(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 110827139 A
(43)申请公布日 2020.02.21

(21)申请号 201911053061.3

(22)申请日 2019.10.31

(71)申请人 中国工商银行股份有限公司
地址 100140 北京市西城区复兴门内大街55号

(72)发明人 柏佳宁 高鸿升 胡强 刘吉洲

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 孙乳笋 汤在彦

(51)Int.Cl.
G06Q 40/02(2012.01)

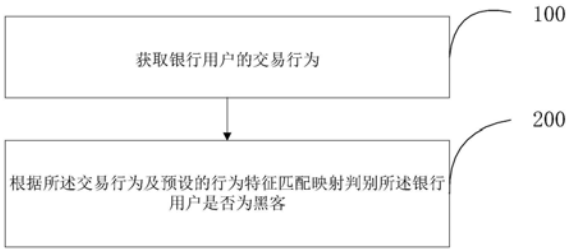
权利要求书1页 说明书9页 附图4页

(54)发明名称

基于行为特征的银行黑客用户判别方法及装置

(57)摘要

本发明提供了一种基于行为特征的银行黑客用户判别方法及装置,基于行为特征的银行黑客用户判别方法包括:获取银行用户的交易行为;根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客。本方法可以提前发现黑客针对银行系统的探索行为,并对其实施冻结措施,避免了黑客长期分析探索系统造成安全威胁的情况。



CN 110827139 A

1.一种基于行为特征的银行黑客用户判别方法,其特征在于,包括:

获取银行用户的交易行为;

根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客。

2.根据权利要求1所述的银行黑客用户判别方法,其特征在于,所述根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客,包括:

判别所述交易行为中交易金额是否为零或者负数;

如果是,初步判别所述银行用户为黑客。

3.根据权利要求2所述的银行黑客用户判别方法,其特征在于,所述初步判别所述银行用户为黑客之后,还包括:

分别判别所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值;

如果是,最终判别所述银行用户为所述黑客。

4.根据权利要求3所述的银行黑客用户判别方法,其特征在于,还包括:

根据所述交易行为以及其交易金额是否为零或者负数的判别结果,以及所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值的判别结果,生成所述交易行为与黑客判别结果的行为特征匹配映射。

5.一种基于行为特征的银行黑客用户判别装置,其特征在于,包括:

交易行为获取单元,用于获取银行用户的交易行为;

黑客判别单元,用于根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客。

6.根据权利要求5所述的黑客用户判别装置,其特征在于,所述黑客识别单元具体用于判别所述交易行为中交易金额是否为零或者负数;如果是,初步判别所述银行用户为黑客。

7.根据权利要求6所述的黑客用户判别装置,其特征在于,所述黑客识别单元具体还用于分别判别所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值;如果是,最终判别所述银行用户为所述黑客。

8.根据权利要求7所述的黑客用户判别装置,其特征在于,还包括:

映射生成单元,用于根据所述交易行为以及其交易金额是否为零或者负数的判别结果,以及所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值的判别结果,生成所述交易行为与黑客判别结果的行为特征匹配映射。

9.一种电子设备,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,其特征在于,所述处理器执行所述程序时实现权利要求1至4任一项所述基于行为特征的银行黑客用户判别方法的步骤。

10.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该计算机程序被处理器执行时实现权利要求1至4任一项所述基于行为特征的银行黑客用户判别方法的步骤。

基于行为特征的银行黑客用户判别方法及装置

技术领域

[0001] 本发明涉银行网络安全技术领域，特别是涉及一种基于行为特征的银行黑客用户判别方法及装置。

背景技术

[0002] 近几年，随着移动互联网的快速发展，银行业面中对于网络金融犯罪的压力越来越大。黑客在真正找到银行可以利用安全漏洞前，需要逐步进行探索才可以实现其目的。现有技术均是在黑客发现安全漏洞之后，甚至实现非法操作之后才进行补救，与之而来带来的不利之处为：一是会使银行和用户的利益收到损失，银行相对于黑客始终是处于被动，不利于提前预判及预先识别黑客及黑客的行为。

发明内容

[0003] 针对现有技术中的问题，本发明提供的基于行为特征的银行黑客用户判别方法，可以在黑客探索银行系统的初期就识别出其客户信息，并对其来探索的客户账户实施冻结，阻止其对银行信息系统进一步实施探索。

[0004] 为解决上述技术问题，本发明提供以下技术方案：

[0005] 第一方面，本发明提供一种基于行为特征的银行黑客用户判别方法，包括：

[0006] 获取银行用户的交易行为；

[0007] 根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客。

[0008] 优选地，所述根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客，包括：

[0009] 判别所述交易行为中交易金额是否为零或者负数；

[0010] 如果是，初步判别所述银行用户为黑客。

[0011] 优选地，所述初步判别所述银行用户为黑客之后，还包括：

[0012] 分别判别所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值；

[0013] 如果是，最终判别所述银行用户为所述黑客。

[0014] 优选地，基于行为特征的银行黑客用户判别方法还包括：

[0015] 根据所述交易行为以及其交易金额是否为零或者负数的判别结果，以及所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值的判别结果，生成所述交易行为与黑客判别结果的行为特征匹配映射。

[0016] 第二方面，本发明提供一种基于行为特征的银行黑客用户判别装置，该装置包括：

[0017] 交易行为获取单元，用于获取银行用户的交易行为；

[0018] 黑客判别单元，用于根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客。

[0019] 优选地，所述黑客识别单元具体用于判别所述交易行为中交易金额是否为零或者

负数;如果是,初步判别所述银行用户为黑客。

[0020] 优选地,所述黑客识别单元具体还用于分别判别所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值;如果是,最终判别所述银行用户为所述黑客。

[0021] 优选地,基于行为特征的银行黑客用户判别装置还包括:

[0022] 映射生成单元,用于根据所述交易行为以及其交易金额是否为零或者负数的判别结果,以及所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值的判别结果,生成所述交易行为与黑客判别结果的行为特征匹配映射。

[0023] 第三方面,本发明提供一种电子设备,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,处理器执行程序时实现基于行为特征的银行黑客用户判别方法的步骤。

[0024] 第四方面,本发明提供一种计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现基于行为特征的银行黑客用户判别方法的步骤。

[0025] 从上述描述可知,本发明提供的基于行为特征的银行黑客用户判别方法及装置,针对银行中的黑客的行为特征(通常对于银行系统特别喜欢进行尝试把付款账号修改成他人账号,转账、购买交易金额修改为0或者负金额的情况),并根据该交易行为以及预设的行为特征匹配映射判别银行用户是否为黑客。进而进行自动预警,提醒运维人员进行相关紧急处理。从发明专利应用的实际效果看,本发明的效果和优点主要体现在如下:使用正常业务报错,发现黑客账号,并冻结账户:由于使用了正常业务报错日志,提前发现了黑客探索行为,并对其实施冻结措施,避免了黑客长期分析探索系统造成安全威胁的情况。冻结账户实现了自动化处理:分析处理黑客攻击账号,对运维人员造成较大工作负担。分析以及处理都实现自动化后会极大减轻运维人员负担。

附图说明

[0026] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术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的前提下,还可以根据这些附图获得其他的附图。

[0027] 图1为本发明的实施例中基于行为特征的银行黑客用户判别方法流程示意图一;

[0028] 图2为本发明的实施例中基于行为特征的银行黑客用户判别方法步骤200的流程示意图一;

[0029] 图3为本发明的实施例中基于行为特征的银行黑客用户判别方法步骤200的流程示意图二;

[0030] 图4为本发明的实施例中基于行为特征的银行黑客用户判别方法流程示意图二;

[0031] 图5为本发明的实施例中基于行为特征的银行黑客用户判别方法流程示意图三;

[0032] 图6为本发明的具体应用实例中基于行为特征的银行黑客用户判别方法的流程示意图;

[0033] 图7为本发明的具体应用实例中基于行为特征的银行黑客用户判别装置的结构示意图一;

[0034] 图8为本发明的具体应用实例中基于行为特征的银行黑客用户判别装置的结构示

意图二；

[0035] 图9为本发明的实施例中的电子设备的结构示意图。

具体实施方式

[0036] 为使本发明实施例的目的、技术方案和优点更加清楚，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、完整的描述，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。

[0037] 鉴于现有技术中存在提升当前验证码系统的安全性和易用性的相关需求，本发明的实施例提供一种基于行为特征的银行黑客用户判别方法的具体实施方式，参见图1，该方法具体包括如下内容：

[0038] 步骤100：获取银行用户的交易行为。

[0039] 可以理解的是，步骤100中的交易行为可以包括：银行用户的交易金额以及单位时间的交易次数。

[0040] 步骤200：根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客。

[0041] 可以理解的是，步骤200中的行为特征包括：银行用户的交易金额是否为零或者负数，以及银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值。

[0042] 从上述描述可知，本发明提供的基于行为特征的银行黑客用户判别方法，针对银行中的黑客的行为特征(通常对于银行系统特别喜欢进行尝试把付款账号修改成他人账号，转账、购买交易金额修改为0或者负金额的情况)，并根据该交易行为以及预设的行为特征匹配映射判别银行用户是否为黑客。进而进行自动预警，提醒运维人员进行相关紧急处理。从发明专利应用的实际效果看，本发明的效果和优点主要体现在如下：使用正常业务报错，发现黑客账号，并冻结账户：由于使用了正常业务报错日志，提前发现了黑客探索行为，并对其实施冻结措施，避免了黑客长期分析探索系统造成安全威胁的情况。冻结账户实现了自动化处理：分析处理黑客攻击账号，对运维人员造成较大工作负担。分析以及处理都实现自动化后会极大减轻运维人员负担。

[0043] 一实施例中，参见图2，步骤200包括：

[0044] 步骤201：判别所述交易行为中交易金额是否为零或者负数；如果是，初步判别所述银行用户为黑客。

[0045] 可以理解的是，在银行系统中，黑客通常利用将付款账号修改成他人账号，转账、购买交易金额修改为0或者负金额的方式，来寻找银行系统中的漏洞，所以可以以此作为初步判别所述银行用户是否为黑客的依据。

[0046] 一实施例中，参见图3，步骤200还包括：

[0047] 步骤202：分别判别所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值；如果是，最终判别所述银行用户为所述黑客。

[0048] 可以理解的是，一旦黑客发现银行系统漏洞之后，会频繁利用漏洞进行非法交易，故在步骤201的结果基础上，可以利用此用户行为特征作为最终判别所述银行用户是否为黑客的依据。

[0049] 一实施例中，参见图4，基于行为特征的银行黑客用户判别方法还包括：

[0050] 步骤300：根据所述交易行为以及其交易金额是否为零或者负数的判别结果，以及所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值的判别结果，生成所述交易行为与黑客判别结果的行为特征匹配映射。

[0051] 一实施例中，参见图5，基于行为特征的银行黑客用户判别方法还包括：

[0052] 步骤400：根据预设的业务编号白名单，排除掉正常业务有可能会导致校验付款账号为非本人账户的日志。

[0053] 可以理解的是，在进行黑客判别之前，需要将白名单中的客户信息编号排除(正常业务有可能会导致交易金额为负的日志)，客户使用的IP地址，客户使用的他人账号，业务编号，金额排出在外。

[0054] 从上述描述可知，本发明提供的基于行为特征的银行黑客用户判别方法，针对银行中的黑客的行为特征(通常对于银行系统特别喜欢进行尝试把付款账号修改成他人账号，转账、购买交易金额修改为0或者负金额的情况)，并根据该交易行为以及预设的行为特征匹配映射判别银行用户是否为黑客。进而进行自动预警，提醒运维人员进行相关紧急处理。从发明专利应用的实际效果看，本发明的效果和优点主要体现在如下：使用正常业务报错，发现黑客账号，并冻结账户：由于使用了正常业务报错日志，提前发现了黑客探索行为，并对其实施冻结措施，避免了黑客长期分析探索系统造成安全威胁的情况。冻结账户实现了自动化处理：分析处理黑客攻击账号，对运维人员造成较大工作负担。分析以及处理都实现自动化后会极大减轻运维人员负担。

[0055] 为进一步地说明本方案，本发明提供基于行为特征的银行黑客用户判别方法的具体应用实例，该具体应用实例具体包括如下内容，参见图6。

[0056] S0：提取银行工作日志。

[0057] 黑客尝试通过篡改付款方账号进行转账交易的时候，会产生一笔报错码为特定数值(本实施例中为96111676)的业务日志。把系统中最近24小时内的所有的报错码为96111676的日志信息提取出来。并过滤掉提取出来的日志记录中，业务编号为业务编号白名单中的记录，过滤掉提取出来日志记录中，客户信息编号为客户信息编号白名单中的记录。黑客尝试通过篡改交易金额进行转账或者付款交易的时候，会生产一笔金额为负的交易失败日志。把系统中最近24小时内的所有的交易金额为0或者为负的交易日志提取出来，并过滤掉提取出来的日志记录中，业务编号为业务编号白名单中的记录，过滤掉提取出来日志记录中，客户信息编号为客户信息编号白名单中的记录。统计提取出来的业务日志中登记的客户信息编号(每个账户的客户信息编号是惟一不变的，业务日志中以这个区分不同客户账户的操作)。统计提取出来的业务日志中登记的IP地址。

[0058] 统计到的异常日志中包括：转账交易中存在校验付款账号为非本人账户的报错日志，提取出所有的客户信息编号，客户使用的IP地址，客户使用的他人账号，业务编号，金额，存储到初步异常筛选表中，类型字段标记为账号错误。统计的系统日志，为数据仓库系统中的转账交易日志表中的数据。为提升数据提取效率，在数据仓库中，给转账交易日志表添加了存储交易报错编号字段的索引，从而提高了根据报错编号提取数据的速度。

[0059] S1：统计步骤S0中的银行用户的交易行为。

[0060] 以步骤S0中判别出的客户信息编号为主键，根据客户信息编号白名单，排除掉白

名单中客户信息编号后,把每一个客户信息编号的最近24小时的所有交易的数量查询出来,并把每一个客户信息编号最近24小时的转入,转出金额以及24小时前的余额以及现在余额统计出来。

[0061] 统计系统日志中转账交易,付款购买交易中存在交易金额为0,交易金额为负的日志,提取出所有客户信息编号,客户使用的IP地址,客户使用的他人账号,业务编号,金额,存储到初步异常筛选表中,类型字段标记为金额错误。统计的系统日志,为的数据仓库系统中的转账交易日志表中的数据。为提升数据提取效率,在数据仓库中,给转账交易日志表添加了金额字段的索引。提高了根据金额字段为0或者为负提取数据的速度。

[0062] 可以理解的是需要对统计后的结果进行过滤,排除掉正常业务有可能会导致校验付款账号为非本人账户的日志。具体过滤算法为:根据统计异常日志中得到的统计后的数据--初步异常筛选表中类型为账号错误的记录,delete掉业务编号为业务编号白名单表中存在的记录。

[0063] 接着,对过滤后的数据进行加工,以客户信息编号为主键,根据客户信息编号白名单,排除掉白名单中客户信息编号后,把每一个客户信息编号的最近24小时的所有交易的数量查询出来,并把每一个客户信息编号最近24小时的转入,转出金额以及24小时前的余额,跟现在余额统计出来。具体加工算法为:根据在执行了数据过滤后初步异常筛选表中新增的数据,查询出所有新增记录的客户信息编号字段,去重。然后关联查询包括转账交易日志在内的各种交易日志,(目前是3000多种,而且还在随着交易种类增加,还在持续增长中),统计出各个客户信息编号的总的交易记录数。存储在内存中供给决策判断模块判断。关联查询转账交易日志,统计出各个客户信息编号最近24小时的总的转入金额,总的转出金额。存储在内存中供给决策判断模块判断。并根据数客户信息编号,查询数据仓库中余额表前24小时的余额记录。查询数据参考中余额表现在的余额记录。存储在内存中供步骤S2判断。

[0064] S2:根据S0及S1中的结果在行为特征匹配映射查询其对应的结果,对银行用户是否为黑客进行判别。

[0065] 具体地,针对单独的客户信息编号最近24小时的交易数量超过1万笔,则该客户为黑客。再比如:最近24小时的转入,转出金额统超过100万的银行用户、使用的IP地址超过5个的银行用户、转入,转出金额,与余额计算不匹配的银行用户、使用的他人账号数量超过5个的银行用户以及交易金额为负数交易成功的银行用户,均冻结其账户互联网交易功能,提示用户需要去柜面解冻,才能继续交易。并显示所有被封禁的客户信息编号,以及被冻结的原因。凡是被解冻过的客户信息编号,均自动加入客户信息编号白名单。总的决策判断的公式如下:

[0066] [(金额,账号异常的账户)-(经过确认的正常的异常业务交易)-(经过确认的正常账户)]×[异常账户的最近24小时的金额变动等情况]=(黑客账户)×(自动冻结等相关处理)。

[0067] 上述方法具体使用场景如下:业务运维人员,在每天晚上12点左右,可以在结果显示界面看到前一天的统计数据,以及已经被冻结的客户信息编号,并对存在疑问的被冻结的客户信息编号实施人工确认并解冻。对于金额统计不连续的,以及负金额成功交易,立即找相关安全测试人员以及开发人员确认交易是否存在安全漏洞。并维护,业务编号白名单;

维护客户信息编号白名单。通过上述技术手段，可以在黑客对银行系统实施探索阶段，就进行成功阻断，降低黑客通过大面积系统探索发现应用安全漏洞的可能性。黑客账户已经被冻结，无法进一步进行系统探索：在识别系统冻结账户后，黑客即使变化自己的IP也无法再使用这个账户实施探索，能有效减少黑客长期蹲守银行系统随意探索分析的情况。

[0068] 黑客提交经过篡改的请求尝试探索系统中是否存在安全漏洞：黑客要攻击成功银行系统，他必须要进行尝试，才能确认系统中是否存在漏洞。而篡改付款账号，跟把付款金额修改为0或者负，如果能交易成功就能迅速盗取银行资金，黑客一般都会喜欢先去使用窜改的方式去确认系统中这2种漏洞是否存在。在实际统计分析银行黑客数据的时候，这2种方式确实是占比非常大的系统探索行为。黑客希望账户能再次使用去柜面申请解冻，在于柜员沟通后。确认不再尝试去非法探索银行系统：一般尝试黑客行为是在认为别人不知道的情况会比较具有新鲜感，而如果被直接告知他不能进行非法的银行系统篡改探索行为，可以避免黑客在违法的道路上越走越远。

[0069] 从上述描述可知，本发明提供的基于行为特征的银行黑客用户判别方法，针对银行中的黑客的行为特征(通常对于银行系统特别喜欢进行尝试把付款账号修改成他人账号，转账、购买交易金额修改为0或者负金额的情况)，并根据该交易行为以及预设的行为特征匹配映射判别银行用户是否为黑客。进而进行自动预警，提醒运维人员进行相关紧急处理。从发明专利应用的实际效果看，本发明的效果和优点主要体现在如下：使用正常业务报错，发现黑客账号，并冻结账户：由于使用了正常业务报错日志，提前发现了黑客探索行为，并对其实施冻结措施，避免了黑客长期分析探索系统造成安全威胁的情况。冻结账户实现了自动化处理：分析处理黑客攻击账号，对运维人员造成较大工作负担。分析以及处理都实现自动化后会极大减轻运维人员负担。

[0070] 基于同一发明构思，本申请实施例还提供了基于行为特征的银行黑客用户判别装置，可以用于实现上述实施例所描述的方法，如下面的实施例。由于基于行为特征的银行黑客用户判别装置解决问题的原理与基于行为特征的银行黑客用户判别方法相似，因此基于行为特征的银行黑客用户判别装置的实施可以参见基于行为特征的银行黑客用户判别方法实施，重复之处不再赘述。以下所使用的，术语“单元”或者“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的系统较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

[0071] 本发明的实施例提供一种能够实现基于行为特征的银行黑客用户判别方法的基于行为特征的银行黑客用户判别装置的具体实施方式，参见图7，基于行为特征的银行黑客用户判别装置具体包括如下内容：

[0072] 交易行为获取单元10，用于获取银行用户的交易行为；

[0073] 黑客判别单元20，用于根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客。

[0074] 优选地，所述黑客识别单元20具体用于判别所述交易行为中交易金额是否为零或者负数；如果是，初步判别所述银行用户为黑客。

[0075] 优选地，所述黑客识别单元20具体还用于分别判别所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值；如果是，最终判别所述银行用户为所述黑客。

[0076] 参见图8，优选地，基于行为特征的银行黑客用户判别装置还包括：

[0077] 映射生成单元30，用于根据所述交易行为以及其交易金额是否为零或者负数的判别结果，以及所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值的判别结果，生成所述交易行为与黑客判别结果的行为特征匹配映射。

[0078] 从上述描述可知，本发明提供的基于行为特征的银行黑客用户判别装置，针对银行中的黑客的行为特征(通常对于银行系统特别喜欢进行尝试把付款账号修改成他人账号，转账、购买交易金额修改为0或者负金额的情况)，并根据该交易行为以及预设的行为特征匹配映射判别银行用户是否为黑客。进而进行自动预警，提醒运维人员进行相关紧急处理。从发明专利应用的实际效果看，本发明的效果和优点主要体现在如下：使用正常业务报错，发现黑客账号，并冻结账户：由于使用了正常业务报错日志，提前发现了黑客探索行为，并对其实施冻结措施，避免了黑客长期分析探索系统造成安全威胁的情况。冻结账户实现了自动化处理：分析处理黑客攻击账号，对运维人员造成较大工作负担。分析以及处理都实现自动化后会极大减轻运维人员负担。

[0079] 本申请的实施例还提供能够实现上述实施例中的基于行为特征的银行黑客用户判别方法中全部步骤的一种电子设备的具体实施方式，参见图9，电子设备具体包括如下内容：

[0080] 处理器(processor)1201、存储器(memory)1202、通信接口(Communications Interface)1203和总线1204；

[0081] 其中，处理器1201、存储器1202、通信接口1203通过总线1204完成相互间的通信；通信接口1203用于实现服务器端设备、记录设备以及用户端设备等相关设备之间的信息传输。

[0082] 处理器1201用于调用存储器1202中的计算机程序，处理器执行计算机程序时实现上述实施例中的基于行为特征的银行黑客用户判别方法中的全部步骤，例如，处理器执行计算机程序时实现下述步骤：

[0083] 步骤100：获取银行用户的交易行为。

[0084] 步骤200：根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客。

[0085] 从上述描述可知，本申请实施例中的电子设备，针对银行中的黑客的行为特征(通常对于银行系统特别喜欢进行尝试把付款账号修改成他人账号，转账、购买交易金额修改为0或者负金额的情况)，并根据该交易行为以及预设的行为特征匹配映射判别银行用户是否为黑客。进而进行自动预警，提醒运维人员进行相关紧急处理。从发明专利应用的实际效果看，本发明的效果和优点主要体现在如下：使用正常业务报错，发现黑客账号，并冻结账户：由于使用了正常业务报错日志，提前发现了黑客探索行为，并对其实施冻结措施，避免了黑客长期分析探索系统造成安全威胁的情况。冻结账户实现了自动化处理：分析处理黑客攻击账号，对运维人员造成较大工作负担。分析以及处理都实现自动化后会极大减轻运维人员负担。

[0086] 本申请的实施例还提供能够实现上述实施例中的基于行为特征的银行黑客用户判别方法中全部步骤的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，该计算机程序被处理器执行时实现上述实施例中的基于行为特征的银行黑客用户判别方法的全部步骤，例如，处理器执行计算机程序时实现下述步骤：

[0087] 步骤100:获取银行用户的交易行为。

[0088] 步骤200:根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客。

[0089] 从上述描述可知,本申请实施例中的计算机可读存储介质,针对银行中的黑客的行为特征(通常对于银行系统特别喜欢进行尝试把付款账号修改成他人账号,转账、购买交易金额修改为0或者负金额的情况),并根据该交易行为以及预设的行为特征匹配映射判别银行用户是否为黑客。进而进行自动预警,提醒运维人员进行相关紧急处理。从发明专利应用的实际效果看,本发明的效果和优点主要体现在如下:使用正常业务报错,发现黑客账号,并冻结账户:由于使用了正常业务报错日志,提前发现了黑客探索行为,并对其实施冻结措施,避免了黑客长期分析探索系统造成安全威胁的情况。冻结账户实现了自动化处理:分析处理黑客攻击账号,对运维人员造成较大工作负担。分析以及处理都实现自动化后会极大减轻运维人员负担。

[0090] 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,对于硬件+程序类实施例而言,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。

[0091] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的或者可能是有利的。

[0092] 虽然本申请提供了如实施例或流程图的方法操作步骤,但基于常规或者无创造性的劳动可以包括更多或者更少的操作步骤。实施例中列举的步骤顺序仅仅为众多步骤执行顺序中的一种方式,不代表唯一的执行顺序。在实际中的装置或客户端产品执行时,可以按照实施例或者附图所示的方法顺序执行或者并行执行(例如并行处理器或者多线程处理的环境)。

[0093] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0094] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0095] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指

令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0096] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0097] 本发明中应用了具体实施例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

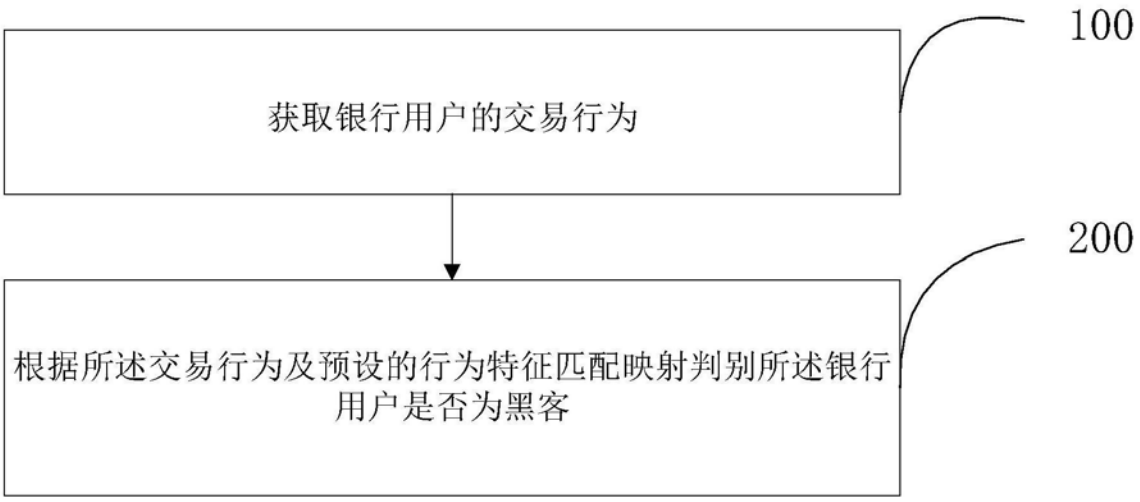

100
获取银行用户的交易行为
200
根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客

图1

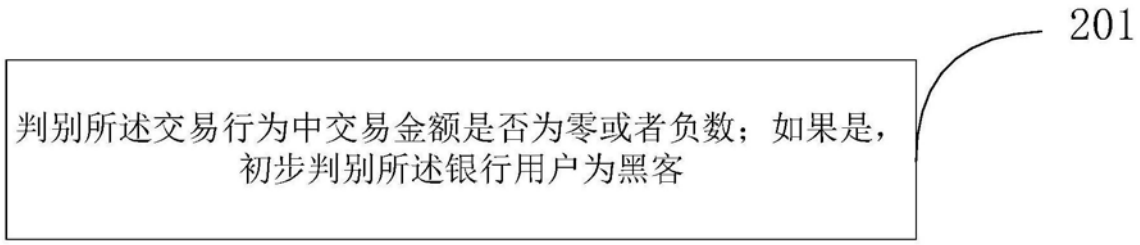

201
判别所述交易行为中交易金额是否为零或者负数；如果是，初步判别所述银行用户为黑客

图2

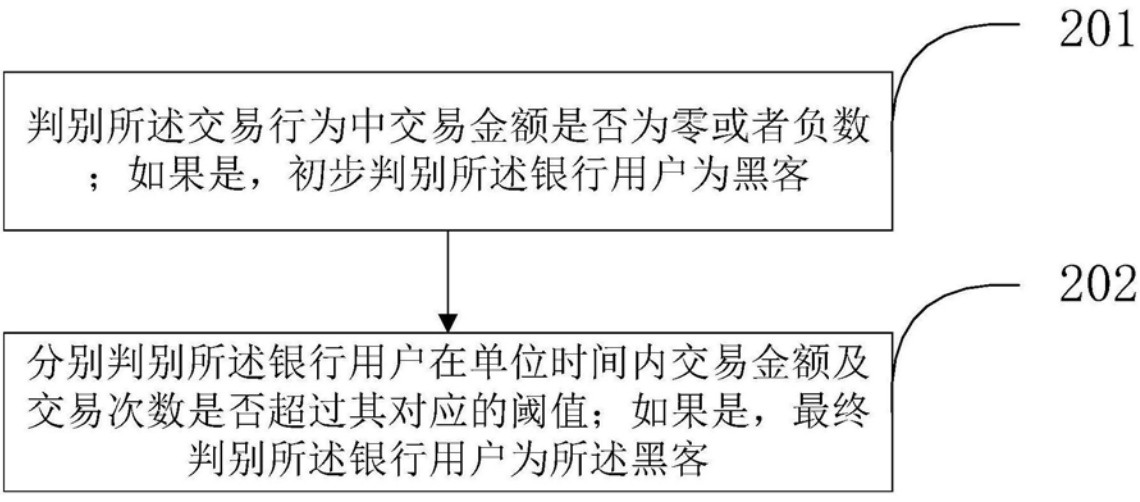

201
判别所述交易行为中交易金额是否为零或者负数；如果是，初步判别所述银行用户为黑客
202
分别判别所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值；如果是，最终判别所述银行用户为所述黑客

图3

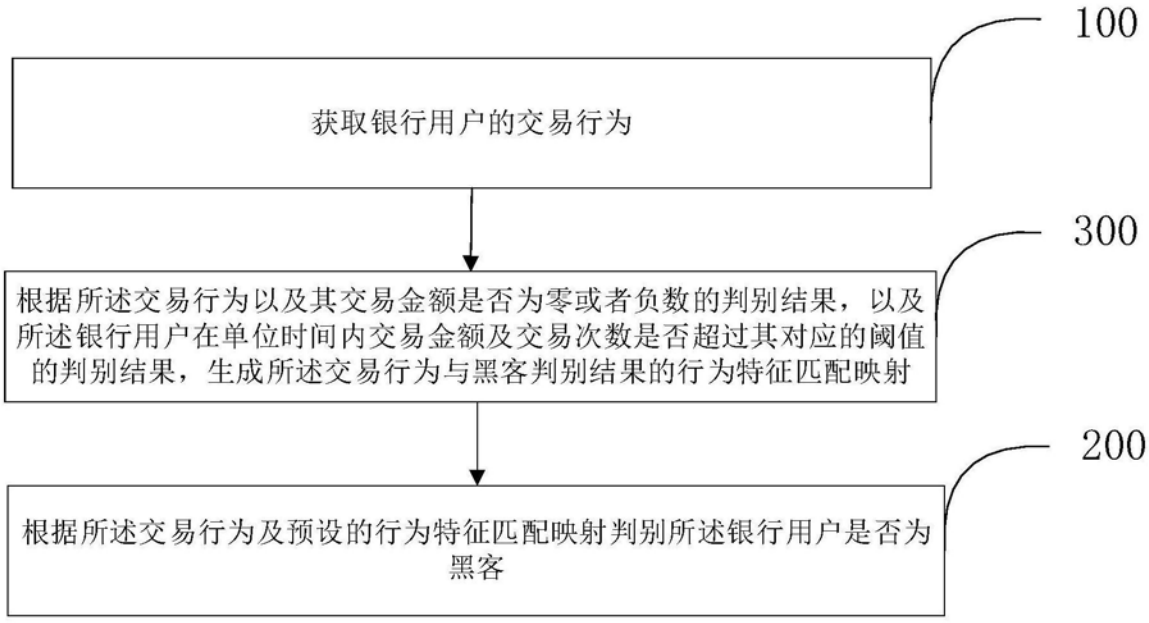

100
获取银行用户的交易行为
300
根据所述交易行为以及其交易金额是否为零或者负数的判别结果，以及所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值的判别结果，生成所述交易行为与黑客判别结果的行为特征匹配映射
200
根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客

图4

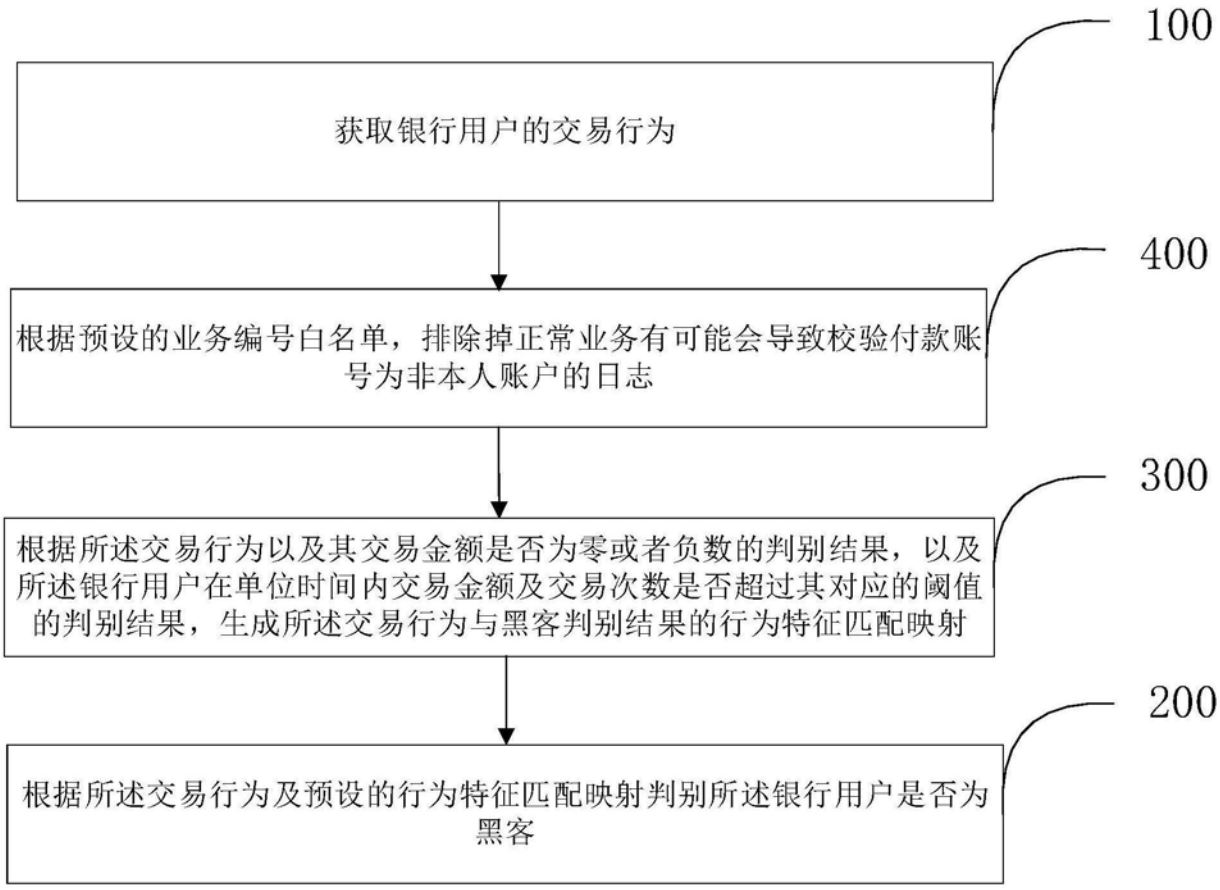

100
获取银行用户的交易行为
400
根据预设的业务编号白名单，排除掉正常业务有可能会导致校验付款账号为非本人账户的日志
300
根据所述交易行为以及其交易金额是否为零或者负数的判别结果，以及所述银行用户在单位时间内交易金额及交易次数是否超过其对应的阈值的判别结果，生成所述交易行为与黑客判别结果的行为特征匹配映射
200
根据所述交易行为及预设的行为特征匹配映射判别所述银行用户是否为黑客

图5

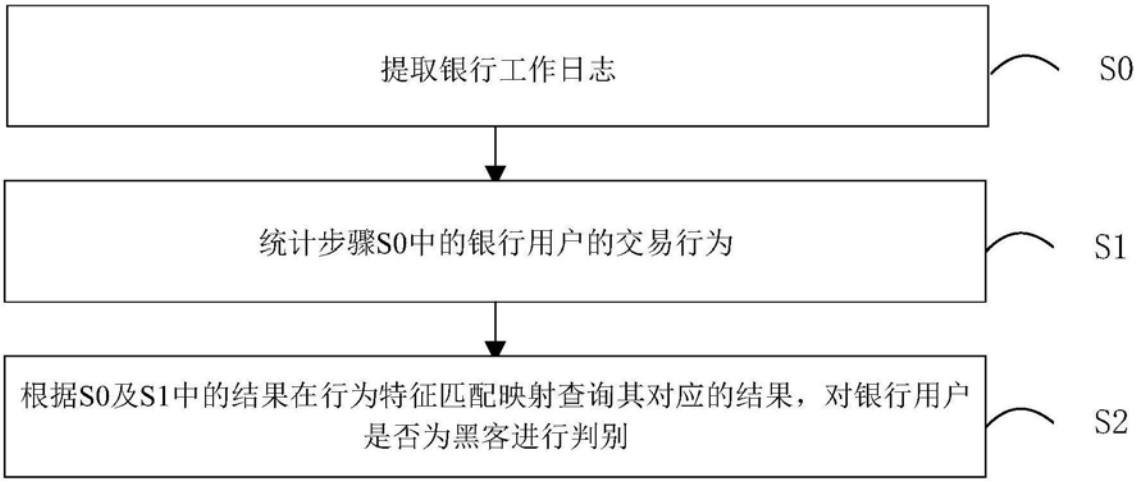

提取银行工作日志
S0
统计步骤S0中的银行用户的交易行为
S1
根据S0及S1中的结果在行为特征匹配映射查询其对应的结果，对银行用户是否为黑客进行判别
S2

图6

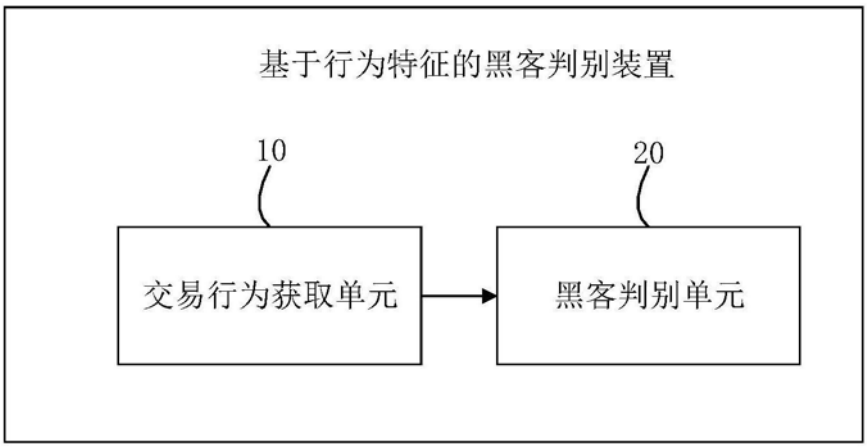

基于行为特征的黑客判别装置
10
20
交易行为获取单元
黑客判别单元

图7

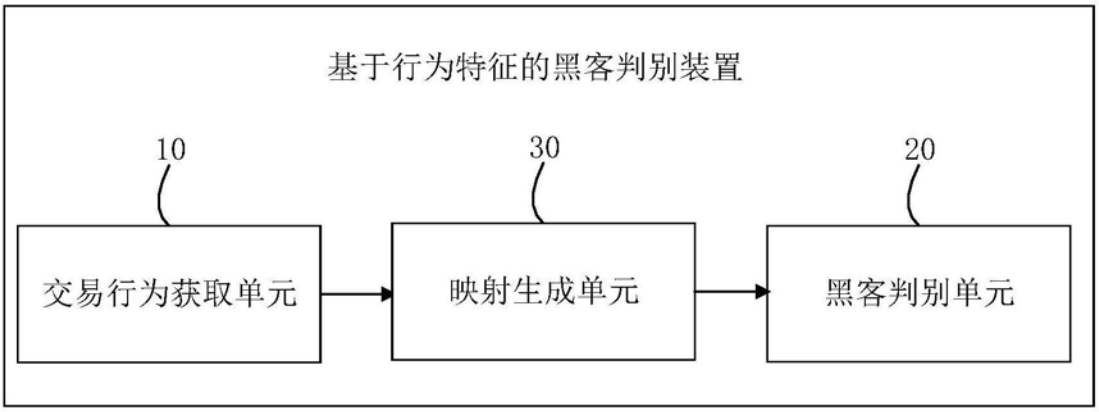

基于行为特征的黑客判别装置
10
30
20
交易行为获取单元
映射生成单元
黑客判别单元

图8

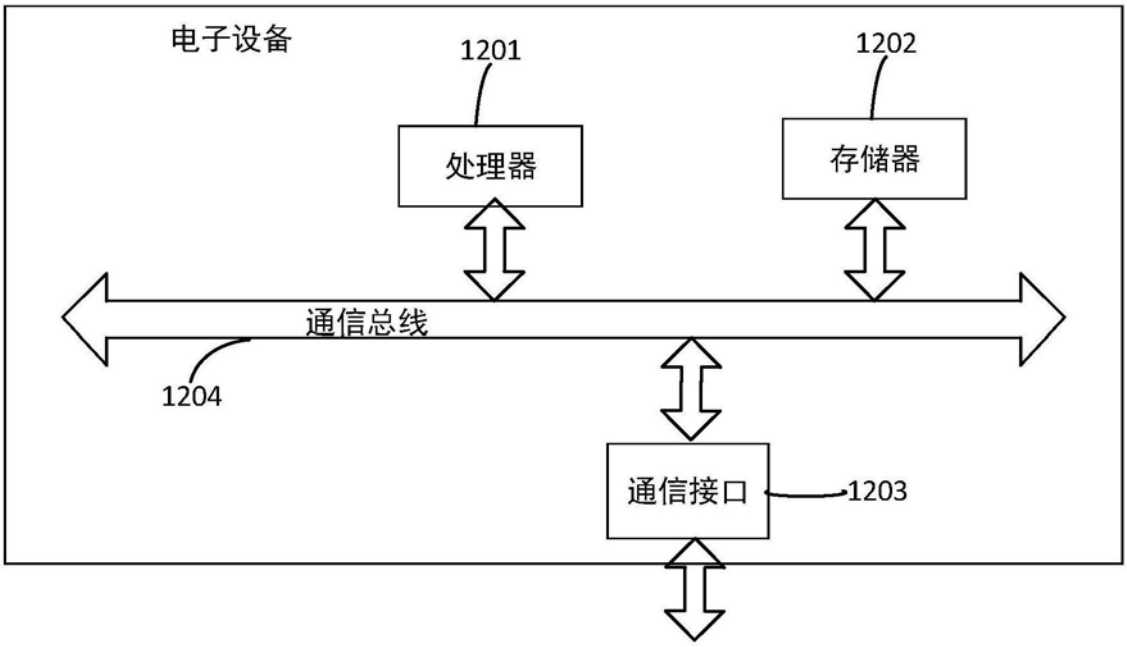


图9