

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06F 12/14 (2006.01)

G06F 12/16 (2006.01)



[12] 发明专利说明书

专利号 ZL 03131061.3

[45] 授权公告日 2007 年 3 月 14 日

[11] 授权公告号 CN 1304963C

[22] 申请日 2003.5.15 [21] 申请号 03131061.3

[73] 专利权人 联想网御科技（北京）有限公司

地址 100086 北京市海淀区中关村南大街
6 号中电信大厦 801 - 810 室

[72] 发明人 叶蓬 顾正华 贾炜

[56] 参考文献

US2002/0144150A1 2002.10.3

US6058426A 2000.5.2

JP2001-358716A 2001.12.26

审查员 尹春梅

[74] 专利代理机构 北京集佳知识产权代理有限公司

代理人 王学强

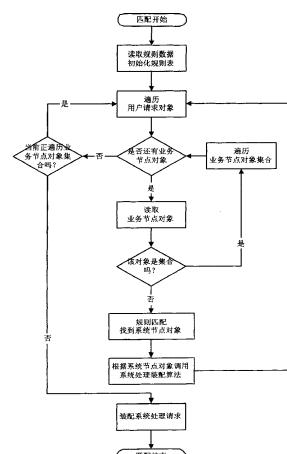
权利要求书 2 页 说明书 9 页 附图 3 页

[54] 发明名称

安全信息处理请求转换系统

[57] 摘要

本发明公开了一种安全信息处理请求转换系统，采用了一种规则驱动的工作模式，由用户处理请求转换模块将 XML 格式的用户处理请求转换为用户请求对象发送到规则匹配模块，再由规则匹配模块根据用户请求对象中的业务节点对象匹配的系统节点对象调用装配算法进行规则装配，形成系统处理请求对安全信息进行处理。它还可以方便地对新的安全设备或应用的安全信息处理提供支持，具有很强的扩展性；在对新设备或应用的安全信息进行处理前，将该设备或应用的安全信息处理规则通过规则编辑模块定制为规则数据存储在存储设备中，进行处理时，就可以很方便地将对于新设备或应用的安全信息处理的用户处理请求转换为系统处理请求。



1、一种安全信息处理请求转换系统，其特征在于：该系统至少设有用户处理请求转换模块、规则匹配模块和结果转发模块；

用户处理请求转换模块，用于将外部输入的用户处理请求转换为用户请求对象输出，并将结果转发模块发来的处理结果对象转换为用户结果信息；规则匹配模块，用于根据用户请求对象读取规则数据表中相应的规则数据，调用装配算法模块中的装配算法，将用户请求对象转换为系统处理请求，利用转换完成后的系统处理请求对存储在数据库中的安全信息数据进行处理，处理后的结果经由数据库发送到结果转发模块中；结果转发模块用于接收规则匹配模块经由数据库发送来的安全信息数据处理后的结果，并将其转换为处理结果对象，再发送到用户处理请求转换模块或将处理结果对象直接输出。

2、根据权利要求1所述的安全信息处理请求转换系统，其特征在于：系统中设有规则编辑模块，用于编辑用户请求对象转换为系统处理请求所依据的所述规则数据，以使该系统对于新的或更改后的安全设备或应用产生的安全信息进行处理。

3、根据权利要求1或2所述的安全信息处理请求转换系统，其特征在于：所述的系统还进一步设有装配算法模块，用于存储规则匹配用到的装配算法。

4、根据权利要求1或2所述的安全信息处理请求转换系统，其特征在于：该系统设有方案保存/加载模块，用于将用户请求对象保存为方案数据；使用时根据需要加载或修改保存的方案数据。

5、根据权利要求1或2所述的安全信息处理请求转换系统，其特征在于：所述规则数据以文件或数据库表的形式存储在存储设备中。

6、根据权利要求4所述的安全信息处理请求转换系统，其特征在于：所

述方案数据以文件或数据库表的形式存储在存储设备中。

7、根据权利要求 1 所述的安全信息处理请求转换系统，其特征在于：所述的用户处理请求或用户结果信息为 XML 格式文件或文本文件或数据库表。

安全信息处理请求转换系统

技术领域

本发明涉及一种信息处理请求转换系统，特别涉及一种对计算机安全设备或应用产生的安全信息进行处理请求转换的系统，属于信息安全技术领域。

背景技术

随着人们对网络安全的逐渐重视，在网络中部署了大量诸如防火墙、入侵监测系统等安全设备和具备安全防护功能的应用（关键应用）。所有这些安全设备、关键应用以及支撑这些关键应用的主机系统都会产生大量的安全信息（事件），而提供对这些安全信息的处理成为网络真正安全可控的重要因素。一个良好的安全信息处理系统应该能够如实、准确地反映网络的工作状况。

目前，对安全信息进行处理时面临的一个比较大的难题是：安全信息内容复杂，不同种类的安全信息间的差异太大。由于每种安全设备所关注的领域不同，网络中部署的具备安全防护功能的应用类型的不同和数量的差异，因此，产生了各种格式的安全信息；即使是同种安全设备，其产生的安全信息在格式和数量上也存在很大差异。因此，一个既有的安全信息处理系统很难在网络中加入新的设备和应用后能够方便地对其进行支持。正是由于上述原因，使得如何对复杂的安全信息进行处理成为现在研究的一个热点。如果单纯使用安全信息格式标准化等手段，虽然能够降低信息处理的复杂度，但却忽略了不同安全信息之间本质的区别。因此一个好的安全信息处理系统应该在维持安全信息某些特性的前提下抽取它们的共性，将各种安全信息格式统一为若干类而不是一类，进而基于这些新构造的安全信息类型进行安全信息处理。这样，在需要扩展支持新的安全设备和关键应用的时候就可以方便

地将新的信息格式映射为已有安全信息格式的一种，而不必为了增加新的安全信息格式而重新修改整个安全信息处理系统。

为了解决复杂安全信息的处理问题，以及实现安全信息处理系统的可扩展性，需要一个安全信息处理请求转换系统。

人们已经在通用的信息处理请求转换系统领域做了很多工作，其中核心的内容就是：使用中间语言将用户处理请求和实际数据处理语言分离开来；目的在于将从用户角度看的处理信息和从系统角度看的处理信息分离开，使得用户有一个人性化和与其业务领域相关的信息处理交互界面，同时保证这种抽象处理能够转换为系统自身认识的处理语言。

但是，这些方法并没有考虑如何有效地支持用户业务领域扩展的问题。以信息安全处理为例：如果用户开始时的业务领域是对某10种安全信息进行处理，经过一段时间，需要对新的10种安全信息进行处理，原有的信息处理请求转换系统如果不进行必要的改动就不能很好的支持。因为这些信息处理请求转换系统针对的是一个通用的用户域，不论它是信息安全领域的处理还是工业领域的处理，不论增加什么新的信息它都按照原有的方式工作。事实上，这个例子中新增加的信息和原有的信息是有关联的，它们具备了很多安全领域共有的特征。如果我们将信息处理请求转换系统的工作范围限定在信息安全领域，利用从这个领域抽取出来的知识——规则作为信息处理请求转换系统的驱动器，就可以比较好的进行新类型安全信息处理的扩展。

美国专利《数据库处理系统》（专利号：5,812,840）公开的数据库处理系统，包括一个处理助手，使得用户只能输入正确的处理条件，并且这个处理条件使用近似英语的中间语言表述。同时，系统提供一个从中间语言到SQL处理语句的转换，使得用户提交的处理最终变成数据库处理语句并得到处理结果。虽然它也提出了使用一种中间语言作为用户处理请求和数据库处理语言之间的中介，但是它关注的是如何为用户提供最自然易用的处理交互界面，而不是如何适应新类型的数据处理需求。其次，该发明中的中间语言

不仅用于处理生成器的输入，而且用于给用户显示出来，这对于产生中间语言的处理助手的要求是很高的，很难做到对各个领域的普适性。

如果将一个处理系统绑定到某个特定问题域（例如信息安全处理领域），加入该领域特定的知识——规则，同样可以提供一种近似自然语言效果的安全信息处理过程，同时还能保证该系统的可扩展性。

发明内容

本发明的目的是提供一种安全信息处理请求转换系统，采用了一种规则驱动的工作模式，可以将用户处理请求转换为系统处理请求，并可以通过定制规则数据，方便地对新的安全信息的处理请求提供支持。

本发明的目的是通过以下技术方案实现的：

一种安全信息处理请求转换系统，设有用户处理请求转换模块，规则匹配模块和结果转发模块；

用户处理请求转换模块，用于将外部输入的用户处理请求转换为用户请求对象输出，将结果转发模块发来的处理结果对象转换为用户结果信息；规则匹配模块，用于根据用户请求对象读取规则数据表中相应的规则数据，调用装配算法模块中的装配算法，将用户请求对象转换为系统处理请求，利用转换完成后的系统处理请求对存储在数据库中的安全信息数据进行处理，处理后的结果经由数据库发送到结果转发模块中；结果转发模块，用于接收规则匹配模块经由数据库发送来的安全信息数据处理后的结果，转换为处理结果对象发送到用户处理请求转换模块或将处理结果对象直接输出。

规则匹配模块将用户请求对象转换为系统处理请求至少包括以下步骤：

- 一、读取规则数据；
- 二、遍历用户请求对象；
- 三、判断是否有尚未匹配的业务节点对象，若有则转到步骤五；
- 四、判断当前是否正在遍历业务节点对象集合，若是则转到步骤二，若否则转到步骤十一；
- 五、读取业务节点对象；

-
- 六、判断步骤五读取的业务节点对象是否是集合，若否则转到步骤八；
 - 七、遍历业务节点对象集合，之后转到步骤三；
 - 八、根据匹配关系找到业务节点对象对应的系统节点对象；
 - 九、根据系统节点对象调用装配算法进行规则装配；
 - 十、转到步骤二；
 - 十一、装配系统处理请求。

上述安全信息处理请求转换系统设有规则编辑模块，用于编辑用户请求对象转换为系统处理请求所依据的规则数据，以使该系统对于新的或更改后的安全设备或应用产生的安全信息进行处理。

上述安全信息处理请求转换系统设有装配算法模块，用于存储规则匹配用到的装配算法。

上述安全信息处理请求转换系统设有方案保存 / 加载模块，用于将用户请求对象保存为方案数据；使用时根据需要加载或修改保存的方案数据。

上述安全信息处理请求转换系统中，所述规则数据以文件或数据库表的形式存储在存储设备中；所述方案数据以文件或数据库表的形式存储在存储设备中；用户处理请求或用户结果信息为 XML 格式文件或文本文件或数据库表。

通过上述技术方案可知，本发明具有如下优点：

1、将用户处理请求通过一个中间层转换为系统处理请求，给用户提供了一种近乎自然语言的安全信息处理方法；本发明提供的安全信息处理请求转换系统，采用了一种规则驱动的工作模式，由用户处理请求转换模块将 XML 格式或文本文件格式或数据库表格式的用户处理请求转换为用户请求对象发送到规则匹配模块，再由规则匹配模块根据用户请求对象中的业务节点对象匹配的系统节点对象调用装配算法进行规则装配，形成系统处理请求对安全信息进行处理。

2、具有可扩展性，可以方便地对新的安全设备或应用的安全信息处理

提供支持。在对新设备或应用的安全信息进行处理前，将该设备或应用的安全信息处理规则通过规则编辑模块定制为规则数据存储在存储设备中，进行处理时，就可以很方便地将对于新设备或应用的安全信息处理的用户处理请求转换为系统处理请求。

附图说明

图 1 为本发明实施例中的用户请求对象的一个实例；

图 2 为本发明实施例的系统组成原理图；

图 3 为本发明实施例用户请求对象与系统装配对象匹配关系的一个实例；

图 4 为本发明实施例用户请求对象转为系统处理请求的流程图。

具体实施方式

以下，结合具体实施例并参照附图，对本发明做进一步的详细说明。

本发明主要应用于信息安全领域，主要任务是对各种安全设备或应用产生的安全信息按照用户的要求进行处理，因此本发明的一个重要任务就是实现安全信息处理请求从用户业务域到系统通用域的转换。

用户在进行安全信息处理条件指定时属于用户业务域，而用户的处理请求经过请求转换系统转换后的系统处理请求属于系统通用域，此时的系统处理请求已经通过规则匹配过程消除了用户业务域的特征信息。

本实施例将表示业务规则基本元素和系统处理条件基本元素的数据结构定义为节点对象，描述业务规则组成的基本元素称为业务节点对象，例如源 IP 地址、端口号、流量等，属于用户特定域，特点是随着用户业务领域的变化而时常变动；描述系统处理条件组成的基本单位称为系统节点对象，例如比较、匹配等，属于系统通用域，特点是基本不发生变动，因而可以固化在转换系统之中。所有的业务节点对象都是从初始业务节点对象派生出来

的；初始业务节点对象定义了所有业务节点对象共有的属性，例如节点名称和标识、数据类型、取值等。同样，所有的系统节点对象也都是从初始系统节点对象派生出来的。

每个用户处理请求的条件对应于一个或多个业务节点对象，多个业务节点对象的集合描述了一个用户处理请求的数据结构，称为用户请求对象；如图 1 所示，为用户请求对象的一个实例；而一个或多个系统节点对象的集合则描述了一个系统处理语句的产生规则（算法），称为系统装配对象。用户处理请求在保存和加载的时候也被称作处理方案。需要指出的是，节点对象自身可以由一个或多个节点对象的集合组成，形成一种递归的构造方式。如下表所示，列举了若干系统节点对象及其对应的系统操作说明。

系统节点对象类型	系统操作说明
赋值节点	装配等于逻辑条件，形如：对象名 = 对象值
比较节点	装配比较范围逻辑条件，形如：对象最小值 <= 对象名 <= 对象最大值
匹配节点	装配字符串比较逻辑条件，形如：对象 like % 对象值%
复合节点	由若干个赋值节点、比较节点、匹配节点或其他基本节点通过逻辑与、或复合而成的节点，形如：对象名 = 对象值 1 and 对象名 = 对象值 2 or

由此可以看出，本实施例的安全信息处理请求转换系统利用了节点对象技术，通过规则定义和规则匹配，将业务节点对象转换为系统节点对象，有效地降低了业务变化带来的系统重构成本，实现了系统的快速扩展。

如图 2 所示，为安全信息处理请求转换系统的原理框图。用户处理请求转换模块将用户处理请求转换为用户请求对象输出到规则匹配模块中；规则匹配模块根据用户请求对象读取规则数据表中相应的规则数据，调用系统处理装配模块中的装配算法，将用户请求对象转换为系统处理请求，规则匹配模块利用转换完成后的系统处理请求对存储在数据库中的安全信息数据进

行处理，处理后的结果由数据库发送到结果转发模块中；结果转发模块用于接收规则匹配模块经由数据库发送来的安全信息数据处理后的结果，并将其转换为处理结果对象，再发送到用户处理请求转换模块或将处理结果对象直接输出。

在对用户处理请求转换成系统处理请求之前，需要将处理请求语言转换为处理请求转换系统的规则匹配模块可以识别的数据结构。为了便于传输、实现分层的信息处理架构以及未来的信息标准化，用户处理请求使用 XML 语言表达。用户处理请求的每个条件都对应于一个 XML 标签，所有的条件都有统一的编号加以标识并注明了数据类型，每个条件都有一个属性表示它的取值。用户处理请求转换模块根据用户处理请求中每个条件的标识、数据类型和取值，将 XML 格式的处理请求转化为用户请求对象。这个过程是本实施例所述系统的一个预处理过程。

本系统的核心过程是由规则匹配模块完成的。规则匹配模块在规则数据的驱动下，遍历用户请求对象的每个业务节点对象，调用装配算法(在系统处理装配对象中定义)，产生系统处理语句；如图 3 所示，为用户请求对象与系统处理装配对象匹配关系的一个实例。

如图 4 所示，为用户请求对象转为系统处理请求的流程图，包括如下步骤：

- 一、读取规则数据，初始化规则表；
- 二、遍历用户请求对象；
- 三、判断是否还有等待匹配的业务节点对象，若有则转到步骤五；
- 四、判断当前是否正在遍历业务节点对象集合，若是则转到步骤二，若否则转到步骤十一；
- 五、读取业务节点对象；
- 六、判断步骤五读取的业务节点对象是否是集合，若否则转到步骤八；
- 七、遍历业务节点对象集合，之后转到步骤三；
- 八、根据匹配关系找到业务节点对象对应的系统节点对象；

九、根据系统节点对象调用装配算法进行规则装配；

十、转到步骤二；

十一、装配系统处理请求；

规则匹配模块在遍历用户请求对象的时候，每读入一个业务节点对象就在规则表中寻找其对应的系统节点对象，紧接着调用这个系统节点对象定义的装配算法产生这个处理条件对应的系统处理语句的片断。遍历完毕，这些处理语句片断就可以组合成为一个完整的系统处理请求。

规则数据定义了一套从用户特定域到系统通用域的转换机制，即从用户请求对象中描述的处理请求转换为系统处理语句的机制。规则数据实质上是一张由若干条规则组成的规则表：每一条规则定义了一个业务节点对象所对应的系统节点对象。

规则数据是可以被修改的。这就是说，用户可以通过修改现有的业务节点对象到系统节点对象的对应关系来修改现有的业务流程，也可以通过定义新的业务节点对象以及它和系统节点对象的关系来扩展现有的业务；规则编辑模块用于定制、修改规则数据。

当系统用于一种新的数据处理业务时，用户需要将特定的数据处理规则在规则编辑模块中编辑并存入规则数据表中。用户提交的处理请求可能转化成不止一次的处理匹配工作。这就是说，信息处理语句返回的结果可能导致处理引擎发送新的信息处理语句，这取决于用户处理请求的内容和匹配规则的制订。

此外，用户请求对象可以输出为处理方案加以保存，反之也可以进行加载。输出就是将用户请求对象转换为 XML 格式的处理请求正文，反之亦然。系统中的方案保存/加载模块，用于将用户某次定义的数据处理请求转换成用户请求对象作为方案保存，以便以后可以方便地直接调用。

最后所应说明的是，以上实施例仅用以说明本发明的技术方案而非限制，尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员

应当理解，可以对本发明的技术方案进行修改或者等同替换，而不脱离本发明技术方案的精神和范围，其均应涵盖在本发明的权利要求范围当中。

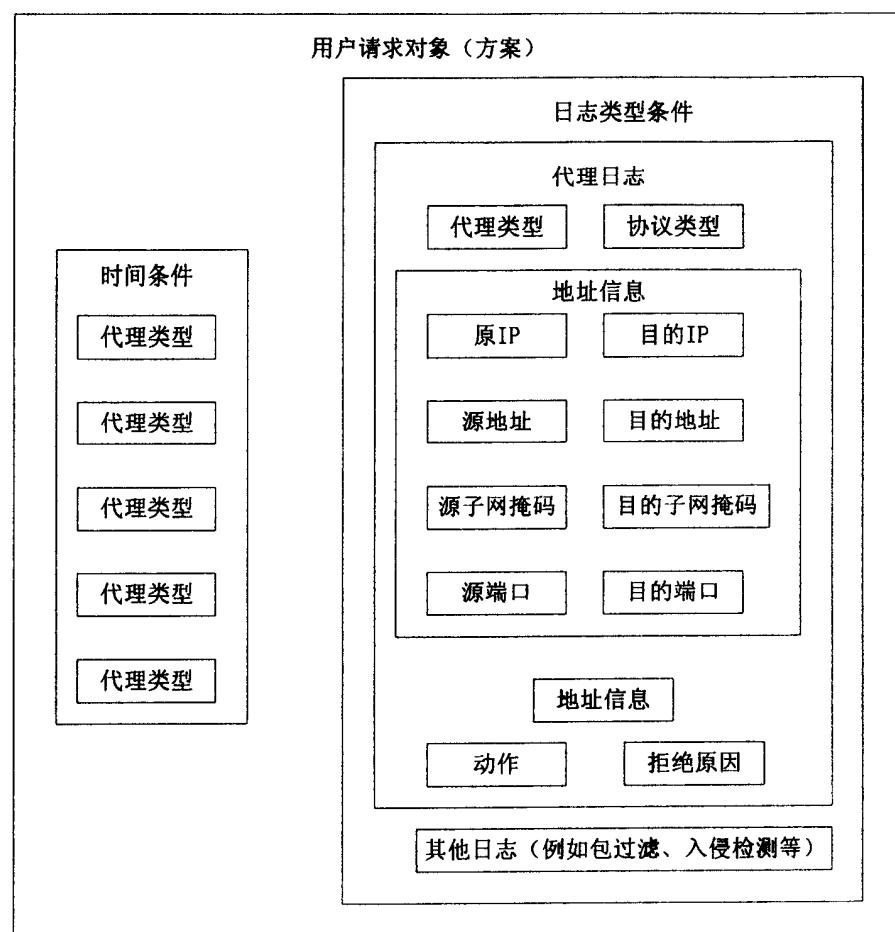


图 1

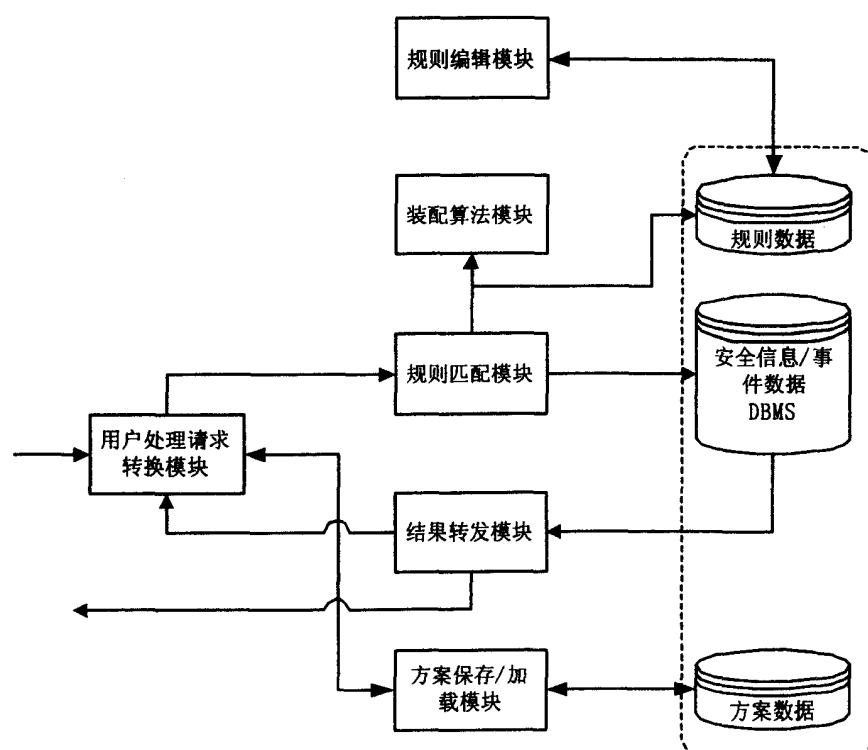


图 2

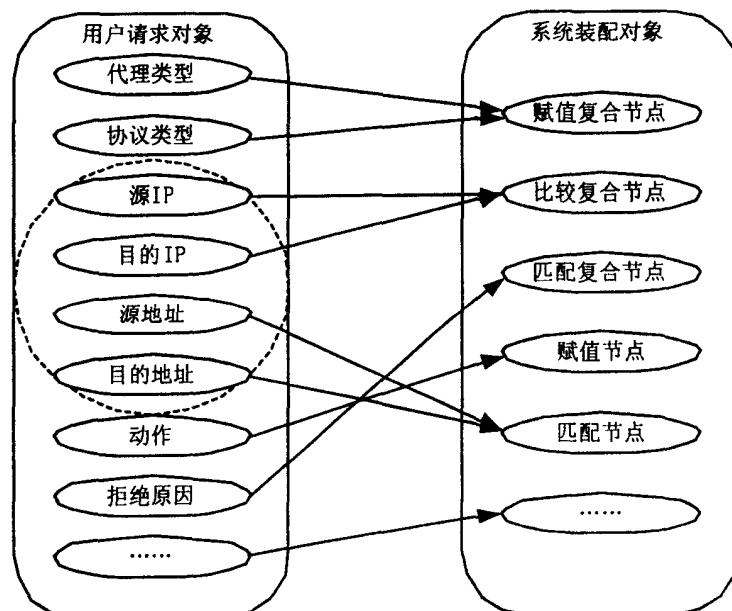


图 3

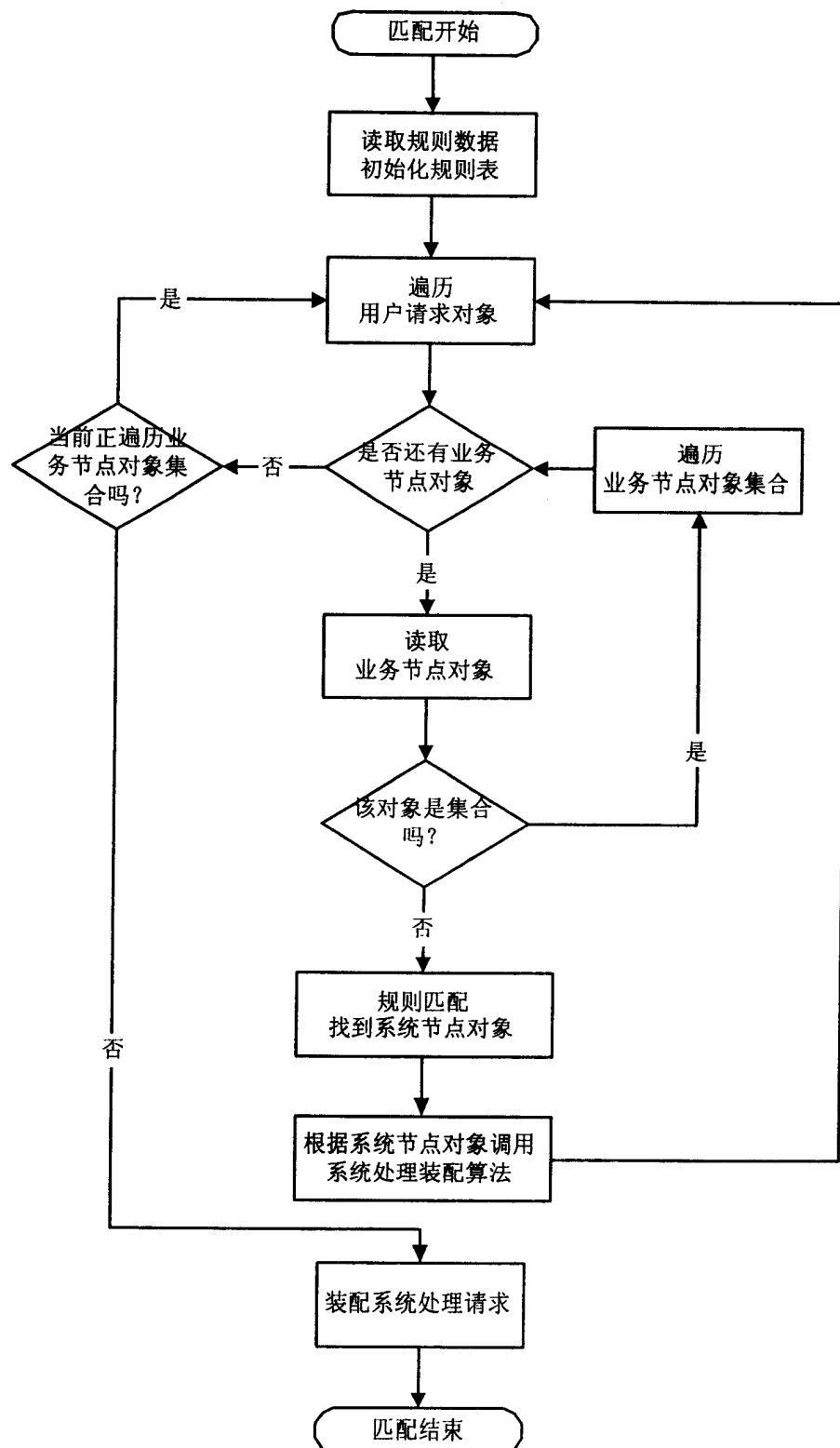


图 4