并获取待检测规则，例如，可以通过订阅营销规则表的变更通知，实时感知营销规则的新增或是修改，而感知的新增的营销规则或是修改的营销规则，即为待检测规则；再例如，可以通过设置相应的监听器，实时监
5 听营销规则的变更情况，当该监听器监听到营销规则出现新增或是修改后，可以确定出新增或是修改的营销规则，并基于营销规则对应的规则标识发送变更消息，以通过该变更消息，来确定并获取待检测规则。

在本说明书实施例中，用于实现一种规则检测的方法的执行主体可以是诸如台式电脑等终端设备，当然，也可以是安装在终端设备上的客户端，抑或是服务器。为了便于描述，
10 本说明书实施例仅以服务器作为执行主体为例，对本说明书实施例中提供的一种规则检测的方法进行说明。

S102：根据所述若干子规则以及所述组合方式，预测所述待检测规则应命中的流量，并从预设的历史流量数据中查询出所述待检测规则实际命中的历史流量数据。

由于无论待检测规则是否出现错配，基于待检测规则中包含的若干子规则之间的组合
15 方式，实际上均可以反映出待检测规则应该命中哪些流量。所以，服务器可以基于上述组合方式，来预测待检测规则应该命中的流量。

在本说明书实施例中，预测出的待检测规则应命中的流量并不一定是指要预测出待检测规则真实所命中的流量，而是主要用于体现出待检测规则应命中的流量所具备的一些特性。这些特性主要可以通过两个方面来体现，一是表示待检测规则应该命中的流量中所包
20 含的字段值的数值范围，二是表示待检测规则应该命中的流量中应该出现哪些字段值，或是不应该出现哪些字段值。

之所以分为上述两个方面，主要是因为在实际应用中，待检测规则中包含的子规则可以分为两种类别，一种属于数值类规则，数值类规则主要用于体现营销规则所适用的范围，例如，当购物累计金额超过 500 时，所有商品享受 7 折优惠，这一营销规则即为一种数值
25 类规则。另一种属于枚举类规则，枚举类规则主要用于体现营销规则适用于哪些个体，例如，如果在商户 A、商户 B 或是商户 C 购物时，可是使用代金券，这一营销规则即为一种枚举类规则。

对于上述数值类规则来说，服务器可以根据待检测规则中各子规则中涉及的字段值以及字段值所对应的比较符号，来预测出待检测规则应该命中的流量中所出现的字段值的最大
30 值和最小值，进入确定出待检测规则应该命中的流量中所出现的字段值的数值范围。

例如，假设待检测规则中包含有子规则 a 和子规则 b，子规则 a 和子规则 b 均属于数值类规则，子规则 a 为结算金额低于 30，无法使用优惠券 a，子规则 b 为结算金额超过 200，无法使用优惠券 a，子规则 a 和子规则 b 之间的组合方式为“且”的方式，那么，服务器预测出的实际命中的流量中包含的可以使用优惠券 a 的结算金额的数值范围为 30~200。

35 对于上述枚举类规则来说，服务器可以根据待检测规则中包含的若干子规则以及各子

规则之间的组合方式，来确定第一集合以及第二集合。

其中，第一集合中包含有服务器预测出的待检测规则应该命中的历史流量数据中所包含的字段值，而第二集合中包含有服务器预测出的待检测规则不能命中的历史流量数据所包含的字段值。

- 5 例如，假设待检测规则中包含有子规则 c 和子规则 d，子规则 c 和子规则 d 均属于枚举类规则，子规则 c 为在商家 A、商家 B 或商家 C 消费可以使用优惠券 V，子规则 d 为在商家 A 或是商家 D 消费可以使用优惠券 V，子规则 c 和子规则 d 之间的组合方式为“或”的方式，而除了商家 A、商家 B、商家 C 和商家 D 外，还有商家 E 和商家 F，那么，基于子规则 c 和子规则 d 的组合方式，服务器预测出的待检测规则应该命中的历史流量数据中所包含的字段值为商家 A、商家 B、商家 C 和商家 D，这四个商家的字段值即构成了第一集合。而服务器预测出的待检测规则不能命中的历史流量数据中所包含的字段值则为商家 E 和商家 F，这两个商家的字段值即构成第二集合。
- 10

服务器后续可以基于上述的第一集合、第二集合或是数值范围，来对待检测规则进行检测，这一具体内容将在后续的步骤 S103 进行详细介绍。

- 15 在本说明书实施例中，服务器还需要从预设的数据库中查询出待检测规则实际所命中的历史流量数据，其中，该数据库中可以保存有历史上全量的流量数据，而服务器可以提取出待检测规则中各子规则所包含的字段值以及各子规则之间的组合方式，然后，根据这些字段值以及组合方式，来构建出查询脚本，如 SQL 查询脚本。服务器可以通过构建出的查询脚本，从数据库中查询出待检测规则实际所命中的历史流量数据。

- 20 S103：根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测。

在实际应用中，多个工作人员可能负责同一业务的营销规则配置，而由于配置的营销规则过多，或是工作人员配置的营销规则彼此之间并不会相互通知，则可能会导致配置的营销规则难免出现错配的情况。

- 25 例如，假设一个营销规则中包含有子规则 i 和子规则 j 两个枚举类规则，子规则 i 为在商家 A、商家 B 或商家 C 中消费可以使用优惠券 H，子规则 j 为在商家 A 或是商家 D 中消费不能使用优惠券 H，子规则 i 和子规则 j 之间的组合方式为“或”的方式。那么待检测规则实际命中的历史流量数据中应该包含商家 A、商家 B 和商家 C 的流量。但是可以明显的看出，实际命中的商家 A 的历史流量数据显然是与子规则 j 相冲突的，这种情况即属于明显的错配情况。
- 30

而为了能够有效地检测出上述错配情况，服务器可以基于在步骤 S102 中实际命中的历史流量数据以及预测出的待检测规则应该命中的流量，对待检测规则进行检测。

- 具体的，若是待检测规则中包含有枚举类的子规则时，则可以通过上述确定出的第一集合和/或第二集合，来对待检测规则进行检测。其中，若是确定待检测规则实际命中的历史流量数据中包含的字段值在第一集合中均有命中，可以确定待检测规则没有出现异常；
- 35

或是，若确定待检测规则实际命中的历史流量数据中包含的字段值在第二集合中有所命中，可以确定待检测规则存在异常；或是，若确定待检测规则实际命中的历史流量数据中包含的字段值在第一集合中有部分命中，但是在第二集合中均未命中，则可以确定待检测规则未出现异常。其他情况在此就不一一举例说明了。

5 若是待检测规则中包含有数值类的子规则，则服务器可以通过上述确定的数值范围，来对待检测规则进行检测。即，服务器可以统计出实际命中的历史流量数据中包含的字段值，并判断这些字段值在该数据范围内的落入情况，若是确定大部分或是全部字段值均落入到该数值范围内，则可以确定待检测规则未出现异常，若是确定有部分或是全部字段值均未落入到该数值范围内，则可以确定待检测规则出现异常。

10 在本说明书实施例中，服务器可以将待检测规则实际命中的历史流量数据以及基于预测出的待检测规则应命中的流量所确定出的参考数据输入到预设的检测模型中，以通过预设的检测模型来完成待检测规则的检测。

其中，这里提到的参考数据可以是指上述提到的第一集合、第二集合、待检测规则所应命中的历史流量数据中包含的字段值的数值范围等数据。

15 检测模型可以将参数数据以及待检测规则实际命中的历史流量数据进行结合，来确定出待检测规则是否存在异常。

而由于在实际应用中，待检测规则所出现的异常可以分为多种情况，所以，在本说明书实施例中，可以设置多个检测模型，不同的检测模型可以按照不同的检测策略对待检测规则进行检测。

20 其中，实际设置的多个检测模块可以包括全流量跌零告警模型、部分跌零告警模型、名单失效告警模型、流量异常放大或缩小告警模型、业务线自定义告警模型。

全流量跌零告警模型主要用于判断待检测规则是否没有命中任何的历史流量数据；

部分流量跌零告警模型主要用于判断待检测规则实际命中的历史流量数据中是否只涉及待检测规则所涉及的部分字段值，例如，假设待检测规则中包含有子规则 A 和子规则 B，
25 子规则 A 为商家 A 或商家 B 可以使用优惠券，子规则 B 为商家 C 或商家 G 可以使用优惠券，这两个子规则的组合方式为“或”的关系。那么，正常情况下，待检测规则应该命中的历史流量数据应该包含有商家 A、商家 B、商家 C、商家 G 的历史流量数据，但是待检测规则实际命中的历史流量数据中仅包含有商家 A、商家 B 和商家 C 的历史流量数据，并没有商家 G 的历史流量数据，那么，这种情况则属于部分跌零情况。

30 名单失效告警模型主要用于判断实际命中的历史流量数据中包含的字段值在上述第一集合以及第二集合中的命中情况，并根据命中情况，来确定待检测规则是否出现名单失效的情况，例如，若是实际命中的历史流量数据中包含的字段值在上述第二集合中有所命中，则可以确定待检测规则出现名单失效的情况。

流量异常放大或缩小告警模型主要用于判断出待检测规则实际命中的历史流量数据的
35 数量是否过多或是过低。

而业务线自定义告警模型则主要用于根据待检测规则所归属的业务线的实际需求而设定的检测策略对待检测规则进行检测。待检测规则所属的业务线可以理解为部署待检测规则的业务线。

5 所以，服务器可以将待检测规则实际命中的历史流量数据以及上述参考数据输入到各个检测模型中，每个检测模型按照各自采用的检测策略，分别对待检测规则进行检测，以确定出待检测规则是否出现不同类型的异常情况。

在本说明书实施例中，服务器向不同的检测模型输入的数据可以是不同的，例如，对于全流量跌零告警模型来说，服务器可以将待检测规则以及待检测规则实际命中的历史流量数据输入到全流量跌零告警模型中，从而确定待检测规则是否出现全流量跌零的情况；
10 再例如，对于名单失效告警模型来说，服务器可以将待检测规则、待检测规则实际命中的历史流量数据、上述第一集合、第二集合以及数值范围输入到名单失效告警模型中，从而确定出待检测规则中的各子规则是否存在组合方式错误的情况。

在通过上述方式确定出待检测规则的检测结果后，服务器可以进一步的将检测结果输入到预设的告警模型中，以通过告警模型输出的告警结果进行告警。

15 其中，告警模型的主要用途在于对于待检测规则出现的异常情况是否需要向工作人员所使用的终端设备发送告警信息，以提示工作人员及时对待检测规则进行修复。

换句话说，待检测规则所出现的异常情况并不是都需要对工作人员进行告警，有些异常情况基于业务的实际应用需求，可以不进行告警。

所以，上述告警模型实际上起到了降噪的作用，即在一定程度上降低了对工作人员过多打扰。而在具体实施过程中，可以设置多个告警模型，不同的告警模型可以对应不同的业务，每个告警模型都是按照各自的业务的实际需求来设置不同的告警规则。
20

例如，假设从数据库中查询出待检测规则实际命中的历史流量数据的过程中，设置为需要获取夜间 11 点~凌晨 3 点的历史流量数据，那么，实际命中的历史流量数据的数量可能过低，但是，由于这一时段本身所产生的流量的数量往往较低，所以，这种情况可以不
25 算是出现实际命中的流量数出现过低的异常情况，进而也无需进行告警。

再例如，假设对于促销节的业务来说，为该业务配置的待检测规则实际命中的历史流量数据的数量可能过于庞大，但是由于促销节期间本身就会产生过多的流量，所以，这种情况可以不算是实际命中的流量数出现过大的异常情况，进而也无需进行告警。

因此，服务器可以先确定出待检测规则所属的业务，作为目标业务，然后，从而上述
30 这些告警模型中确定出目标业务所对应的告警模型，进而将待检测规则的检测结果输入到该告警模型中，从而确定出是否需要向工作人员发出针对待检测规则的告警信息。

在本说明书实施例中，告警模型中可以基于业务的实际需求，设置不同的膨胀系数或是缩放系数，所谓的膨胀系数或是缩放系数主要是用于划分出预警范围，如果基于待检测规则的检测结果确定出位于预警范围内，则需要向工作人员发送告警信息，如果确定出未
35 处于该预警范围，则可以不向工作人员发送告警信息。

例如，对于待检测规则实际命中的历史流量数据的数量是否过大或是过小的情况来说，假设经过膨胀系数或是缩放系数后所确定出的预警范围为小于 8000 或大于 12000 条的历史流量数据，那么，如果待检测规则实际命中的历史流量数据的数量为 9000 条，则可以确定待检测规则实际命中的历史流量数据未落入到该预警范围内，进而可以确定不向工作人员发送告警信息。

在本说明书实施例中，可以根据业务的实际需求，设置一个基本的预警范围，然后，再通过上述膨胀系数或是缩放系数，对基本的预警范围进行膨胀或是缩放，从而确定出实际使用的预警范围。

例如，假设基于业务 A 的实际需求确定出基本的预警范围为 0~10000 条，而基于业务 A 的实际需求所确定出的膨胀系数为 1.2，那么，确定出最终实际使用的预警范围为 0~12000 条。所以，当业务 A 的待检测规则实际命中的历史流量数据的数量落入在该预警范围内时，则确定待检测规则实际命中的历史流量数据过低。

对于任意一个告警模型来说，都可以按照自身所采用的告警策略输出告警结果，而服务器可以将这些告警模型输出的告警结果进行聚合，并基于聚合结果进行告警。其中，若是任意一个告警模型输出需要进行告警的告警结果，则可以向工作人员所使用的终端设备发送告警信息。当然，对于待检测规则所出现的不同类型的异常情况，也可以向不同的工作人员所使用的终端设备发送告警信息。例如，如果确定待检测规则出现实际命中的历史流量数据过多或是过低的情况，则可以向专门处理此类异常情况的工作人员发送告警信息，如果确定待检测规则出现实际命中的历史流量数据全部跌零的情况，则可以向专门处理此类异常情况的工作人员发送告警信息。

从上述的方法可以看出，在获取到待检测规则后，可以先通过历史流量数据，确定出待检测规则实际所能命中的历史流量数据，然后，通过待检测规则中所包含的各子规则之间的组合方式以及待检测规则实际所能命中的历史流量数据，来检测待检测规则是否存在错配的情况。通过这种方式，不仅可以极大的提高检测效率，降低规则检测的时间成本，并且，可以有效的提高规则检测的准确性。

除此之外，通过设置用于降噪的告警模型，可以对不必要的告警信息进行过滤，从而可以降低对工作人员的不必要打扰。

另外，本说明书实施例提供的规则检测方法除了可以对常规的线上业务的营销规则进行检测外，还可以对涉及跨境支付或是跨境结算的业务所使用的营销规则进行检测。例如，对于跨境结算业务来说，其配置的营销规则中可以会规定所使用的利率，税率等，所以，服务器可以通过上述方法，来检测待检测规则中所配置的利率、税率等信息进行检测，以判断出待检测规则配置的是否合理。

为了更清楚的解释本说明书提供的规则检测方法，这里使用一个详细的例子进行说明，如图 2 所示。

图 2 为本说明书实施例提供的一种规则检测的详细流程图。

从图 2 中可以看出, 首先, 服务器通过监听器, 监听到的营销规则表的变更情况, 当营销规则出现新增或是修改后, 基于营销规则对应的规则标识发送变更消息, 以获取待检测规则。服务器根据获取到的待检测规则的子规则以及子规则之间的组合方式, 确定出第一集合以及第二集合, 与此同时, 根据待检测规则中各子规则所包含的字段值以及各子规则之间的组合方式, 构建查询脚本, 以通过构建出的查询脚本, 从数据库中查询出待检测规则实际所命中的历史流量数据。

然后, 将待检测规则实际命中的历史流量数据以及基于预测出的待检测规则应命中的流量所确定出的参考数据输入到预设的检测模型中, 也就是说, 服务器将待检测规则实际命中的历史流量数据、第一集合、第二集合、待检测规则所应命中的历史流量数据中包含的字段值的数值范围等输入到预设的检测模型中, 这里的检测模型可以是全流量跌零告警模型、部分跌零告警模型、名单失效告警模型、流量异常放大或缩小告警模型、业务线自定义告警模型。服务器将检测模型输出的针对待检测规则的检测结果进一步输入到告警模型中, 以对检测结果进行降噪, 随后将所有针对待检测规则的告警信息进行聚合, 判断是否需要进行告警, 如果是, 向对应的工作人员推送告警信息。

例如, 假设待检测规则中包含有子规则 A、子规则 B、子规则 C, 子规则 A 为商家 A 或商家 B 可以使用优惠券, 子规则 B 为商家 B 不可以使用优惠券, 子规则 C 为支付金额大于 50 才可以使用优惠券, 若按照子规则 A、子规则 B、子规则 C 的顺序对子规则进行组合, 子规则 A 与子规则 B 的组合方式为“或”的关系, 子规则 B 与子规则 C 的组合方式为“且”的关系, 此时, 根据待检测规则中子规则 A、子规则 B、子规则 C 以及各子规则之间的组合方式, 可以确定第一集合中包含的字段值为商家 A、商家 B, 第二集合中包含的字段值为商家 B。进一步地, 服务器从数据库中查询出的待检测规则实际命中的历史流量数据中包含商家 A、商家 B 的历史流量数据, 并且待检测规则实际命中的历史流量数据中的支付金额的数值范围为 50~150。在此基础上, 服务器将待检测规则实际命中的历史流量数据、第一集合、第二集合、待检测规则所应命中的历史流量数据中包含的字段值的数值范围等输入到预设的检测模型中。可以看出, 待检测规则实际命中的历史流量数据中的支付金额的数值范围为 50~150, 符合待检测规则所应命中的历史流量数据中包含的字段值的数值范围, 而待检测规则实际命中的历史流量数据中包括商家 B 的历史流量数据, 但在正常情况下, 第二集合中的商家 B 不应出现在待检测规则实际命中的历史流量数据中, 说明待检测规则存在异常。然后, 服务器将待检测规则存在异常的检测结果输入到告警模型进行降噪后, 得到针对待检测规则的告警信息, 进一步地, 服务器将针对待检测规则的告警信息发送给工作人员, 以使工作人员及时根据告警信息对待检测规则进行修正。

The specification also provides a computer-readable non-transitory storage medium, wherein the storage medium stores a computer program, which, when executed by a processor, can be used to perform one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Herein, the computer-readable non-transitory storage medium or media may include one or more semiconductor-based or other integrated circuits (ICs)

(such, as for example, field-programmable gate arrays (FPGAs) or application-specific ICs (ASICs)), hard disk drives (HDDs), hybrid hard drives (HHDs), optical discs, optical disc drives (ODDs), magneto-optical discs, magneto-optical drives, floppy diskettes, floppy disk drives (FDDs), magnetic tapes, solid-state drives (SSDs), RAM-drives, SECURE DIGITAL cards or drives, any other suitable computer-readable non-transitory storage media, or any suitable combination of two or more of these, where appropriate. A computer-readable non-transitory storage medium may be volatile, non-volatile, or a combination of volatile and non-volatile, where appropriate.

The specification also provides a computer system. FIG. 3 illustrates an example computer system **300**. In particular embodiments, one or more computer systems **300** perform one or more steps of one or more methods described or illustrated herein. In particular embodiments, one or more computer systems **300** provide functionality described or illustrated herein. In particular embodiments, software running on one or more computer systems **300** performs one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Particular embodiments include one or more portions of one or more computer systems **300**. Herein, reference to a computer system may encompass a computing device, and vice versa, where appropriate. Moreover, reference to a computer system may encompass one or more computer systems, where appropriate.

This disclosure contemplates any suitable number of computer systems **300**. This disclosure contemplates computer system **300** taking any suitable physical form. As example and not by way of limitation, computer system **300** may be an embedded computer system, a system-on-chip (SOC), a single-board computer system (SBC) (such as, for example, a computer-on-module (COM) or system-on-module (SOM)), a desktop computer system, a laptop or notebook computer system, an interactive kiosk, a mainframe, a mesh of computer systems, a mobile telephone, a personal digital assistant (PDA), a server, a tablet computer system, or a combination of two or more of these. Where appropriate, computer system **300** may include one or more computer systems **300**; be unitary or distributed; span multiple locations; span multiple machines; span multiple data centers; or reside in a cloud, which may include one or more cloud components in one or more networks. Where appropriate, one or more computer systems **300** may perform without substantial spatial or temporal limitation one or more steps of one or more methods described or illustrated herein. As an example and not by way of limitation, one or more computer systems **300** may perform in real time or in batch mode one or more steps of one or more methods described or illustrated herein. One or more computer systems **300** may perform at different times or at different locations one or more steps of one or more methods described or illustrated herein, where appropriate.

In particular embodiments, computer system **300** includes a processor **302**, memory **304**, storage **306**, an input/output (I/O) interface **308**, a communication interface **310**, and a bus **312**. Altho

ugh this disclosure describes and illustrates a particular computer system having a particular number of particular components in a particular arrangement, this disclosure contemplates any suitable computer system having any suitable number of any suitable components in any suitable arrangement.

5 In particular embodiments, processor **302** includes hardware for executing instructions, such as those making up a computer program. As an example and not by way of limitation, to execute instructions, processor **302** may retrieve (or fetch) the instructions from an internal register, an internal cache, memory **304**, or storage **306**; decode and execute them; and then write one or more results to an internal register, an internal cache, memory **304**, or storage **306**. In particular embodiments, processor **302** may include one or more internal caches for data, instructions, or addresses. This disclosure contemplates processor **302** including any suitable number of any suitable internal caches, where appropriate. As an example and not by way of limitation, processor **302** may include one or more instruction caches, one or more data caches, and one or more translation lookaside buffers (TLBs). Instructions in the instruction caches may be copies of instructions in memory **304** or storage **306**, and the instruction caches may speed up retrieval of those instructions by processor **302**. Data in the data caches may be copies of data of **80** in memory **304** or storage **306** for instructions executing at processor **302** to operate on; the results of previous instructions executed at processor **302** for access by subsequent instructions executing at processor **302** or for writing to memory **304** or storage **306**; or other suitable data. The data caches may speed up read or write operations by processor **302**. The TLBs may speed up virtual-address translation for processor **302**. In particular embodiments, processor **302** may include one or more internal registers for data, instructions, or addresses. This disclosure contemplates processor **302** including any suitable number of any suitable internal registers, where appropriate. Where appropriate, processor **302** may include one or more arithmetic logic units (ALUs); be a multi-core processor; or include one or more processors **302**. Although this disclosure describes and illustrates a particular processor, this disclosure contemplates any suitable processor.

In particular embodiments, memory **304** includes main memory for storing instructions for processor **302** to execute or data for processor **302** to operate on. As an example and not by way of limitation, computer system **300** may load instructions from storage **306** or another source (such as, for example, another computer system **300**) to memory **304**. Processor **302** may then load the instructions from memory **304** to an internal register or internal cache. To execute the instructions, processor **302** may retrieve the instructions from the internal register or internal cache and decode them. During or after execution of the instructions, processor **302** may write one or more results (which may be intermediate or final results) to the internal register or internal cache. Processor **302** may then write one or more of those results to memory **304**. In particular embodiments, processor

302 executes only instructions in one or more internal registers or internal caches or in memory **304** (as opposed to storage **306** or elsewhere) and operates only on data in one or more internal registers or internal caches or in memory **304** (as opposed to storage **306** or elsewhere). One or more memory buses (which may each include an address bus and a data bus) may couple processor **302** to memory **304**. Bus **312** may include one or more memory buses, as described below. In particular embodiments, one or more memory management units (MMUs) reside between processor **302** and memory **304** and facilitate accesses to memory **304** requested by processor **302**. In particular embodiments, memory **304** includes random access memory (RAM). This RAM may be volatile memory, where appropriate. Where appropriate, this RAM may be dynamic RAM (DRAM) or static RAM (SRAM). Moreover, where appropriate, this RAM may be single-ported or multi-ported RAM. This disclosure contemplates any suitable RAM. Memory **304** may include one or more memories **304**, where appropriate. Although this disclosure describes and illustrates particular memory, this disclosure contemplates any suitable memory.

In particular embodiments, storage **306** includes mass storage for data or instructions. As an example and not by way of limitation, storage **306** may include a hard disk drive (HDD), a floppy disk drive, flash memory, an optical disc, a magneto-optical disc, magnetic tape, or a Universal Serial Bus (USB) drive or a combination of two or more of these. Storage **306** may include removable or non-removable (or fixed) media, where appropriate. Storage **306** may be internal or external to computer system **300**, where appropriate. In particular embodiments, storage **306** is non-volatile, solid-state memory. In particular embodiments, storage **306** includes read-only memory (ROM). Where appropriate, this ROM may be mask-programmed ROM, programmable ROM (PROM), erasable PROM (EPROM), electrically erasable PROM (EEPROM), electrically alterable ROM (EAROM), or flash memory or a combination of two or more of these. This disclosure contemplates mass storage **306** taking any suitable physical form. Storage **306** may include one or more storage control units facilitating communication between processor **302** and storage **306**, where appropriate. Where appropriate, storage **306** may include one or more storages **306**. Although this disclosure describes and illustrates particular storage, this disclosure contemplates any suitable storage.

In particular embodiments, I/O interface **308** includes hardware, software, or both, providing one or more interfaces for communication between computer system **300** and one or more I/O devices. Computer system **300** may include one or more of these I/O devices, where appropriate. One or more of these I/O devices may enable communication between a person and computer system **300**. As an example and not by way of limitation, an I/O device may include a keyboard, keypad, microphone, monitor, mouse, printer, scanner, speaker, still camera, stylus, tablet, touch screen, trackball, video camera, another suitable I/O device or a combination of two or more of these. An I/

O device may include one or more sensors. This disclosure contemplates any suitable I/O devices and any suitable I/O interfaces **308** for them. Where appropriate, I/O interface **308** may include one or more device or software drivers enabling processor **302** to drive one or more of these I/O devices. I/O interface **308** may include one or more I/O interfaces **308**, where appropriate. Although this disclosure describes and illustrates a particular I/O interface, this disclosure contemplates any suitable I/O interface.

In particular embodiments, communication interface **310** includes hardware, software, or both providing one or more interfaces for communication (such as, for example, packet-based communication) between computer system **300** and one or more other computer systems **300** or one or more networks. As an example and not by way of limitation, communication interface **310** may include a network interface controller (NIC) or network adapter for communicating with an Ethernet or other wire-based network or a wireless NIC (WNIC) or wireless adapter for communicating with a wireless network, such as a WI-FI network. This disclosure contemplates any suitable network and any suitable communication interface **310** for it. As an example and not by way of limitation, computer system **300** may communicate with an ad hoc network, a personal area network (PAN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), or one or more portions of the Internet or a combination of two or more of these. One or more portions of one or more of these networks may be wired or wireless. As an example, computer system **300** may communicate with a wireless PAN (WPAN) (such as, for example, a BLUETOOTH WPAN), a WI-FI network, a WI-MAX network, a cellular telephone network (such as, for example, a Global System for Mobile Communications (GSM) network), or other suitable wireless network or a combination of two or more of these. Computer system **300** may include any suitable communication interface **310** for any of these networks, where appropriate. Communication interface **310** may include one or more communication interfaces **310**, where appropriate. Although this disclosure describes and illustrates a particular communication interface, this disclosure contemplates any suitable communication interface.

In particular embodiments, bus **312** includes hardware, software, or both coupling components of computer system **300** to each other. As an example and not by way of limitation, bus **312** may include an Accelerated Graphics Port (AGP) or other graphics bus, an Enhanced Industry Standard Architecture (EISA) bus, a front-side bus (FSB), a HYPERTRANSPORT (HT) interconnect, an Industry Standard Architecture (ISA) bus, an INFINIBAND interconnect, a low-pin-count (LPC) bus, a memory bus, a Micro Channel Architecture (MCA) bus, a Peripheral Component Interconnect (PCI) bus, a PCI-Express (PCIe) bus, a serial advanced technology attachment (SATA) bus, a Video Electronics Standards Association local (VLB) bus, or another suitable bus or a combination of two or more of these. Bus **312** may include one or more buses **312**, where appropriate. Although

gh this disclosure describes and illustrates a particular bus, this disclosure contemplates any suitable bus or interconnect.

还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。5 在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施10 例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

权 利 要 求 书

1、一种规则检测方法，包括：

获取待检测规则，所述待检测规则中记录有若干子规则以及各子规则之间的组合方式；

根据所述若干子规则以及所述组合方式，预测所述待检测规则应命中的流量，并从预

5 设的历史流量数据中查询出所述待检测规则实际命中的历史流量数据；

根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测。

2、如权利要求 1 所述的方法，从预设的历史流量数据中查询出所述待检测规则实际命中的历史流量数据，具体包括：

10 根据所述组合方式，构建查询脚本；

通过所述查询脚本，从预设的历史流量数据中查询出所述待检测规则实际命中的历史流量数据。

3、如权利要求 1 所述的方法，子规则包括枚举类规则；

15 根据所述若干子规则以及所述组合方式，预测所述待检测规则应命中的流量，具体包括：

根据所述若干子规则以及所述组合方式，确定第一集合以及第二集合，所述第一集合中包含有预测出的所述待检测规则所应命中的历史流量数据所包含的字段值，第二集合中包含有预测出的所述待检测规则不能命中的历史流量数据所包含的字段值；

20 根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测，具体包括：

根据所述待检测规则实际命中的历史流量数据中包含的字段值在所述第一集合中的命中情况和/或所述待检测规则实际命中的历史流量数据中包含的字段值在所述第二集合中的命中情况，以对所述待检测规则进行检测。

4、如权利要求 1 所述的方法，子规则包括数值类规则；

25 根据所述若干子规则以及所述组合方式，预测所述待检测规则应命中的流量，具体包括：

根据所述若干子规则以及所述组合方式，预测出所述待检测规则所应命中的历史流量数据中包含的字段值的数值范围；

30 根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测，具体包括：

根据所述数值范围以及所述待检测规则实际命中的历史流量数据，对所述待检测规则进行检测。

5、如权利要求 1 所述的方法，根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测，具体包括：

35 将所述待检测规则实际命中的历史流量数据以及基于预测出的所述待检测规则应命中

的流量所确定出的参考数据输入到预设的检测模型中，以通过所述检测模型输出的检测结果，对所述待检测规则进行检测。

- 6、如权利要求 5 所述的方法，将所述待检测规则实际命中的历史流量数据以及基于预测出的所述待检测规则应命中的流量所确定出的参考数据输入到预设的检测模型中，以通过所述检测模型输出的检测结果，对所述待检测规则进行检测，具体包括：

将所述待检测规则实际命中的历史流量数据以及基于预测出的所述待检测规则应命中的流量所确定出的参考数据输入到预设的各检测模型中，以通过每个检测模型输出的检测结果，对所述待检测规则进行检测，其中，不同的检测模型按照不同的检测策略对所述待检测模型进行检测。

- 10 7、如权利要求 1 所述的方法，所述方法还包括：

将针对所述待检测规则的检测结果输入到预设的告警模型，以通过所述告警模型输出的告警结果进行告警。

8、如权利要求 7 所述的方法，将针对所述待检测规则的检测结果输入到预设的告警模型，以通过所述告警模型输出的告警结果进行告警，具体包括：

- 15 确定所述待检测规则所属的业务，作为目标业务；

将针对所述待检测规则的检测结果输入到所述目标业务所对应的告警模型中，以通过所述目标业务所对应的告警模型输出的告警结果进行告警。

9、一种计算机系统，所述计算机系统包括存储器、处理器及存储在所述存储器上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程序时实现如下步骤：

- 20 获取待检测规则，所述待检测规则中记录有若干子规则以及各子规则之间的组合方式；

根据所述若干子规则以及所述组合方式，预测所述待检测规则应命中的流量，并从预设的历史流量数据中查询出所述待检测规则实际命中的历史流量数据；

根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测。

- 25 10、如权利要求 9 所述的计算机系统，从预设的历史流量数据中查询出所述待检测规则实际命中的历史流量数据，具体包括：

根据所述组合方式，构建查询脚本；

通过所述查询脚本，从预设的历史流量数据中查询出所述待检测规则实际命中的历史流量数据。

- 30 11、如权利要求 9 所述的计算机系统，子规则包括枚举类规则；

根据所述若干子规则以及所述组合方式，预测所述待检测规则应命中的流量，具体包括：

根据所述若干子规则以及所述组合方式，确定第一集合以及第二集合，所述第一集合中包含有预测出的所述待检测规则所应命中的历史流量数据所包含的字段值，第二集合中包含有预测出的所述待检测规则不能命中的历史流量数据所包含的字段值；

根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测，具体包括：

根据所述待检测规则实际命中的历史流量数据中包含的字段值在所述第一集合中的命中情况和/或所述待检测规则实际命中的历史流量数据中包含的字段值在所述第二集合中的命中情况，以对所述待检测规则进行检测。

12、如权利要求 9 所述的计算机系统，子规则包括数值类规则；

根据所述若干子规则以及所述组合方式，预测所述待检测规则应命中的流量，具体包括：

根据所述若干子规则以及所述组合方式，预测出所述待检测规则所应命中的历史流量数据中包含的字段值的数值范围；

根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测，具体包括：

根据所述数值范围以及所述待检测规则实际命中的历史流量数据，对所述待检测规则进行检测。

13、如权利要求 9 所述的计算机系统，根据所述待检测规则实际命中的历史流量数据以及预测出的所述待检测规则应命中的流量，对所述待检测规则进行检测，具体包括：

将所述待检测规则实际命中的历史流量数据以及基于预测出的所述待检测规则应命中的流量所确定出的参考数据输入到预设的检测模型中，以通过所述检测模型输出的检测结果，对所述待检测规则进行检测。

14、如权利要求 13 所述的计算机系统，将所述待检测规则实际命中的历史流量数据以及基于预测出的所述待检测规则应命中的流量所确定出的参考数据输入到预设的检测模型中，以通过所述检测模型输出的检测结果，对所述待检测规则进行检测，具体包括：

将所述待检测规则实际命中的历史流量数据以及基于预测出的所述待检测规则应命中的流量所确定出的参考数据输入到预设的各检测模型中，以通过每个检测模型输出的检测结果，对所述待检测规则进行检测，其中，不同的检测模型按照不同的检测策略对所述待检测模型进行检测。

15、如权利要求 9 所述的计算机系统，所述计算机系统还用于，将针对所述待检测规则的检测结果输入到预设的告警模型，以通过所述告警模型输出的告警结果进行告警。

16、如权利要求 15 所述的计算机系统，将针对所述待检测规则的检测结果输入到预设的告警模型，以通过所述告警模型输出的告警结果进行告警，具体包括：

确定所述待检测规则所属的业务，作为目标业务；

将针对所述待检测规则的检测结果输入到所述目标业务所对应的告警模型中，以通过所述目标业务所对应的告警模型输出的告警结果进行告警。

17、一种计算机可读存储介质，所述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权利要求 1~8 任一项所述的方法。