(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 113360354 A
(43)申请公布日 2021.09.07

(21)申请号 202110589466.X

(22)申请日 2021.05.27

(71)申请人 广州品粤信息科技有限公司
地址 510000 广东省广州市花都区金熙二街1号1013房
申请人 高永

(72)发明人 高永

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 梁爽

(51)Int.Cl.
G06F 11/34(2006.01)
G06F 11/30(2006.01)
G06K 9/62(2006.01)

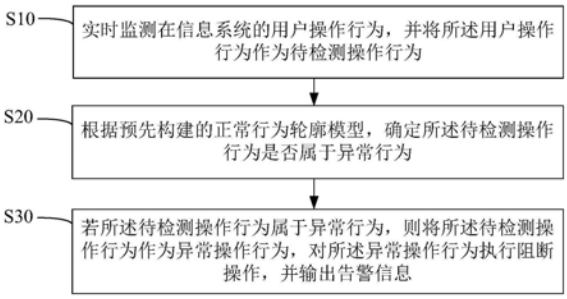
权利要求书2页 说明书10页 附图2页

(54)发明名称

用户操作行为监控方法、装置、设备及可读存储介质

(57)摘要

本发明公开了一种用户操作行为监控方法、装置、设备及可读存储介质，该用户操作行为监控方法包括以下步骤：实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为；根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为；若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息。本发明实现了对信息系统实时产生的用户操作行为进行检测，监测信息系统是否产生异常操作行为，从而可以抵御来源于内部的攻击行为，解决了现有的信息系统无法抵御来源于内部的攻击的技术问题。



CN 113360354 A

1.一种用户操作行为监控方法,其特征在于,所述用户操作行为监控方法包括以下步骤:

实时监测在信息系统的用户操作行为,并将所述用户操作行为作为待检测操作行为;

根据预先构建的正常行为轮廓模型,确定所述待检测操作行为是否属于异常行为;

若所述待检测操作行为属于异常行为,则将所述待检测操作行为作为异常操作行为,对所述异常操作行为执行阻断操作,并输出告警信息。

2.如权利要求1所述的用户操作行为监控方法,其特征在于,所述根据预先构建的正常行为轮廓模型,确定所述待检测操作行为是否属于异常行为的步骤之前,还包括:

采集所述信息系统中与用户操作行为相关的系统运行数据,其中,所述系统运行数据包括信息系统操作日志、数据库连接日志、WEB系统访问日志和操作系统访问日志;

对所述系统运行数据执行清洗操作,确定用户操作行为数据,并将所述用户操作行为数据存储于所述信息系统的存储模块中;

根据所述用户操作行为数据,构建正常行为轮廓模型。

3.如权利要求2所述的用户操作行为监控方法,其特征在于,所述清洗操作包括有效性的验证操作和标准化操作,所述对所述系统运行数据执行清洗操作,确定用户操作行为数据的步骤包括:

对所述系统运行数据执行有效性的验证操作,并基于所述有效性的验证操作筛选出所述系统运行数据中的有效数据;

对所述有效数据执行标准化操作,确定用户操作行为数据。

4.如权利要求3所述的用户操作行为监控方法,其特征在于,所述标准化操作包括分组操作和排序操作,所述对所述有效数据执行标准化操作,确定用户操作行为数据的步骤包括:

按照用户ID对所述有效数据执行分组操作,得到不同用户ID对应的分组结果;

按照时间顺序对所述分组结果执行排序操作,得到用户操作行为数据。

5.如权利要求2所述的用户操作行为监控方法,其特征在于,所述根据所述用户操作行为数据,构建正常行为轮廓模型的步骤包括:

定时从所述存储模块中获取用户操作行为数据,构建第一正常行为轮廓模型;

若存在上一次训练得到的第二正常行为轮廓模型,则根据所述第一正常行为轮廓模型和所述第二正常行为轮廓模型,修正所述第一正常行为轮廓模型的残差,得到正常行为轮廓模型。

6.如权利要求1所述的用户操作行为监控方法,其特征在于,所述根据预先构建的正常行为轮廓模型,确定所述待检测操作行为是否属于异常行为的步骤之前,还包括:

获取当前的正常行为轮廓模型对应的建立时间以及当前的系统时间;

若所述建立时间与所述系统时间之差的绝对值大于预设阈值,则重新获取系统行为数据;

根据所述系统行为数据,构建正常行为轮廓模型。

7.如权利要求1至6任一项所述的用户操作行为监控方法,其特征在于,所述根据预先构建的正常行为轮廓模型,确定所述待检测操作行为是否属于异常行为的步骤包括:

根据预先构建的正常行为轮廓模型,计算所述待检测操作行为和所述正常行为轮廓模

型对应的正常行为轮廓之间的相似度；

若所述相似度大于或等于预设的相似度阈值，则确定所述待检测操作行为属于正常行为；

若所述相似度小于所述预设的相似度阈值，则确定所述待检测操作行为属于异常行为。

8.一种用户操作行为监控装置，其特征在于，所述用户操作行为监控装置包括：

第一检测模块，用于实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为；

第二检测模块，用于根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为；

告警模块，用于若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息。

9.一种用户操作行为监控设备，其特征在于，所述用户操作行为监控设备包括：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用户操作行为监控程序，所述用户操作行为监控程序被所述处理器执行时实现如权利要求1至7中任一项所述的用户操作行为监控方法的步骤。

10.一种可读存储介质，其特征在于，所述可读存储介质上存储有用户操作行为监控程序，所述用户操作行为监控程序被处理器执行时实现如权利要求1至7中任一项所述的用户操作行为监控方法的步骤。

用户操作行为监控方法、装置、设备及可读存储介质

技术领域

[0001] 本发明涉及信息系统监控技术领域，尤其涉及一种用户操作行为监控方法、装置、设备及可读存储介质。

背景技术

[0002] 信息系统作为数据的管理和存储系统，往往承载了一些企业/部门的核心数据，比如账户信息、生产数据、营业数据等，这些信息一旦被恶意访问、泄露或篡改，会造成企业的经济损失，甚至影响社会安定。

[0003] 长期以来，企业组织往往集中主要的精力和资源应对来自信息系统外部的威胁，凭借防火墙、信息加密、访问控制等网络安全技术，有效地抵御了大部分来自企业外部的攻击。然而内部威胁的攻击者是来自安全边界以内的，内部威胁的攻击者可以躲避防火墙等外部安全设备的检测，因此现有的信息系统无法抵御来源于内部的攻击，需要更加有效的手段来检测内部威胁。

[0004] 全球企业每年因为内部用户蓄意破坏或无意失职而造成的损失所占比重越来越大，内部威胁日益成为企业安全关注的重点。2015年的网络犯罪调查显示，23％的电子犯罪事件来自于内部人员，45％的受访者认为内部人员攻击造成的损害要远高于外部攻击带来的损害。以及，《2017年数据泄露调查报告》指出，15％的数据泄露是由内部人员造成的。以及，2018年的一个在线调查显示，53％的组织确认过去一年内遭受过内部威胁攻击，29％的组织认为内部威胁攻击越来越频繁。

[0005] 据调查，对一个企业而言，所有计算机安全事件中来自企业内部信息(数据)泄漏或篡改造成的经济损失连续5年排在第一位。在众多的安全事件中，最主要、也是最危险的安全事件是来源于企业内部的信息泄漏。由于员工的有意或无意造成的信息(数据)泄漏所产生的危害极大且防不胜防，它可导致企业的核心竞争力下降，造成企业的声誉损害，可见信息系统内部安全问题是目前亟须解决的首要问题。

[0006] 上述内容仅用于辅助理解本发明的技术方案，并不代表承认上述内容是现有技术。

发明内容

[0007] 本发明的主要目的在于提供一种用户操作行为监控方法、装置、设备及可读存储介质，旨在解决现有的信息系统无法抵御来源于内部的攻击的技术问题。

[0008] 为实现上述目的，本发明提供一种用户操作行为监控方法，所述用户操作行为监控方法包括以下步骤：

[0009] 实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为；

[0010] 根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为；

[0011] 若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息。

[0012] 可选地，所述根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为的步骤之前，还包括：

[0013] 采集所述信息系统中与用户操作行为相关的系统运行数据，其中，所述系统运行数据包括信息系统操作日志、数据库连接日志、WEB系统访问日志和操作系统访问日志；

[0014] 对所述系统运行数据执行清洗操作，确定用户操作行为数据，并将所述用户操作行为数据存储于所述信息系统的存储模块中；

[0015] 根据所述用户操作行为数据，构建正常行为轮廓模型。

[0016] 可选地，所述清洗操作包括有效性的验证操作和标准化操作，所述对所述系统运行数据执行清洗操作，确定用户操作行为数据的步骤包括：

[0017] 对所述系统运行数据执行有效性的验证操作，并基于所述有效性的验证操作筛选出所述系统运行数据中的有效数据；

[0018] 对所述有效数据执行标准化操作，确定用户操作行为数据。

[0019] 可选地，所述标准化操作包括分组操作和排序操作，所述对所述有效数据执行标准化操作，确定用户操作行为数据的步骤包括：

[0020] 按照用户ID对所述有效数据执行分组操作，得到不同用户ID对应的分组结果；

[0021] 按照时间顺序对所述分组结果执行排序操作，得到用户操作行为数据。

[0022] 可选地，所述根据所述用户操作行为数据，构建正常行为轮廓模型的步骤包括：

[0023] 定时从所述存储模块中获取用户操作行为数据，构建第一正常行为轮廓模型；

[0024] 若存在上一次训练得到的第二正常行为轮廓模型，则根据所述第一正常行为轮廓模型和所述第二正常行为轮廓模型，修正所述第一正常行为轮廓模型的残差，得到正常行为轮廓模型。

[0025] 可选地，所述根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为的步骤之前，还包括：

[0026] 获取当前的正常行为轮廓模型对应的建立时间以及当前的系统时间；

[0027] 若所述建立时间与所述系统时间之差的绝对值大于预设阈值，则重新获取系统行为数据；

[0028] 根据所述系统行为数据，构建正常行为轮廓模型。

[0029] 可选地，所述根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为的步骤包括：

[0030] 根据预先构建的正常行为轮廓模型，计算所述待检测操作行为和所述正常行为轮廓模型对应的正常行为轮廓之间的相似度；

[0031] 若所述相似度大于或等于预设的相似度阈值，则确定所述待检测操作行为属于正常行为；

[0032] 若所述相似度小于所述预设的相似度阈值，则确定所述待检测操作行为属于异常行为。

[0033] 此外，为实现上述目的，本发明还提供一种用户操作行为监控装置，所述用户操作行为监控装置包括：

[0034] 第一检测模块，用于实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为；

[0035] 第二检测模块，用于根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为；

[0036] 告警模块，用于若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息。

[0037] 此外，为实现上述目的，本发明还提供一种用户操作行为监控设备，所述用户操作行为监控设备包括：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用户操作行为监控程序，所述用户操作行为监控程序被所述处理器执行时实现如上述的用户操作行为监控方法的步骤。

[0038] 此外，为实现上述目的，本发明还提供一种可读存储介质，所述可读存储介质上存储有用户操作行为监控程序，所述用户操作行为监控程序被处理器执行时实现如上述的用户操作行为监控方法的步骤。

[0039] 本发明通过实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为；根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为；若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息。在本实施例中，通过对信息系统进行实时监测，以监测信息系统中所产生的用户操作行为，并将用户操作行为作为待检测操作行为，之后，通过正常行为轮廓模型对待检测操作行为进行检测，以判断待检测操作行为是否属于异常行为，若待检测操作行为属于异常行为，则对待检测操作行为执行阻断操作，并输出告警信息，从而可以对信息系统实时产生的用户操作行为进行检测，监测信息系统是否产生异常操作行为，从而可以抵御来源于内部的攻击行为，解决了现有的信息系统无法抵御来源于内部的攻击的技术问题。

附图说明

[0040] 图1是本发明实施例方案涉及的硬件运行环境的用户操作行为监控设备结构示意图；

[0041] 图2为本发明用户操作行为监控方法第一实施例的流程示意图；

[0042] 图3为本发明用户操作行为监控方法第二实施例的流程示意图。

[0043] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0044] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0045] 如图1所示，图1是本发明实施例方案涉及的硬件运行环境的用户操作行为监控设备结构示意图。

[0046] 本发明实施例用户操作行为监控设备可以是PC，也可以是智能手机、平板电脑、电子书阅读器、MP3(Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面3)播放器、MP4(Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面4)播放器、便携计算机等具有显示功能的可移动式终端设备。

[0047] 如图1所示，该用户操作行为监控设备可以包括：处理器1001，例如CPU，网络接口1004，用户接口1003，存储器1005，通信总线1002。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)、输入单元比如键盘(Keyboard)，可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器，也可以是稳定的存储器(non-volatile memory)，例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0048] 可选地，用户操作行为监控设备还可以包括摄像头、RF(Radio Frequency，射频)电路，传感器、音频电路、WiFi模块等等。其中，传感器比如光传感器、运动传感器以及其他传感器。具体地，光传感器可包括环境光传感器及接近传感器，其中，环境光传感器可根据环境光线的明暗来调节显示屏的亮度，接近传感器可在移动终端移动到耳边时，关闭显示屏和/或背光。作为运动传感器的一种，重力加速度传感器可检测各个方向上(一般为三轴)加速度的大小，静止时可检测出重力的大小及方向，可用于识别移动终端姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等；当然，用户操作行为监控设备还可配置陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

[0049] 本领域技术人员可以理解，图1中示出的用户操作行为监控设备结构并不构成对用户操作行为监控设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0050] 如图1所示，作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及用户操作行为监控程序。

[0051] 在图1所示的用户操作行为监控设备中，网络接口1004主要用于连接后台服务器，与后台服务器进行数据通信；用户接口1003主要用于连接客户端(用户端)，与客户端进行数据通信；而处理器1001可以用于调用存储器1005中存储的用户操作行为监控程序。

[0052] 在本实施例中，用户操作行为监控设备包括：存储器1005、处理器1001及存储在所述存储器1005上并可在所述处理器1001上运行的用户操作行为监控程序，其中，处理器1001调用存储器1005中存储的用户操作行为监控程序时，并执行以下操作：

[0053] 实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为；

[0054] 根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为；

[0055] 若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息。

[0056] 进一步地，处理器1001可以调用存储器1005中存储的用户操作行为监控程序，还执行以下操作：

[0057] 采集所述信息系统中与用户操作行为相关的系统运行数据，其中，所述系统运行数据包括信息系统操作日志、数据库连接日志、WEB系统访问日志和操作系统访问日志；

[0058] 对所述系统运行数据执行清洗操作，确定用户操作行为数据，并将所述用户操作行为数据存储于所述信息系统的存储模块中；

[0059] 根据所述用户操作行为数据，构建正常行为轮廓模型。

[0060] 进一步地，处理器1001可以调用存储器1005中存储的用户操作行为监控程序，还执行以下操作：

[0061] 对所述系统运行数据执行有效性的验证操作，并基于所述有效性的验证操作筛选出所述系统运行数据中的有效数据；

[0062] 对所述有效数据执行标准化操作，确定用户操作行为数据。

[0063] 进一步地，处理器1001可以调用存储器1005中存储的用户操作行为监控程序，还执行以下操作：

[0064] 按照用户ID对所述有效数据执行分组操作，得到不同用户ID对应的分组结果；

[0065] 按照时间顺序对所述分组结果执行排序操作，得到用户操作行为数据。

[0066] 进一步地，处理器1001可以调用存储器1005中存储的用户操作行为监控程序，还执行以下操作：

[0067] 定时从所述存储模块中获取用户操作行为数据，构建第一正常行为轮廓模型；

[0068] 若存在上一次训练得到的第二正常行为轮廓模型，则根据所述第一正常行为轮廓模型和所述第二正常行为轮廓模型，修正所述第一正常行为轮廓模型的残差，得到正常行为轮廓模型。

[0069] 进一步地，处理器1001可以调用存储器1005中存储的用户操作行为监控程序，还执行以下操作：

[0070] 获取当前的正常行为轮廓模型对应的建立时间以及当前的系统时间；

[0071] 若所述建立时间与所述系统时间之差的绝对值大于预设阈值，则重新获取系统行为数据；

[0072] 根据所述系统行为数据，构建正常行为轮廓模型。

[0073] 进一步地，处理器1001可以调用存储器1005中存储的用户操作行为监控程序，还执行以下操作：

[0074] 根据预先构建的正常行为轮廓模型，计算所述待检测操作行为和所述正常行为轮廓模型对应的正常行为轮廓之间的相似度；

[0075] 若所述相似度大于或等于预设的相似度阈值，则确定所述待检测操作行为属于正常行为；

[0076] 若所述相似度小于所述预设的相似度阈值，则确定所述待检测操作行为属于异常行为。

[0077] 本发明还提供一种用户操作行为监控方法，参照图2，图2为本发明用户操作行为监控方法第一实施例的流程示意图。

[0078] 步骤S10，实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为；

[0079] 本发明提出的用户操作行为监控方法应用于信息系统，信息系统一种是数据的管理和存储系统，用于所收集用户的数据进行管理以及存储，并且提供WEB前端的交互页面供用户往信息系统里输入相关的信息，例如，对于银行的交易系统，对银行用户的身份信息和银行账户信息进行管理以及存储的功能，或者企业的对员工个人信息的管理系统或者研发数据的管理系统等等，上述银行的交易系统、企业的员工个人信息管理系统以及研发数据

的管理系统等均属于信息系统。在实际的情况中，通常各企业对应的企业终端会建立诸如防火墙等安全系统来为信息系统抵御来自外界攻击者的攻击，内部威胁攻击中，攻击者来自企业内部，攻击行为往往发生在工作时间，恶意行为嵌入大量正常数据中，增加了数据挖掘分析的难度。同时，内部攻击者往往具有组织安全防御机制的相关知识，会采取措施规避安全检测，因此往往难以检测到信息系统中触发的存在安全威胁的攻击操作。

[0080] 单用户行为会呈现出明显的规律性和偶然性，本发明通过为用户操作行为建立正常行为轮廓，将信息系统的用户操作行为与正常行为轮廓进行比较，根据用户操作行为和正常行为轮廓的偏离程度来识别异常操作行为，如果偏差足够大，则认为发生异常，优势在于可以识别未知的风险。

[0081] 用户在信息系统中访问文件、使用应用程序、获取内部资源、使用设施设备的时间和频率等操作会形成一个相对固定的行为模式。相同角色、相同工作部门的用户的工作性质相近，其行为模式具有一定的相似性。若用户操作行为明显偏离正常模式，则表示该用户有意隐藏其恶意行为或存在违反企业相关政策违规获取工作需求之外信息的行为。

[0082] 用户每天进行大量业务操作，因此用户操作行为具有稳定性和固定性。采用隐马尔可夫模型整合多类行为数据，提取用户行为序列，可以揭示隐藏在行为背后的业务逻辑，预测用户操作行为的转移概率，刻画用户操作行为模式。根据转移概率的大小可以判定用户操作行为偏离正常行为特征的程度。

[0083] 在本实施例中，对信息系统中的用户操作行为进行实时监测，并获取用户在信息系统当前的用户操作行为，将用户操作行为作为待检测操作行为。具体地，信息系统实时监测系统中的用户操作行为，以在信息系统上存在用户的执行操作时，获取当前的执行操作对应的操作数据，其中，用户操作行为是在预设时间范围内的相关操作数据。也就是说，当有用户在系统上触发执行操作时，信息系统会对用户在当前时间段发生的系列的操作数据记录下来。

[0084] 步骤S20，根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为；

[0085] 在本实施例中，对于信息系统，实时记录信息系统的用户操作数据，并将用户操作数据存储至信息系统的存储模块中，并将所监测的用户操作数据作为历史操作数据，需要说明的是，历史操作数据用于构建正常行为轮廓模型。因此，信息系统可以往存储模块中存储入最新的用户操作数据，可以随时从存储模操作块中获取用户的历史数据来构建和更新正常行为轮廓模型。在得到待检测操作行为后，将待检测操作行为输入至正常行为轮廓模型，以通过预先构建的正常行为轮廓模型，检测待检测操作行为是否属于异常行为。

[0086] 需要说明的是，对用户正常行为进行画像，并加以对比分析，可以有效检测用户行为模式变化。用户对信息系统的访问模式、数据库操作、主机登陆等操作行为，都可以用来描述该用户的历史性、习惯性行为。通过自动化提取用户操作的行为特征，利用一分类支持向量机集群对用户操作行为进行构建用户行为细节画像即正常行为轮廓，可以判断用户操作行为是否与历史操作行为习惯存在明显差异。

[0087] 进一步地，所述根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为的步骤包括：

[0088] 步骤S21，根据预先构建的正常行为轮廓模型，计算所述待检测操作行为和所述正

常行为轮廓模型对应的正常行为轮廓之间的相似度；

[0089] 步骤S22，若所述相似度大于或等于预设的相似度阈值，则确定所述待检测操作行为属于正常行为；

[0090] 步骤S23，若所述相似度小于所述预设的相似度阈值，则确定所述待检测操作行为属于异常行为。

[0091] 在本实施例中，得到待检测操作行为后，将待检测操作行为输入至正常行为轮廓模型，以通过正常行为轮廓模型计算待检测操作行为和正常行为轮廓模型所包含的正常行为轮廓之间的相似度，以根据待检测操作行为和正常行为轮廓之间的相似度来判断待检测操作行为的类型，即判断待检测操作行为属于异常行为还是属于正常行为。具体地，计算到待检测操作行为和正常行为轮廓之间的相似度后，将该相似度和相似度阈值进行比较，若相似度大于或者等于相似度阈值，则判定待检测操作行为属于正常行为；若相似度小于相似度阈值，则判定待检测操作行为属于异常行为。其中，相似度阈值代表属于正常行为与属于异常行为之间的临界值。

[0092] 步骤S30，若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息。

[0093] 在本实施例中，若检测到待检测操作属于异常行为，则将待检测操作行为标识成异常操作行为，并将待检测操作对应的用户ID标识成异常ID，并对异常操作行为执行阻断操作，同时向信息系统的管理模块输出告警信息，以供管理员可以通过告警信息对异常操作行为执行管理员权限的阻断操作。其中，告警信息包含产生异常操作行为的用户ID和该用户ID的异常操作行为，阻断操作可以是限制待检测操作行为对应的用户ID的操作，还可以是断开发生待检测操作行为的主机端的网络连接。

[0094] 本实施例提出的用户操作行为监控方法，通过实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为；根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为；若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息。在本实施例中，通过对信息系统进行实时监测，以监测信息系统中所产生的用户操作行为，并将用户操作行为作为待检测操作行为，之后，通过正常行为轮廓模型对待检测操作行为进行检测，以判断待检测操作行为是否属于异常行为，若待检测操作行为属于异常行为，则对待检测操作行为执行阻断操作，并输出告警信息，从而可以对信息系统实时产生的用户操作行为进行检测，监测信息系统是否产生异常操作行为，从而可以抵御来源于内部的攻击行为，解决了现有的信息系统无法抵御来源于内部的攻击的技术问题。

[0095] 基于第一实施例，提出本发明用户操作行为监控方法的第二实施例，参照图3，在本实施例中，步骤S20之前，还包括：

[0096] 步骤S40，采集所述信息系统中与用户操作行为相关的系统运行数据，其中，所述系统运行数据包括信息系统操作日志、数据库连接日志、WEB系统访问日志和操作系统访问日志；

[0097] 步骤S50，对所述系统运行数据执行清洗操作，确定用户操作行为数据，并将所述用户操作行为数据存储于所述信息系统的存储模块中；

[0098] 步骤S60，根据所述用户操作行为数据，构建正常行为轮廓模型。

[0099] 在本实施例中，在构建正常行为轮廓模型之前，需要进行采集信息系统中的数据，以通过所采集的数据进行构建正常行为轮廓模型。具体地，采集信息系统中与用户操作行为相关的系统运行数据，并将系统运行数据存储至存储模块中，以从存储模块中依次获取部分的系统运行数据来执行预处理操作，预处理操作即清洗操作；对系统运行数据执行清洗操作，以筛选出系统运行数据中有效的数据，在对系统运行数据清洗完成后，得到清洗系统运行数据后对应的用户操作行为数据，之后再将用户操作行为数据存储于信息系统的存储模块中，以供按需求从存储模块中获取用户操作行为数据来构建正常轮廓模型。其中，用户操作行为数据即为清洗完成后的系统运行数据，系统运行数据包括信息系统操作日志、数据库连接日志、WEB系统访问日志和操作系统访问日志。

[0100] 进一步地，信息系统通过基于Java agent的APM在前端代码中自动嵌入JS脚本的方式来获取用户在WEB前端的操作行为数据，并以信息系统操作日志的方式存储下来，采集到的用户操作行为主要包括用户在Web页面上的鼠标点击、按钮组件获取等事件，采集相关日志发送到数据接收模块。通过数据库防火墙、数据库旁路审计、数据库主机探针等方式获取数据库连接日志。通过WEB LOG日志采集方式获取WEB系统访问日志，WEB系统访问日志包括：IIS、APACHE、NGINX、TOMCAT、WEBLOGIC、JETTY等WEB系统的访问日志。通过系统LOG日志采集、主机探针的方式获取操作系统访问日志。

[0101] 进一步地，清洗操作包括有效性的验证操作和标准化操作，对系统运行数据执行清洗操作具体包括：先对系统运行数据执行有效性的验证操作，并基于有效性的验证操作筛选出系统运行数据中的有效数据，以剔除系统运行数据中不规范的或者有错漏的数据；对有效数据执行标准化操作，确定用户操作行为数据。

[0102] 进一步地，所述标准化操作包括分组操作和排序操作，所述对所述有效数据执行标准化操作，确定用户操作行为数据的步骤包括：

[0103] 步骤S51，按照用户ID对所述有效数据执行分组操作，得到不同用户ID对应的分组结果；

[0104] 步骤S52，按照时间顺序对所述分组结果执行排序操作，得到用户操作行为数据。

[0105] 在本实施例中，标准化操作即对数据执行规范化的操作，以使数据能够用于构建正常行为轮廓模型，标准化操作包括分组操作和排序操作，对有效数据执行标准化操作具体包括：按照用户ID对有效数据执行分组操作，得到不同用户ID对应的分组结果，即分组结果是根据用户ID的不同进行分组的，分组结果中属于同一个用户ID的有效数据分为同一组；之后再对分好组的有效数据进行排序操作，排序操作为按照时间顺序进行排序，即按照时间顺序对分组后的有效数据执行排序操作，得到用户操作行为数据，具体地，按照时间顺序的时间先后分别对分组结果中的各组数据进行排序。

[0106] 进一步地，所述根据所述用户操作行为数据，构建正常行为轮廓模型的步骤包括：

[0107] 步骤S61，定时从所述存储模块中获取用户操作行为数据，构建第一正常行为轮廓模型；

[0108] 步骤S62，若存在上一次训练得到的第二正常行为轮廓模型，则根据所述第一正常行为轮廓模型和所述第二正常行为轮廓模型，修正所述第一正常行为轮廓模型的残差，得到正常行为轮廓模型。

[0109] 在本实施例中，在对系统运行数据清洗并将清洗后的系统运行数据存储至存储模

块中后，按照一定的时间间隔从存储模块中获取用户操作行为数据来构建正常行为轮廓模型，即定时从存储模块中获取用户操作行为数据，先构建第一正常行为轮廓模型；构建完成后，若信息系统存在上一次训练得到的第二正常行为轮廓模型，则获取上一次训练得到的第二正常行为轮廓模型，并根据第一正常行为轮廓模型的第一模型参数和第二正常行为轮廓模型的第二模型参数来修正第一正常行为轮廓模型的残差，也就是说，每次在构建正常行为轮廓模型时，均获取上一次构建的正常行为轮廓模型和本次构建的正常行为轮廓模型进行比较，从而考虑到了历史的正常行为轮廓模型，并根据历史的正常行为轮廓模型来修正本次构建的模型的模型参数，最终得到修正残差后的第一正常行为轮廓模型，即正常行为轮廓模型。

[0110] 进一步地，所述根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为的步骤之前，还包括：

[0111] 步骤S70，获取当前的正常行为轮廓模型对应的建立时间以及当前的系统时间；

[0112] 步骤S80，若所述建立时间与所述系统时间之差的绝对值大于预设阈值，则重新获取系统行为数据；

[0113] 步骤S90，根据所述系统行为数据，构建正常行为轮廓模型。

[0114] 在本实施例中，在对用户的待检测操作行为进行检测之前，获取信息系统当前的正常行为轮廓模型对应的建立时间以及当前的系统时间，并将建立时间以及系统时间进行比较，计算建立时间与系统时间之差的绝对值；若建立时间与系统时间之差的绝对值大于预设阈值，说明信息系统当前的正常行为轮廓模型已过期，那么重新获取系统中的用户操作行为数据来构建正常行为轮廓模型，因此在该用户还未建立正常行为轮廓模型或建立的正常行为轮廓模型已过期(建立时间与当前系统时间差距过大)，则触发学习模块重新获取系统行为数据，以根据最新的数据进行训练并建立正常行为轮廓模型，再进行对待检测操作行为的异常检测。其中，系统行为数据为信息系统的存储模块中所存储的用户操作行为数据。

[0115] 此外，本发明实施例还提出一种用户操作行为监控装置，所述用户操作行为监控装置包括：

[0116] 第一检测模块，用于实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为；

[0117] 第二检测模块，用于根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为；

[0118] 告警模块，用于若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息。

[0119] 此外，本发明实施例还提出一种可读存储介质，所述可读存储介质上存储有用户操作行为监控程序，所述用户操作行为监控程序被处理器执行时实现如上述中任一项所述的用户操作行为监控方法的步骤。

[0120] 本发明可读存储介质具体实施例与上述用户操作行为监控方法的各实施例基本相同，在此不再详细赘述。

[0121] 需要说明的是，在本文中，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、物品或者系统不仅包括那些要素，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、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0122] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0123] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0124] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

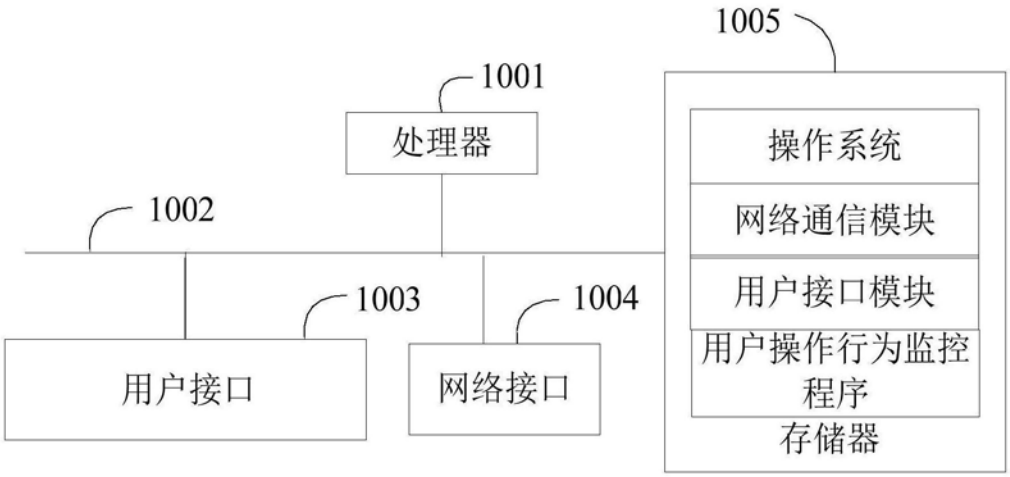

1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
1003
1004
用户操作行为监控程序
用户接口
网络接口
存储器

图1

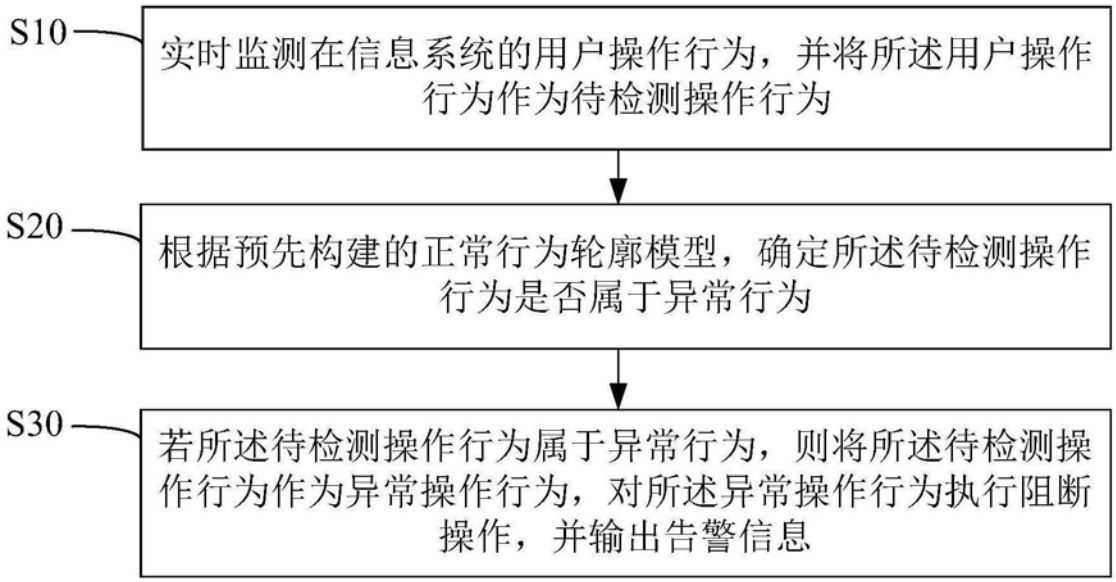

S10
实时监测在信息系统的用户操作行为，并将所述用户操作行为作为待检测操作行为
S20
根据预先构建的正常行为轮廓模型，确定所述待检测操作行为是否属于异常行为
S30
若所述待检测操作行为属于异常行为，则将所述待检测操作行为作为异常操作行为，对所述异常操作行为执行阻断操作，并输出告警信息

图2

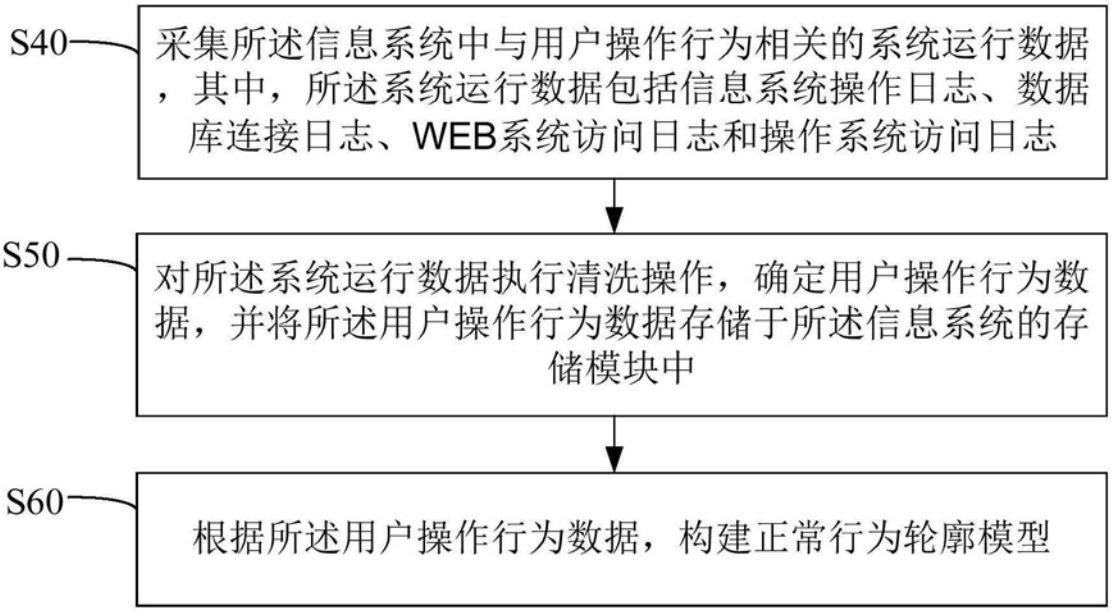

S40
采集所述信息系统中与用户操作行为相关的系统运行数据，其中，所述系统运行数据包括信息系统操作日志、数据库连接日志、WEB系统访问日志和操作系统访问日志
S50
对所述系统运行数据执行清洗操作，确定用户操作行为数据，并将所述用户操作行为数据存储于所述信息系统的存储模块中
S60
根据所述用户操作行为数据，构建正常行为轮廓模型

图3