(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112686029 B
(45)授权公告日 2024.07.26

(21)申请号 202011579141.5
(22)申请日 2020.12.28
(65)同一申请的已公布的文献号
申请公布号 CN 112686029 A
(43)申请公布日 2021.04.20
(73)专利权人 江苏苏宁云计算有限公司
地址 210042 江苏省南京市玄武区徐庄软件园苏宁大道1-1号
(72)发明人 韦建明 葛毅 李宗霖
(74)专利代理机构 北京市万慧达律师事务所 11111
专利代理师 黄玉东
(51)Int.Cl.
G06F 40/253(2020.01)
G06F 40/284(2020.01)
G06F 16/242(2019.01)
(56)对比文件
CN 105373607 A,2016.03.02
审查员 辛欣

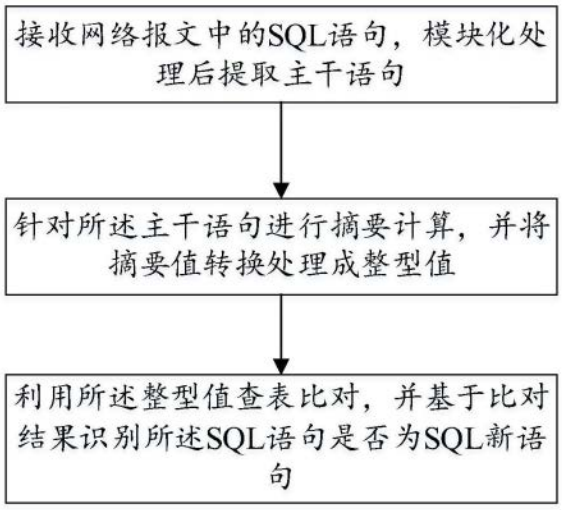
权利要求书2页 说明书7页 附图4页

(54)发明名称

用于数据库审计系统的SQL新语句识别方法及装置

(57)摘要

本发明公开一种用于数据库审计系统的SQL新语句识别方法及装置,涉及大数据技术领域,能够有效降低数据库审计系统的资源占用量,进而提升系统性能。该方法包括:接收网络报文中的SQL语句,模块化处理后提取主干语句;针对主干语句进行摘要计算,并将摘要值转换处理成整型值;利用整型值查表比对,并基于比对结果识别SQL语句是否为SQL新语句。该装置应用有上述方案所提的方法。



CN 112686029 B

1.一种用于数据库审计系统的SQL新语句识别方法,其特征在于,包括:

接收网络报文中的SQL语句,模块化处理后提取主干语句;

针对所述主干语句进行摘要计算,并将摘要值转换处理成整型值;

利用所述整型值查表比对,并基于比对结果识别所述SQL语句是否为SQL新语句;

其中,模块化处理后提取主干语句包括:

识别所述SQL语句中的SQL语法关键字,剔除所述SQL语句中除SQL语法关键字之外的内容得到所述主干语句,所述语法关键字包括SELECT、INSERT,所述语法关键字之外的内容包括所述SQL语句中的数值、字符串;

其中,针对所述主干语句进行摘要计算,并将摘要值转换处理成整型值包括:对特定语句插入的多行语句进行合并处理,保留SQL语法主干,提取为不包含具体数值的主干语句,对所述提取的不包含具体数值的主干语句做MD5摘要计算,取16位字节摘要值的高位8字节,并将该8字节数据转换成64bit整型值,以使用一个长整型数值表示一条SQL语句,将该长整型值保存到HASH表中,其中,所述特定语句为WHEREAND()、INSERT。

2.根据权利要求1所述的方法,其特征在于,针对所述主干语句进行摘要计算之前还包括:

识别所述主干语句中是否存在组合值;

若存在则对组合值进行合并处理,再对其中的参数值采用通用字符替换进行去值处理;

若不存在,则直接对其中的参数值采用通用字符替换进行去值处理;

所述参数值包括变量参数和/或字符串。

3.根据权利要求1或2所述的方法,其特征在于,针对所述主干语句进行摘要计算之前还包括:

将所述主干语句的非ascii码采用通用字符进行替换处理。

4.根据权利要求1所述的方法,其特征在于,利用所述整型值查表比对,并基于比对结果识别所述SQL语句是否为SQL新语句的方法包括:

所述表中包括多个与主干语句一一对应的key-value键值对,所述key值为对应主干语句的整型值,所述value值为对应SQL语句的接收时间;

针对当前接收到的SQL语句对应的整型值查表,若所述表中存在与所述整型值相同的key值,则识别所述SQL语句不是SQL新语句,同时将所述整型值作为key值,将所述SQL语句的接收时间作为value值,以key-value键值对的形式存入表中;

若所述表中不存在与所述整型值相同的key值,则识别所述SQL语句为SQL新语句。

5.根据权利要求4所述的方法,其特征在于,识别所述SQL语句不是SQL新语句之后还包括:

比较新加入表中的所述SQL语句与表中已存在的相同key值对应SQL语句的接收时间差值,并在接收时间差值超过阈值时删除表中已存在的key-value键值对。

6.根据权利要求1所述的方法,其特征在于,还包括:

对识别为SQL新语句的SQL语句进行新语句标识;

将标识结果、对应的所述SQL语句、对应的所述整型值整合成一条json数据,提交至消息队列以供消费;

利用风险引擎从消息队列中消费所述json数据,提供针对SQL新语句的风险分析服务。

7.一种用于数据库审计系统的SQL新语句识别装置,其特征在于,包括:

主干提取单元,用于接收网络报文中的SQL语句,模块化处理后提取主干语句;其中,模块化处理后提取主干语句包括:识别所述SQL语句中的SQL语法关键字,剔除所述SQL语句中除SQL语法关键字之外的内容得到所述主干语句,所述语法关键字包括SELECT、INSERT,所述语法关键字之外的内容包括所述SQL语句中的数值、字符串;

整型处理单元,用于针对所述主干语句进行摘要计算,并将摘要值转换处理成整型值;其中,针对所述主干语句进行摘要计算,并将摘要值转换处理成整型值包括:对特定语句插入的多行语句进行合并处理,保留SQL语法主干,提取为不包含具体数值的主干语句,对所述提取的不包含具体数值的主干语句做MD5摘要计算,取16位字节摘要值的高位8字节,并将该8字节数据转换成64bit整型值,以使用一个长整型数值表示一条SQL语句,将该长整型值保存到HASH表中,其中,所述特定语句为WHERE AND()、INSERT;

识别单元,用于利用所述整型值查表比对,并基于比对结果识别所述SQL语句是否为SQL新语句。

8.一种计算机可读存储介质,计算机可读存储介质上存储有计算机程序,其特征在于,计算机程序被处理器运行时执行上述权利要求1至6任一项所述方法的步骤。

用于数据库审计系统的SQL新语句识别方法及装置

技术领域

[0001] 本发明涉及大数据技术领域,尤其涉及一种用于数据库审计系统的SQL新语句识别方法及装置。

背景技术

[0002] 数据库审计系统主要用于审计数据库服务器上的各类操作行为,通过旁路镜像或者安装插件的方式获取数据库服务器的网络报文,然后提取报文中的SQL语句保存到数据库审计系统的数据库中,以便后续进行查询、过滤、分析等操作,从而实现对数据库服务器的监控和审计。

[0003] 数据库审计系统通过分析提取的SQL语句,判断被审计的数据库服务器是否存在漏洞或者被攻击行为。从技术实现角度看就是对SQL语句的提取、分析、保存,其中分析就是审计SQL语句是否存在漏洞或者攻击。为了确保审计的准确性,审计系统需要分析所有的SQL语句,随着审计系统部署的数据库服务器的数量越来越多,被审计的数据库业务流量流越来越大,已有的软硬件平台已经不能满足需求。

[0004] 经过分析发现,在实际的业务流量中,有很多SQL语句都是相同的,另外还有一些语句的语法主干相同,只是参数值不同而已。以上这类相同的语句在审计系统中其实只需要分析一次,假设数据库审计系统只处理这些不同的SQL语句,那它只需要很小的一部分流量。这就需要审计系统在进行SQL分析前就能识别出哪些语句是首次出现的。

[0005] 常用的几种识别SQL语句的方法主要有:字符匹配、AI识别、SQL语义解析等。上述几种方法都有一定的弊端,比如字符匹配无法忽略不同参数值,如ID=3和ID=4,字符匹配会认为这是两条语句,无法有效过滤重复语句,另外大量超长SQL语句对CPU和存储空间都有很高的要求;AI识别在实际使用中短时间内也无法保证准确度,另外还需要增加额外的硬件服务器,反而会增加系统的部署成本;SQL语义分析同样比较占资源,新语句识别就是为了过滤掉大量重复的语句,降低后续SQL语义分析的负载,只有新语句才需要做语义分析。

发明内容

[0006] 本发明的目的在于提供一种用于数据库审计系统的SQL新语句识别方法及装置,能够有效降低数据库审计系统的资源占用量,进而提升系统性能。

[0007] 为了实现上述目的,本发明的第一方面提供一种用于数据库审计系统的SQL新语句识别方法,包括:

[0008] 接收网络报文中的SQL语句,模块化处理后提取主干语句;

[0009] 针对所述主干语句进行摘要计算,并将摘要值转换处理成整型值;

[0010] 利用所述整型值查表比对,并基于比对结果识别所述SQL语句是否为SQL新语句。

[0011] 优选地,模块化处理后提取主干语句的方法包括:

[0012] 识别所述SQL语句中的SQL语法关键字,剔除所述SQL语句中除SQL语法关键字之外

的内容得到所述主干语句。

[0013] 较佳地,针对所述主干语句进行摘要计算之前还包括:

[0014] 识别所述主干语句中是否存在组合值;

[0015] 若存在则对组合值进行合并处理,再对其中的参数值采用通用字符替换进行去值处理;

[0016] 若不存在,则直接对其中的参数值采用通用字符替换进行去值处理;

[0017] 所述参数值包括变量参数和/或字符串。

[0018] 较佳地,针对所述主干语句进行摘要计算之前还包括:

[0019] 将所述主干语句的非ascii码采用通用字符进行替换处理。

[0020] 优选地,针对所述主干语句进行摘要计算,并将摘要值转换处理得到整型值的方法包括:

[0021] 采用MD5算法对处理后的所述主干语句进行摘要计算,得到摘要值;

[0022] 从所述摘要值中提取固定位置的部分字节数据,采用整型算法转化成整型值。

[0023] 进一步地,利用所述整型值查表比对,并基于比对结果识别所述SQL语句是否为SQL新语句的方法包括:

[0024] 所述表中包括多个与主干语句一一对应的key-value键值对,所述key值为对应主干语句的整型值,所述value值为对应SQL语句的接收时间;

[0025] 针对当前接收到的SQL语句对应的整型值查表,若所述表中存在与所述整型值相同的key值,则识别所述SQL语句不是SQL新语句,同时将所述整型值作为key值,将所述SQL语句的接收时间作为value值,以key-value键值对的形式存入表中;

[0026] 若所述表中不存在与所述整型值相同的key值,则识别所述SQL语句为SQL新语句。

[0027] 进一步地,识别所述SQL语句不是SQL新语句之后还包括:

[0028] 比较新加入表中的所述SQL语句与表中已存在的相同key值对应SQL语句的接收时间差值,并在接收时间差值超过阈值时删除表中已存在的key-value键值对。

[0029] 优选地,根据权利要求1所述的方法,其特征在于,还包括:

[0030] 对识别为SQL新语句的SQL语句进行新语句标识;

[0031] 将标识结果、对应的所述SQL语句、对应的所述整型值整合成一条json数据,提交至消息队列以供消费;

[0032] 利用风险引擎从消息队列中消费所述json数据,提供针对SQL新语句的风险分析服务。

[0033] 与现有技术相比,本发明提供的用于数据库审计系统的SQL新语句识别方法具有以下有益效果:

[0034] 本发明提供的用于数据库审计系统的SQL新语句识别方法中,在接收到网络报文的SQL语句时,通过模块化处理后提取主干语句,并针对主干语句进行摘要计算,并将摘要值转换处理成整型值,之后利用整型值查表比对,若表中存在与整型值相同的key值,则识别SQL语句不是SQL新语句,同时将整型值作为key值,将SQL语句的接收时间作为value值,以key-value键值对的形式存入表中,若表中不存在与整型值相同的key值,则识别SQL语句为SQL新语句。

[0035] 可见,本发明首先对SQL语句进行模板化处理,提取SQL语法主干,然后对SQL语法

主干进行摘要计算,最终用一个整型数值标识一组具备相同语义的SQL语句。与现有技术中的字符匹配方案相比,本发明方案屏蔽了不停变化的value值信息,只关注语句主干。与现有技术中的SQL语义分析相比,本发明方案不做具体的语义分析,重点关注语句是否相同,避免了不必要的语义分析占用过多的系统资源。通过生产环境实际使用数据表明,采用本发明方案的新语句识别方法所占资源在系统中几乎可以忽略不计,因此可以有效降低数据库审计系统的资源占用量,提升系统性能。

[0036] 本发明的第二方面提供一种用于数据库审计系统的SQL新语句识别装置,应用于上述技术方案所述的用于数据库审计系统的SQL新语句识别方法中,所述装置包括:

[0037] 主干提取单元,用于接收网络报文中的SQL语句,模块化处理后得到主干语句;

[0038] 整型处理单元,用于针对所述主干语句进行摘要计算,并将摘要值转换处理成整型值;

[0039] 识别单元,用于利用所述整型值查表比对,并基于比对结果识别所述SQL语句是否为SQL新语句。

[0040] 与现有技术相比,本发明提供的用于数据库审计系统的SQL新语句识别装置的有益效果与上述技术方案提供的用于数据库审计系统的SQL新语句识别方法的有益效果相同,在此不做赘述。

[0041] 本发明的第三方面提供一种计算机可读存储介质,计算机可读存储介质上存储有计算机程序,计算机程序被处理器运行时执行上述用于数据库审计系统的SQL新语句识别方法的步骤。

[0042] 与现有技术相比,本发明提供的计算机可读存储介质的有益效果与上述技术方案提供的用于数据库审计系统的SQL新语句识别方法的有益效果相同,在此不做赘述。

附图说明

[0043] 此处所说明的附图用来提供对本发明的进一步理解,构成本发明的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0044] 图1为本发明实施例中用于数据库审计系统的SQL新语句识别方法的一种流程示意图;

[0045] 图2为本发明实施例中SQL语句模板化的处理流程示意图;

[0046] 图3为本发明实施例中SQL新语句识别处理的流程示意图;

[0047] 图4为本发明实施例中风险引擎检测SQL新语句的流程示意图。

具体实施方式

[0048] 为使本发明的上述目的、特征和优点能够更加明显易懂,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,所描述的实施例仅仅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的前提下所获得的所有其它实施例,均属于本发明保护的范围。

[0049] 实施例一

[0050] 请参阅图1-图4,本实施例提供一种用于数据库审计系统的SQL新语句识别方法,

包括：

[0051] 接收网络报文中的SQL语句,模块化处理后提取主干语句;针对主干语句进行摘要计算,并将摘要值转换处理成整型值;利用整型值查表比对,并基于比对结果识别SQL语句是否为SQL新语句。

[0052] 本实施例提供的用于数据库审计系统的SQL新语句识别方法中,在接收到网络报文的SQL语句时,通过模块化处理后提取主干语句,针对主干语句进行摘要计算,并将摘要值转换处理成整型值,之后利用整型值查表比对,若表中存在与整型值相同的key值,则识别SQL语句不是SQL新语句,同时将整型值作为key值,将SQL语句的接收时间作为value值,以key-value键值对的形式存入表中,若表中不存在与整型值相同的key值,则识别SQL语句为SQL新语句。

[0053] 可见,本实施例首先对SQL语句进行模板化处理,提取SQL语法主干,然后对SQL语法主干进行摘要计算,最终用一个整型数值标识一组具备相同语义的SQL语句。与现有技术中的字符匹配方案相比,本实施例方案屏蔽了不停变化的value值信息,只关注语句主干。与现有技术中的SQL语义分析相比,本实施例方案不做具体的语义分析,重点关注语句是否相同,避免了不必要的语义分析占用过多的系统资源。通过生产环境实际使用的数据表明,采用本实施例方案的新语句识别方法所占资源在系统中几乎可以忽略不计,因此可以有效降低数据库审计系统的资源占用量,提升系统性能。

[0054] 请参阅图2,上述实施例中,模块化处理后提取主干语句的方法包括：

[0055] 识别SQL语句中的SQL语法关键字,剔除SQL语句中除SQL语法关键字之外的内容得到主干语句。示例性地,SQL语法关键字包括SELECT和INSERT等。

[0056] 上述实施例中,针对主干语句进行摘要计算之前还包括：

[0057] 识别主干语句中是否存在组合值;若存在则对组合值进行合并处理,再对其中的参数值采用通用字符替换进行去值处理;若不存在,则直接对其中的参数值采用通用字符替换进行去值处理;例如,组合值为VALUES(1,'TOM'),(2,'JIMMY'),(3,'SAM'),(4,'LI'),具体实施时,通用字符可采用"?",采用通用字符替换后的value值为VALUES(?)。参数值包括变量参数和/或字符串,示例性地,变量参数为"1",字符串为"TOM"。

[0058] 上述实施例中,针对主干语句进行摘要计算之前还包括：

[0059] 将主干语句的非ascii码采用通用字符进行替换处理,如在concat('%',赞比特,'%')中,将汉字字符串替换成"?"。

[0060] 上述实施例中,针对主干语句进行摘要计算,并将摘要值转换处理得到整型值的方法包括：

[0061] 采用MD5算法对处理后的主干语句进行摘要计算,得到摘要值;从摘要值中提取固定位置的部分字节数据,采用整型算法转化成整型值。示例性地,摘要值为10055897659947028311共16位,取16位字节中的第8到15位的字节数据,将这8字节值转化成64bit整型值。

[0062] 上述实施例中,利用整型值查表比对,并基于比对结果识别SQL语句是否为SQL新语句的方法包括：

[0063] 表中包括多个与主干语句一一对应的key-value键值对,key值为对应主干语句的整型值,value值为对应SQL语句的接收时间;针对当前接收到的SQL语句对应的整型值查

表,若表中存在与整型值相同的key值,则识别SQL语句不是SQL新语句,同时将整型值作为key值,将SQL语句的接收时间作为value值,以key-value键值对的形式存入表中;若表中不存在与整型值相同的key值,则识别SQL语句为SQL新语句。

[0064] 上述实施例中,在识别SQL语句不是SQL新语句之后还包括:

[0065] 比较新加入表中的SQL语句与表中已存在的相同key值对应SQL语句的接收时间差值,并在接收时间差值超过阈值时删除表中已存在的key-value键值对。具体实施时,系统周期地检测表中的key-value键值对,若新加入SQL语句的key值能够在表中的key-value键值对中匹配上,则根据新加入SQL语句的value值与表中对应的value值计算接收时间差值,如果接收时间差值超过阈值时删除表中之前的key-value键值对。

[0066] 上述实施例中,在利用所述整型值查表比对,并基于比对结果识别所述SQL语句是否为SQL新语句之后还包括:

[0067] 对识别为SQL新语句的SQL语句进行新语句标识;将标识结果、对应的SQL语句、对应的整型值整合成一条json数据,提交至消息队列以供消费;利用风险引擎从消息队列中消费json数据,提供针对SQL新语句的风险分析服务。

[0068] 为便于理解,现对本实施例方案做如下示例性描述:

[0069] 具体实施时,通过对SQL语句进行模板化处理,只保留SQL语句中的SQL语法关键字,如SELECT、INSERT等,屏蔽掉SQL语句中的value值,如数值、字符串等数据,并对特定的语句WHERE AND()、INSERT插入的多行语句进行合并处理,只保留SQL语法主干,提取成一个不包含具体数值的主干语句,然后对提取的主干语句做MD5摘要计算,取16位字节摘要值的高位8字节,并将该8字节数据转换成64bit整型值,目的是使用一个长整型数值表示一条SQL语句,最后将该长整型值保存到HASH表中。具体的实施方式步骤如下:

[0070] 步骤1:接收从网络报文中提取的SQL语句,该SQL语句是一条完整的SQ语句,包括INSERT和/或SELECT SQL语法关键字;例如INSERT语法关键字为:INSERT INTO USERINFO_0(USERID、USERNAME)VALUES(1,'TOM'),(2,'JIMMY'),(3,'SAM'),(4,'LI');SELECT语法关键字为:SELECT*FROM USERINFO_0WHERE ID=1;

[0071] 步骤2:对该SQL语句进行去值处理,即将SQL语句中的数值或者字符串统一替换成“?”,如将WHERE ID=1替换成WHERE ID=?,将WHERE NAME=“titlename”替换成WHERE NAME=“?”,需要强调的是,一个完整的数值只能替换成一个问号,如123替换成“?”,而不是“???”。

[0072] 经过步骤2处理后,上文中的SELECT语法关键字替换成:SELECT*FROM USERINFO_0WHERE ID=?;

[0073] 步骤3:将INSERT语句中多条记录的组合值进行合并处理,如INSERT语句插入的是一个JSON数组对象数据,该数组对象中包含多条记录,不同记录数会导致被识别成不同的语句,所以需要将多条记录合并一条处理;

[0074] 经过步骤3,INSERT语句替换成:INSERT INTO USERINFO_0(USERID,USERNAME)VALUES(?,?);

[0075] 步骤4:将SELECT语法关键字中其它需要合并值的语句,如将WHERE AND、WHERE OR、WHERE NOT等语句中的多个条件进行合并处理;

[0076] 步骤5:处理非ascii码,如在concat('%',赞比特,'%')中,将汉字字符串替换成

“?”;

[0077] 步骤6:步骤5处理完成后,得到一个主干语句,对该主干语句进行MD5摘要处理,例如,上述步骤中的INSERT语句和SELECT语句分别对应的摘要值为10055897659947028311和3935916992245373588;

[0078] 步骤7:对摘要值进行简化处理,取16位字节中的第8到15位的字节数据,将这8字节值转化成64bit整型值。

[0079] 当一条完整的SQL语句经过图2步骤简化成一个整型值后,将被学习到一张hashmap表中,该表的key就是SQL语句简化的整型值,vlaue是接收到该条SQL语句的时间戳。

[0080] 步骤1:从网络报文中提取SQL语句,经过如图2步骤所示进行模板化处理后,提取摘要值;

[0081] 步骤2:使用摘要计算取得的整型值做为key读取hashmap存储表,如果能从hashmap存储表中读取到,则认为不是SQL新语句,此时只需更新该节点的时间戳即可,该时间戳用于超时判断。如果不能从hashmap存储表中读取到,则认为是SQL新语句,此时需将key值和value值添加入hashmap存储表中;

[0082] 步骤3:如果是SQL新语句增加新语句标识,并将该新语句标识、该SQL语句和SQL语句摘要整型值一起组织成一条json数据;

[0083] 步骤4:将json数据提交到消息队列中以供消费。

[0084] 图4是风险引擎处理SQL新语句的流程图,风险引擎对SQL语句进行安全分析,风险引擎只处理带新语句标识的SQL语句。

[0085] 步骤1:风险引擎从消息队列中读取JSON数据,其中包含一条完整SQL语句和新语句标识。

[0086] 步骤2:风险引擎根据新语句标识判断该条SQL语句为新语句,并做语句分析处理,识别其是否存在风险,如果不是新语句则不处理该SQL语句。

[0087] 综上,本实施例具备如下有益效果:

[0088] SQL语句模板化:对SQL语句进行去值、合并处理,提取语句主干,形成SQL语句模板,能够减少系统资源的占用,提升系统性能;

[0089] 摘要处理:对处理后的SQL语句模板进行摘要处理,用一个长整型数值标识一个主干语句,能够加快查表速度;

[0090] KMP优化算法:模板化处理过程中需要对语句进行匹配操作,普通直观的字符匹配时间复杂度是O(MxN),KMP算法的时间复杂度是O(M+N),本实施例利用SQL语句特点优化了KMP算法,将时间复杂度降低到O(M-2N)以下。

[0091] 实施例二

[0092] 本实施例提供一种用于数据库审计系统的SQL新语句识别装置,包括:

[0093] 主干提取单元,用于接收网络报文中的SQL语句,模块化处理后提取主干语句;

[0094] 整型处理单元,用于针对所述主干语句进行摘要计算,并将摘要值转换处理成整型值;

[0095] 识别单元,用于利用所述整型值查表比对,并基于比对结果识别所述SQL语句是否为SQL新语句。

[0096] 与现有技术相比,本发明实施例提供的用于数据库审计系统的SQL新语句识别装置的有益效果与上述实施例一提供的用于数据库审计系统的SQL新语句识别方法的有益效果相同,在此不做赘述。

[0097] 实施例三

[0098] 本实施例提供一种计算机可读存储介质,计算机可读存储介质上存储有计算机程序,计算机程序被处理器运行时执行上述用于数据库审计系统的SQL新语句识别方法的步骤。

[0099] 与现有技术相比,本实施例提供的计算机可读存储介质的有益效果与上述技术方案提供的用于数据库审计系统的SQL新语句识别方法的有益效果相同,在此不做赘述。

[0100] 本领域普通技术人员可以理解,实现上述发明方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成,上述程序可以存储于计算机可读取存储介质中,该程序在执行时,包括上述实施例方法的各步骤,而的存储介质可以是:ROM/RAM、磁碟、光盘、存储卡等。

[0101] 以上,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以所述权利要求的保护范围为准。

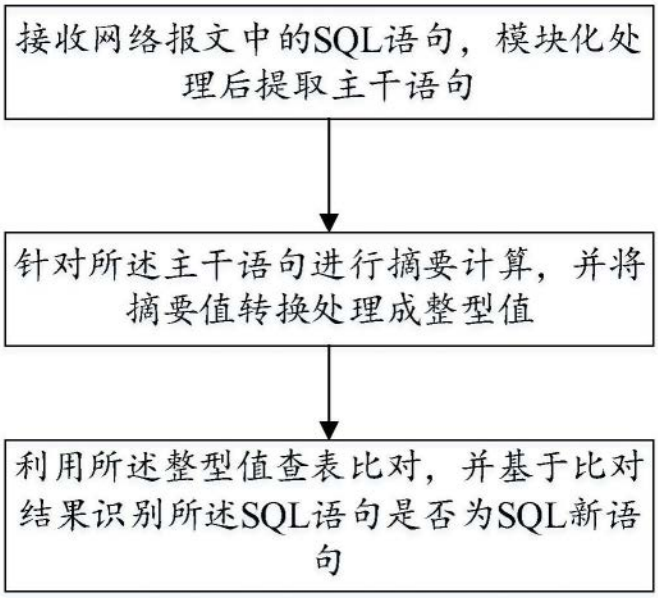

接收网络报文中的SQL语句，模块化处理后提取主干语句
针对所述主干语句进行摘要计算，并将摘要值转换处理成整型值
利用所述整型值查表比对，并基于比对结果识别所述SQL语句是否为SQL新语句

图1



图2

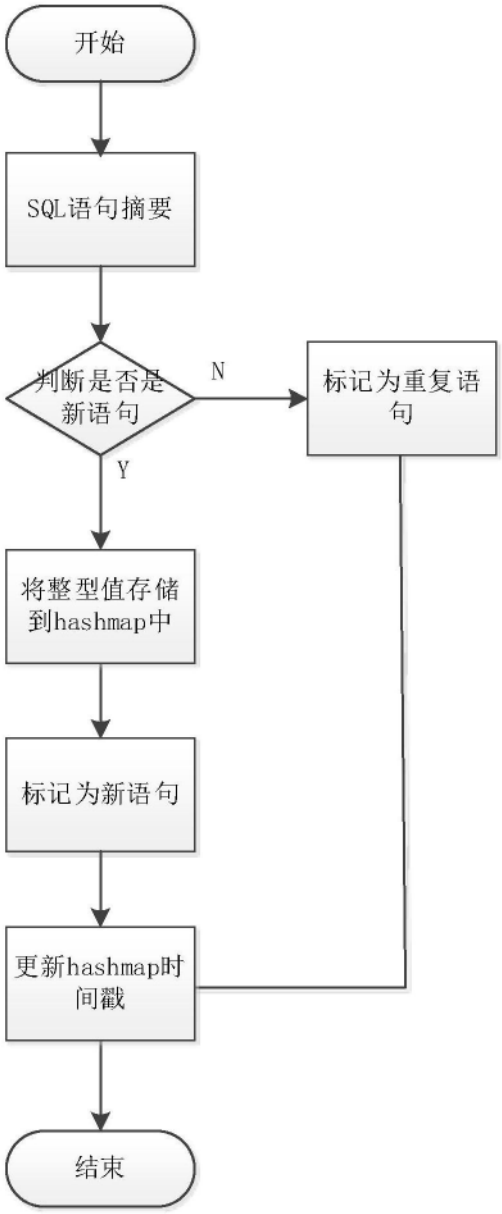

开始
SQL语句摘要
判断是否是新语句
N
标记为重复语句
Y
将整型值存储到hashmap中
标记为新语句
更新hashmap时间戳
结束

图3

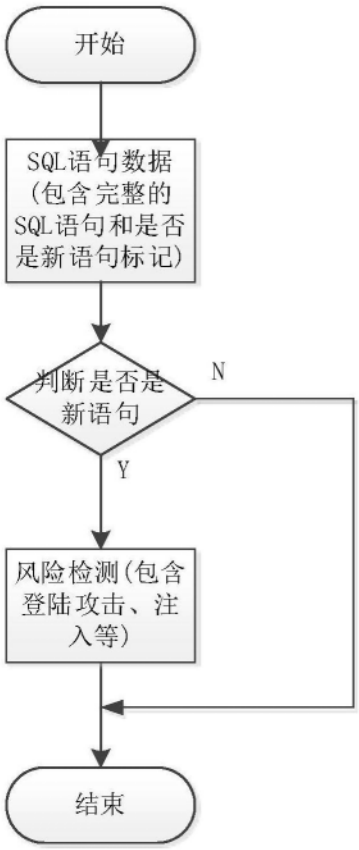

开始
SQL语句数据（包含完整的SQL语句和是否是新语句标记）
判断是否是新语句
N
Y
风险检测(包含登陆攻击、注入等)
结束

图4