



(21) 申请号 201980081446.2

(22) 申请日 2019.12.10

(65) 同一申请的已公布的文献号
申请公布号 CN 113168469 A

(43) 申请公布日 2021.07.23

(30) 优先权数据
16/215,251 2018.12.10 US

(85) PCT国际申请进入国家阶段日
2021.06.09

(86) PCT国际申请的申请数据
PCT/EP2019/084312 2019.12.10

(87) PCT国际申请的公布数据
W02020/120429 EN 2020.06.18

(73) 专利权人 比特梵德知识产权管理有限公司
地址 塞浦路斯尼科西亚

(72) 发明人 D·迪基乌 S·尼古拉
E·A·博辛恰努 S·N·扎姆菲尔
A·丁库 A·A·阿波斯托阿耶

(74) 专利代理机构 北京律盟知识产权代理有限公司 11287
专利代理师 张世俊

(51) Int.Cl.
H04L 9/40 (2022.01)
G06F 21/55 (2013.01)

(56) 对比文件
US 2012137367 A1, 2012.05.31
US 2014215618 A1, 2014.07.31
US 2016149936 A1, 2016.05.26
US 2016300049 A1, 2016.10.13
US 2016352759 A1, 2016.12.01
US 2017039198 A1, 2017.02.09
US 2017140384 A1, 2017.05.18
US 6526405 B1, 2003.02.25
US 7818797 B1, 2010.10.19
US 2018004961 A1, 2017.10.24

审查员 马铭泽

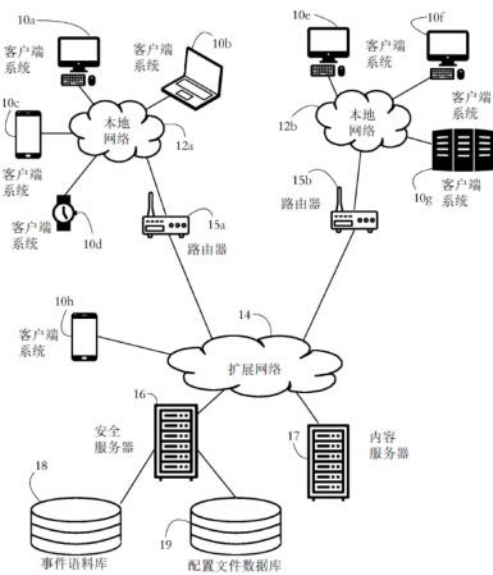
权利要求书4页 说明书16页 附图15页

(54) 发明名称

用于行为威胁检测的系统及方法

(57) 摘要

在一些实施例中,一种行为计算机安全系统保护客户端及网络使其免受例如恶意软件及入侵等的威胁。根据在客户端上发生的事件的训练语料库构建一组客户端配置文件,其中每一客户端配置文件表示受保护机器的子集,且每一客户端配置文件指示使用指派到所述客户端相应配置文件的所述机器的正常或基线模式。客户端配置文件可将具有类似事件统计的机器分组在一起。在训练之后,对照与客户端相关联的客户端配置文件选择性地分析在所述相应客户端上检测到的事件,以检测异常行为。在一些实施例中,在其它事件的上下文中使用多维事件嵌入空间分析个别事件。



1. 一种包括至少一个硬件处理器的服务器计算机系统,所述至少一个硬件处理器经配置以:

响应于目标事件在目标客户端系统上发生,所述目标事件选自由进程的发起和试图存取文件组成的群组,根据所述目标事件确定所述目标客户端系统是否包括恶意软件;以及

响应于确定所述目标客户端系统包括恶意软件,执行安全动作以保护所述目标客户端系统;

其中确定所述目标客户端系统是否包括恶意软件包括:

确定所述目标事件的事件上下文,所述事件上下文包括在所述目标事件之前在所述目标客户端系统上发生的一组事件以及在所述目标事件之后在所述客户端系统上发生的另一组事件,

根据所述目标事件从多个预定客户端配置文件中选择客户端配置文件,所选择的客户端配置文件表征所选择的客户端系统集群的基线行为,

响应于选择所述客户端配置文件,采用特定于所选择的客户端配置文件的行为模型来根据所述事件上下文确定多个预测分数,所述多个预测分数中的每个分数是针对不同事件类型而确定的并指示所述不同事件类型的事件发生于所选择的客户端配置文件的所述事件上下文中的可能性,以及

从所述多个预测分数中选择针对所述目标事件的事件类型确定的分数,以及将所选择的分数与预定阈值进行比较;且

其中通过分析在多个客户端系统上发生的事件集合来确定所选择的客户端系统集群的组成以确定所述多个客户端系统中的哪些客户端系统表现出相似行为。

2. 根据权利要求1所述的服务器计算机系统,其中确定所述目标客户端系统是否包括恶意软件包括:

当所选择的分数指示所述目标事件很可能在所述事件上下文中发生时,确定所述目标客户端系统不包括恶意软件;及

当所选择的分数指示所述目标事件不太可能在所述事件上下文中发生时,确定所述目标客户端系统包括恶意软件。

3. 根据权利要求1所述的服务器计算机系统,其中确定所述目标客户端系统是否包括恶意软件包括:

根据所述多个预测分数确定经预测事件;

比较所述经预测事件与所述目标事件;及

作为响应,根据所述比较的结果确定所述目标客户端系统是否包括恶意软件。

4. 根据权利要求1所述的服务器计算机系统,其中:

所述行为模型包括事件编码器,所述事件编码器经配置以确定指示所述目标事件在事件嵌入空间中的位置的一组坐标;且

所述硬件处理器进一步经配置以根据所述位置确定所述目标客户端系统是否包括恶意软件。

5. 根据权利要求1所述的服务器计算机系统,其中确定所述客户端系统的所述所选择集群的所述组成包括:

根据所述事件集合的所选择的事件是否发生于所述事件集合的其它事件的所选择的

上下文中构建多个事件类别；

响应于构建所述多个事件类别，根据每一客户端系统的事件配置文件决定每一客户端系统是否属于所选择的客户端系统集群，所述事件配置文件根据在所述每一客户端系统上发生且属于所述多个事件类别的所选择的事件类别的事件计数进行确定。

6. 根据权利要求1所述的服务器计算机系统，其中训练所述行为模型包括：

组装具有训练中心事件及训练事件上下文的事件的训练序列，其中所述训练序列中的每个成员是根据所述每个成员是否已发生在所述所选择的客户端系统集群的成员上而从所述事件集合中选择的；

采用所述行为模型，响应于接收到所述训练序列的所述训练事件上下文，产生指示所述训练中心事件属于所述训练序列的可能性的训练预测；及

根据所述训练预测调整所述行为模型的一组参数值。

7. 根据权利要求1所述的服务器计算机系统，其进一步经配置以根据所述目标客户端系统是否是所选择的集群的成员选择所述客户端配置文件。

8. 根据权利要求1所述的服务器计算机系统，其中选择所述客户端配置文件包括：

确定指示所述目标客户端系统在高维嵌入空间中的位置的一组坐标；

作为响应，根据所述一组坐标选择所述多个集群中的目标集群；及

根据所述目标集群选择所述客户端配置文件。

9. 根据权利要求8所述的服务器计算机系统，其经配置以进一步根据指示所述目标集群的成员在所述嵌入空间中的位置的另一组坐标选择所述目标集群。

10. 根据权利要求1所述的计算机系统，其中所述至少一个硬件处理器经配置以进一步根据所述目标客户端系统的当前用户来选择所述客户端配置文件。

11. 根据权利要求1所述的计算机系统，其中所述目标事件的所述事件上下文包括所述目标客户端系统试图存取所选择的网络位置。

12. 一种计算机实施方法，其包括：

响应于目标事件在目标客户端系统上发生，所述目标事件选自由进程的发起和试图存取文件组成的群组，采用计算机系统的至少一个硬件处理器根据所述目标事件确定所述目标客户端系统是否包括恶意软件；

响应于确定所述目标客户端系统包括恶意软件，执行安全动作以保护所述目标客户端系统；

其中确定所述目标客户端系统是否包括恶意软件包括：确定所述目标事件的事件上下文，所述事件上下文包括在所述目标事件之前在所述目标客户端系统上发生的一组事件以及在所述目标事件之后在所述客户端系统上发生的另一组事件，

根据所述目标事件从多个预定客户端配置文件中选择客户端配置文件，所选择的客户端配置文件表征所选择的客户端系统集群的基线行为，

响应于选择所述客户端配置文件，采用特定于所选择的客户端配置文件的模型来根据所述事件上下文确定多个预测分数，所述多个预测分数中的每个分数是针对不同事件类型而确定的并指示所述不同事件类型的事件发生于所选择的客户端配置文件的所述事件上下文中的可能性，

从所述多个预测分数中选择针对所述目标事件的事件类型确定的分数，以及将所选择

的分数与预定阈值进行比较;且

其中通过分析在多个客户端系统上发生的事件集合来确定所选择的客户端系统集群的组成以确定所述多个客户端系统中的哪些客户端系统表现出相似行为。

13. 根据权利要求12所述的计算机实施方法,其中确定所述目标客户端系统是否包括恶意软件包括:

当所选择的分数指示所述目标事件很可能在所述事件上下文中发生时,确定所述目标客户端系统不包括恶意软件;及

当所选择的分数指示所述目标事件不太可能在所述事件上下文中发生时,确定所述目标客户端系统包括恶意软件。

14. 根据权利要求12所述的计算机实施方法,其中确定所述目标客户端系统是否包括恶意软件包括:

根据所述多个预测分数确定经预测事件;

比较所述经预测事件与所述目标事件;及

作为响应,根据所述比较的结果确定所述目标客户端系统是否包括恶意软件。

15. 根据权利要求12所述的计算机实施方法,其中:

所述行为模型包括事件编码器,所述事件编码器经配置以确定指示所述目标事件在事件嵌入空间中的位置的一组坐标;且

所述至少一个硬件处理器进一步经配置以根据所述位置确定所述目标客户端系统是否包括恶意软件。

16. 根据权利要求12所述的计算机实施方法,其中确定所述客户端系统的所述所选择集群的所述组成包括:

根据所述事件集合的所选择的事件是否发生于所述事件集合的其它事件的所选择的上下文中构建多个事件类别;

响应于构建所述多个事件类别,根据每一客户端系统的事件配置文件决定每一客户端系统是否属于所选择的客户端系统集群,所述事件配置文件根据在所述每一客户端系统上发生且属于所述多个事件类别的所选择的事件类别的事件计数进行确定。

17. 根据权利要求12所述的计算机实施方法,其中训练所述行为模型包括:

组装具有训练中心事件及训练事件上下文的事件的训练序列,其中所述训练序列中的每个成员是根据所述每个成员是否已发生在所述所选择的客户端系统集群的成员上而从所述事件集合中选择的;

采用所述行为模型,响应于接收到所述训练序列的所述训练事件上下文,产生指示所述训练中心事件属于所述训练序列的可能性的训练预测;及

根据所述训练预测调整所述行为模型的一组参数值。

18. 根据权利要求12所述的计算机实施方法,其进一步包括根据所述目标客户端系统是否是所选择的集群的成员选择所述客户端配置文件。

19. 根据权利要求12所述的计算机实施方法,其中选择所述客户端配置文件包括:

确定指示所述目标客户端系统在多维嵌入空间中的位置的一组坐标;

作为响应,根据所述一组坐标选择所述多个集群中的目标集群;及

根据所述目标集群选择所述客户端配置文件。

20.根据权利要求19所述的计算机实施方法,其包括进一步根据指示所述目标集群的成员在所述嵌入空间中的位置的另一组坐标选择所述目标集群。

21.根据权利要求12所述的方法,其中所述至少一个硬件处理器经配置以进一步根据所述目标客户端系统的当前用户来选择所述客户端配置文件。

22.根据权利要求12所述的方法,其中所述目标事件的所述事件上下文包括所述目标客户端系统试图存取所选择的网络位置。

23.一种存储指令的非暂时性计算机可读媒体,所述指令在由计算机系统的至少一个硬件处理器执行时致使所述计算机系统进行以下操作:

响应于目标事件在目标客户端系统上发生,所述目标事件选自由进程的发起和试图存取文件组成的群组,根据所述目标事件确定所述目标客户端系统是否包括恶意软件;以及

响应于确定所述目标客户端系统包括恶意软件,执行安全动作以保护所述目标客户端系统;

其中确定所述目标客户端系统是否包括恶意软件包括:

确定所述目标事件的事件上下文,所述事件上下文包括在所述目标事件之前在所述目标客户端系统上发生的一组事件以及在所述目标事件之后在所述客户端系统上发生的另一组事件,

根据所述目标事件从多个预定客户端配置文件中选择客户端配置文件,所选择的客户端配置文件表征所选择的客户端系统集群的基线行为,

响应于选择所述客户端配置文件,采用特定于所述客户端配置文件的行为模型来根据所述事件上下文确定多个预测分数,所述多个预测分数中的每个分数是针对不同事件类型而确定的并指示所述不同事件类型的事件发生于所选择的客户端配置文件的所述事件上下文中的可能性,

从所述多个预测分数中选择针对所述目标事件的事件类型确定的分数,以及将所选择的分数与预定阈值进行比较;且

其中通过分析在多个客户端系统上发生的事件集合来确定所选择的客户端系统集群的组成以确定所述多个客户端系统中的哪些客户端系统表现出相似行为。

用于行为威胁检测的系统及方法

背景技术

[0001] 本发明涉及计算机安全系统及方法,且特定来说,涉及用于检测恶意软件及/或对计算机系统及/或通信网络的入侵的系统及方法。

[0002] 近年来,计算机及网络安全对个人及公司两者来说都变得越来越重要。电子通信技术的快速发展,在日常活动中对软件日益增加的依赖性,及物联网的出现使公司及个人容易失去隐私及遭受数据盗窃。

[0003] 熟练的攻击者可尝试使用各种技术(例如,通过恶意软件安装在公司计算机上的后门)渗透到公司网络中。接着,攻击者可获得、修改、或破坏敏感信息。其它示范性攻击尤其包含停用物理安全系统(例如防窃警报器)或以其它方式使所述物理安全系统失去能力、安装间谍软件、及干扰控制商品及服务的制造或分配的自动化系统(例如电力网)。

[0004] 在计算机系统中执行的软件可用于自动检测及/或防止未授权入侵及其它恶意活动。通常称为入侵检测系统(IDS)的此软件可监测网络及/或计算机活动的异常事件或策略违规。典型的IDS记录与观测到的事件相关的信息、通知用户或网络管理员、且产生报告。一些IDS可例如通过响应于检测到入侵而改变安全设置(例如,重新配置防火墙)进一步防止入侵者执行恶意活动。

[0005] 然而,随着软件服务的逐步非定域化及在信息网络上流动的数据量的增加,使安全软件筛选此大量信息以找到恶意活动的指示符变得越来越不切实际。因此,开发更稳健且可扩展的入侵检测系统及方法引起了人们的极大兴趣。

发明内容

[0006] 根据一个方面,一种服务器计算机系统包括至少一个硬件处理器,其经配置以:响应于接收到目标事件在目标客户端系统上发生的指示,组装包含所述目标事件的事件序列,所述事件序列中的所有事件都已发生于所述目标客户端系统上,其中所述事件序列的成员根据所述事件序列中的每一事件的发生时间布置。所述至少一个硬件处理器进一步经配置:响应于接收到所述指示,根据所述目标客户端系统从多个参数值选择参数值;及使用所述参数值实例化行为模型,所述行为模型经配置以输入所述事件序列的所选择的事件且作为响应产生指示所述事件序列包含所述目标事件的可能性的预测指示符。所述至少一个硬件处理器进一步经配置:响应于实例化所述行为模型,根据所述预测指示符确定所述目标事件是否指示计算机安全威胁。所述多个参数值根据已经发生于分组到多个客户端集群中的多个客户端系统上的事件的训练语料库进行确定。所述多个参数值中的每一者根据所述训练语料库的相异子集进行确定,每一相异子集已经发生于多个客户端集群的相异集群的成员上。选择所述参数值包括根据所述目标客户端系统从所述多个客户端集群选择目标集群,及根据所述目标集群选择所述参数值。

[0007] 根据另一方面,一种计算机实施方法包括:响应于接收到目标事件在目标客户端系统上发生的指示,采用计算机系统的至少一个硬件处理器组装包含所述目标事件的事件序列,所述事件序列中的所有事件都已发生于所述目标客户端系统上,其中所述事件序列

的成员根据所述事件序列中的每一事件的发生时间布置。所述方法进一步包括：响应于接收到所述指示，采用所述计算机系统的至少一个硬件处理器根据所述目标客户端系统从多个参数值选择参数值。所述方法进一步包括：响应于选择所述参数值，采用所述计算机系统的至少一个硬件处理器使用所述参数值实例化行为模型，所述行为模型经配置以输入所述事件序列的所选择的事件且作为响应产生指示所述事件序列包含所述目标事件的可能性的预测指示符。所述方法进一步包括：响应于实例化所述行为模型，采用所述计算机系统的至少一个硬件处理器根据所述预测指示符确定所述目标事件是否指示计算机安全威胁。所述多个参数值根据已经发生于分组到多个客户端集群中的多个客户端系统上的事件的训练语料库进行确定。所述多个参数值中的每一者根据所述训练语料库的相异子集进行确定，每一相异子集已经发生于多个客户端集群的相异集群的成员上。选择所述参数值包括根据所述目标客户端系统从所述多个客户端集群选择目标集群，及根据所述目标集群选择所述参数值。

[0008] 根据另一方面，一种存储指令的非暂时性计算机可读媒体，所述指令在由计算机系统的至少一个硬件处理器执行时致使所述计算机系统进行以下操作：响应于接收到目标事件在目标客户端系统上发生的指示，组装包含所述目标事件的事件序列，所述事件序列中的所有事件都已发生于所述目标客户端系统上，其中所述事件序列的成员根据所述事件序列中的每一事件的发生时间布置。所述指令进一步致使所述计算机系统：响应于接收到所述指示，根据所述目标客户端系统从多个参数值选择参数值；及响应于选择所述参数值，使用所述参数值实例化行为模型，所述行为模型经配置以输入所述事件序列的所选择的事件且作为响应产生指示所述事件序列包含所述目标事件的可能性的预测指示符。所述指令进一步致使所述计算机系统：响应于实例化所述行为模型，根据所述预测指示符确定所述目标事件是否指示计算机安全威胁。所述多个参数值根据已经发生于分组到多个客户端集群中的多个客户端系统上的事件的训练语料库进行确定。所述多个参数值中的每一者根据所述训练语料库的相异子集进行确定，每一相异子集已经发生于多个客户端集群的相异集群的成员上。选择所述参数值包括根据所述目标客户端系统从所述多个客户端集群选择目标集群，及根据所述目标集群选择所述参数值。

附图说明

[0009] 在阅读了以下详细描述且在参考了图式之后，将更好地理解本发明的前述方面及优点，其中：

[0010] 图1展示根据本发明的一些实施例的若干示范性互连客户端系统，其中安全服务器充当入侵检测系统。

[0011] 图2展示根据本发明的一些实施例的经实施以保护客户端系统的示范性数据交换。

[0012] 图3-A说明根据本发明的一些实施例的客户端系统的示范性硬件配置。

[0013] 图3-B说明根据本发明的一些实施例的安全服务器的示范性硬件配置。

[0014] 图4展示根据本发明的一些实施例的在受保护的客户端系统上执行的示范性软件组件。

[0015] 图5展示根据本发明的一些实施例的安全服务器的示范性软件架构。

- [0016] 图6说明根据本发明的一些实施例的分析引擎的示范性操作。
- [0017] 图7展示根据本发明的一些实施例的由分析引擎实施的示范性步骤序列。
- [0018] 图8-A展示根据本发明的一些实施例的事件编码器的示范性训练。
- [0019] 图8-B展示根据本发明的一些实施例的事件编码器的替代示范性训练。
- [0020] 图9展示经执行以训练呈图8-A的配置的事件解码器的示范性步骤序列。
- [0021] 图10说明根据本发明的一些实施例的示范性事件嵌入空间及一组示范性事件集群。
- [0022] 图11说明根据本发明的一些实施例的示范性客户端配置文件空间及一组客户端集群。
- [0023] 图12展示根据本发明的一些实施例的客户端系统的示范性事件配置文件。
- [0024] 图13展示根据本发明的一些实施例的异常检测器的示范性组件及操作。
- [0025] 图14说明根据本发明的一些实施例的在训练期间由异常检测器执行的示范性步骤序列。
- [0026] 图15展示根据本发明的一些实施例的形成异常检测器的部分的行为模型的示范性组件。
- [0027] 图16说明根据本发明的一些实施例的由经训练异常检测器执行的示范性步骤序列。
- [0028] 图17-A展示包括采用本发明的一些实施例检测实际计算机安全威胁的实验的结果。
- [0029] 图17-B展示使用一些实施例检测实际计算机安全威胁的其它实验结果。

具体实施方式

[0030] 在以下描述中,应理解,结构之间的所有引述的连接可为直接有效连接或通过中间结构的间接有效连接。一组元件包含一或多个元件。应理解,对元件的任何引述涉及至少一个元件。多个元件包含至少两个元件。除非另外指定,否则“或”的任何使用是指非排他或。除非另外需要,否则所描述的任何方法步骤都无需必定以所说明的特定顺序执行。从第二元素导出的第一元素(例如数据)涵盖等于第二元素的第一元素,还涵盖通过处理第二元素产生的第一元素及任选的其它数据。根据参数作出确定或决策涵盖根据参数且任选地根据其它数据作出确定或决策。除非另外指定,否则一些数量/数据的指示符可为数量/数据本身、或不同于数量/数据本身的指示符。计算机程序是实施任务的处理器指令序列。本发明的一些实施例中描述的计算机程序可为其它计算机程序的独立软件实体或子实体(例如子例程、库)。除非另外指定,否则计算机安全涵盖使设备及数据免受非法存取、修改、及/或破坏。计算机可读媒体涵盖非暂时性媒体(例如磁性、光学、及半导体存储媒体(例如硬盘驱动器、光盘、快闪存储器、DRAM)),还涵盖通信链路(例如导电电缆及光纤链路)。根据一些实施例,本发明尤其提供包括经编程以执行本文中描述的方法的硬件(例如一或多个处理器)、以及编码用于执行本文中描述的方法的指令的计算机可读媒体的计算机系统。

[0031] 以下描述通过实例且不一定通过限制来说明本发明的实施例。

[0032] 图1展示根据本发明的一些实施例的被保护而免受计算机安全威胁的一组示范性客户端系统10a到h。客户端系统10a到h一般表示具有处理器、存储器、及通信接口的任何电

子装置。示范性客户端系统10a到h包含个人计算机、膝上型计算机、平板计算机、移动通信装置(例如智能电话)、媒体播放器、TV、游戏机、家用电器(例如冰箱、智能加热及/或照明系统)、及穿戴式装置(例如智能手表、健身器材)等。客户端系统10a到h可执行各种软件,例如文档处理、游戏、电子信息收发、及社交媒体应用程序等。一些客户端可与远程内容服务器17交换信息,例如因特网浏览。

[0033] 所说明的客户端系统通过本地网络12a到b连接,且进一步经连接到扩展网络14,例如广域网(WAN)或因特网。在一个实例中,客户端系统10a到d表示通过家用网络12a互连的家庭电子装置。同时,客户端系统10e到g可标示办公大楼内部的个人计算机及/或企业大型机。接着,本地网络12a到b可表示企业网络(例如局域网-LAN)的区段。

[0034] 路由器包括实现多个客户端系统之间的通信及/或相应客户端到扩展网络14的接入的电子设备。在图1的实例中,路由器15a到b互连本地网络12a到b上的客户端及/或使客户端10a到g能接入因特网。路由器15a到b可分别充当本地网络12a到b与扩展网络14之间的网关且可进一步将一组网络服务提供到客户端系统10a到g。此类服务包含例如将网络配置参数分配到客户端系统10a到g(例如经由动态主机配置协议-DHCP指派网络地址)、及通过一系列网络节点路由通信。一些客户端系统(例如示范性客户端系统10h)可例如经由电信中继器直接连接到扩展网络14。

[0035] 图1进一步展示连接到扩展网络14的安全服务器16。服务器16一般表示可或可不彼此物理接近的一组通信耦合的计算机系统。服务器16保护客户端系统10a到h使其免受计算机安全威胁,例如恶意软件及入侵。在一些实施例中,此保护包括安全服务器16检测在客户端系统处发生的可疑活动,例如攻击者控制相应客户端系统的动作。

[0036] 安全服务器16与客户端系统10之间的示范性数据交换在图2中说明。客户端系统10可表示图1中的任何客户端10a到h。在一些实施例中,服务器16经配置以从客户端系统10接收事件指示符20a,指示符20a指示在客户端10上执行软件期间发生特定类型的事件。此类事件的实例包含进程/线程的发起(例如,用户发起应用程序、父进程创建子进程等)、试图存取相应客户端系统的输入装置(例如相机、麦克风)、试图存取本地或远程网络资源(例如存取特定URL的超文本传输协议-HTTP请求、试图通过本地网络存取文档存储库)、以特定统一资源标识符方案制定的请求(例如mailto:或ftp:请求)、特定处理器指令(例如系统调用)的执行、试图加载库(例如动态链接库-DLL)、试图创建新的磁盘文件、试图从磁盘上的特定位置进行读取或写入到磁盘上的特定位置(例如试图盖写现存文件、试图打开特定文件夹或文档)、及试图发送电子消息(例如电子邮件、短消息服务-SMS等)等。在一些实施例中,非活动周期,即事件之间的时间间隙及/或当相应客户端系统空闲、不登记用户活动、或仅实施内部系统任务时的时间间隔也算作事件且可经由事件指示符向安全服务器报告。此类非活动周期可进一步被分化为短时间间隙(例如,大约几秒)及长时间间隙(例如,大约几分钟到几个小时)。检测到的事件可指示或可不指示恶意本身;一些事件可在与其它事件一起发生时及/或在以特定顺序发生时为指示为恶意的。其它事件可在其在一天当中的特定时间发生或以异常频率发生时为恶意的,例如在几秒间隔内从特定磁盘文件夹连续读取1000次。

[0037] 每一事件指示符20a可尤其包括相应事件的类型的指示符及指示相应事件发生的时刻的时间戳。事件指示符20a可进一步包含相应客户端系统的标识符(客户端ID)及/或同

时操作相应客户端系统的用户的指示符(用户ID)。例如,当所传达的事件包括进程创建时,用户指示符可指示父进程的所有者。事件指示符20a可编码其它参数,例如进程名称、文件系统位置/发起进程的路径、网络地址(例如因特网协议-IP地址)、HTTP请求的统一资源定位符(URL)等。

[0038] 在一些实施例中,服务器16还可从路由器15a到b采集信息,如由图2中的事件指示符20b说明。此类事件指示符可包含例如网络事件的指示符,例如由连接到相应路由器/网关的客户端系统发出的网络接入请求。例如,事件指示符20b可包含始发IP地址、目的地IP地址、时间戳、及有效负载大小。在一些实施例中,事件指示符20b包括由相应路由器根据各种数据处理协议聚合的客户端事件数据(例如网络流量、网络日志等)。

[0039] 安全服务器16维持表示操作客户端系统10a到h的子集的基线、正常、及/或合法方式的一组用户行为模型。此类行为模型在本文中认为是客户端配置文件。此类行为模型的参数一般被表示为图1中的配置文件数据库19且可包含事件及/或客户端聚类算法的输出,如在下文详细展示。在其中配置文件由客户端或事件集群表示的一个示范性实施例中,相应配置文件的参数可包含集群质心的坐标及指示相应集群沿着各个轴的范围的一组数字。其它配置文件参数可尤其包含相应集群的离心率量度、集群成员与集群的质心之间的平均距离等。客户端配置文件可使用监管式或非监管式学习方法及算法自动产生,如在下文展示。

[0040] 客户端配置文件可捕获单个用户的行为或可共同捕获多个用户的行为。为了给出一些实例,智能电话主要可由单个用户使用,因此附加到相应智能电话的客户端配置文件可基本上捕获其主要用户的基线行为。相比之下,属于大学计算机实验室的计算机可由许多不同学生使用;附加到这些机器中的一者的客户端配置文件可共同表示所有相应学生的基线行为。一个客户端配置文件可经附加到单个客户端系统/物理机(例如智能电话、膝上型计算机)。在一些实施例中,一个客户端配置文件可共同表示多个物理机。在一个此实例中,图1中的客户端系统10a到d可共同由捕获特定家族的成员的正常或基线行为的单个客户端配置文件表示。在另一实例中,一个客户端配置文件用于表示企业的会计部门中的所有计算机,而另一客户端配置文件表示由相应企业的研究及开发团队使用的所有计算机。在云计算环境中,例如其中物理机可为各个分布式用户执行多个虚拟机的虚拟桌面基础设施(VDI)环境,一个客户端配置文件可经附加到在相应物理机上执行的多个虚拟机。

[0041] 在一些实施例中,单个用户可由多个相异客户端配置文件表示。例如,同一个人可在工作时具有一个客户端配置文件/基线行为且在家时具有相异客户端配置文件/基线行为。客户端配置文件的其它实例可与特定年龄群(例如青少年)、特定个人兴趣(例如游戏)、特定职业(例如工程师、艺术家、教育家)等的用户相关联。在又一示范性实施例中,相异客户端配置文件可对应于相异计算机活动,例如对应于使用相异计算机程序:浏览因特网、使用社交媒体、进行办公室工作等。又其它示范性客户端配置文件可经附加到相异装置类型(例如智能电话对PC)。可根据更复杂准则设想共同配置文件,例如指示工程师从公司X浏览因特网的典型/基线方式的客户端配置文件。另一此示范性配置文件可指示年轻人使用平板电脑的典型方式。

[0042] 事件指示符20a到b的子集可经收集以形成进一步用于导出客户端配置文件的事件语料库,如在下文详细展示。事件指示符的另一子集可用于检测安全威胁。例如,响应于

接收到事件指示符20a到b,安全服务器16可确定由相应事件指示符传达的事件与根据相应客户端指示符选择的客户端配置文件是否一致。换种方式来说,安全服务器16可确定相应事件是否匹配编码于相应客户端配置文件中的正常/基线行为的模式。当不匹配时,相应事件可指示可疑活动,在此情况中一些实施例可采取保护动作,例如将安全警告22a到b发送到相应客户端系统及/或相应客户端系统的管理员。在保护动作的另一实例中,一些实施例指示属于与可疑客户端系统相同的本地网络的路由器阻止到及/或来自相应可疑客户端系统的通信。客户端配置文件及由安全服务器16进行的事件指示符的处理在下文进一步描述。

[0043] 图3-A展示根据本发明的一些实施例的客户端系统的示范性硬件配置。客户端系统10可表示图1中的客户端系统10a到h中的任一者。为了清楚起见,所说明的客户端系统是计算机系统。其它客户端系统(例如移动电话、平板计算机、及穿戴式装置)可具有略微不同的配置。处理器32包括经配置以使用一组信号及/或数据执行计算/或逻辑操作的物理装置(例如微处理器、形成于半导体衬底上的多核集成电路)。此类信号或数据可呈处理器指令(例如机器代码)的形式经编码且递送到处理器32。存储器单元34可包括在实施操作的过程时存储由处理器32存取或产生的数据/信号的易失性计算机可读媒体(例如动态随机存取存储器-DRAM)。

[0044] 输入装置36可包含计算机键盘、鼠标、及麦克风等,包含允许用户将数据及/或指令引入到客户端系统10的相应硬件接口及/或适配器。输出装置38可包含显示器装置,例如监视器及扬声器等,还包含使相应客户端系统能将数据传达到用户的硬件接口/适配器,例如图形卡。在一些实施例中,输入及输出装置36到38共享共同硬件零件(例如触摸屏)。存储装置42包含实现软件指令及/或数据的非易失性存储、读取、及写入的计算机可读媒体。示范性存储装置包含磁盘及光盘及快闪存储器装置,还包含可装卸媒体,例如CD及/或DVD盘及驱动器。网络适配器44使客户端系统10能连接到电子通信网络(例如图1中的网络12、14)及/或其它装置/计算机系统。

[0045] 控制器集线器40一般表示多个系统、外围设备、及/或芯片组总线、及/或使能在处理器32与客户端系统10的剩余硬件组件之间通信的所有其它电路系统。例如,控制器集线器40可包括存储器控制器、输入/输出(I/O)控制器、及中断控制器。取决于硬件制造商,一些此类控制器可经并入到单个集成电路中,及/或可与处理器集成。在另一实例中,控制器集线器40可包括将处理器32连接到存储器34的北桥、及/或将处理器32连接到装置36、38、42及44的南桥。

[0046] 图3-B展示根据本发明的一些实施例的安全服务器16的示范性硬件配置。服务器16包括至少一个硬件处理器132(例如微处理器、多核集成电路)、物理存储器134(例如DRAM)、服务器存储装置142、及一组服务器网络适配器144。服务器处理器132可包含中央处理单元(CPU)及/或图形处理单元(GPU)阵列。适配器144可包含使安全服务器16能连接到通信网络14的网络卡及其它通信接口。服务器存储装置142可存储数据,例如事件指示符及/或客户端配置文件参数。在一些实施例中,服务器16进一步包括输入及输出装置,其功能可分别类似于客户端系统10的输入/输出装置36及38。

[0047] 图4展示根据本发明的一些实施例的在客户端系统10上执行的示范性软件组件。此软件可包含提供客户端系统10的硬件与其它计算机程序(例如在相应客户端系统上执行

的用户应用程序48)之间的接口的操作系统(OS)46。示范性操作系统尤其包含 Windows®、MacOS®、iOS®、及 Android®。用户应用程序48一般表示任何应用程序,例如文字处理、图像处理、电子表格、日历、线上游戏、社交媒体、网页浏览器、及电子通信应用程序等。在一些实施例中,安全应用程序50经配置以保护客户端系统10使其免受计算机安全威胁,例如恶意软件及入侵。除了其它功能之外,安全应用程序50尤其经配置以将事件指示符发射到安全服务器16及/或接收安全警告。在一些实施例中,应用程序50进一步包括事件采集器52及网络滤波器53。网络滤波器53的一些功能性可直接实施于硬件中。当客户端系统10操作硬件虚拟化平台时,其中OS 46及应用程序48在虚拟机内执行(例如,在云计算环境中),事件采集器52及/或网络滤波器53可在相应虚拟机外部例如在暴露相应虚拟机的虚拟机管理程序的等级下使用所属领域称为自省的技术的操作。

[0048] 事件采集器52经配置以检测在由客户端系统10执行软件期间发生的各种事件。一些实施例可给每一检测到的事件加时间戳以记录相应事件的发生时间。监测到的事件可为机器及/或操作系统特定的。示范性事件尤其包含进程发起、进程终止、子进程的产生、对外围设备(例如硬盘、网络适配器)的存取请求、由用户键入到命令行接口中的命令等。此类硬件及/或软件事件可使用计算机安全领域中已知的任何方法例如通过拦截操作系统的特定功能、检测系统调用、采用文件系统微过滤器、改变存储器存取权限以检测执行来自特定存储器地址的代码的意图等来检测。

[0049] 一些实施例使用内置于OS 46内的系统日志记录工具(例如UNIX®中的Syslog)来监测硬件及/或软件事件。此类工具可产生事件描述符列表,其包含每一事件的时间戳、识别事件类型的数值码、产生相应事件的进程或应用程序的类型的指示符、及其它事件参数。安全应用程序50可从相应系统日志提取此类信息以制定事件指示符。

[0050] 下面给出示范性syslog条目:

[0051] <30>Feb 8 21:36:51dtm charon:12[IKE]establishing CHILD_SA dtmhq5 {5}

[0052] <30>Feb 8 21:36:51 dtm charon:12[IKE]establishing CHILD_SA dtmhq5 {5}

[0053] <187>Feb 8 21:37:56 example.domain.biz dhcpd:DHCPDISCOVER from 0c:14:7b:11:

[0054] 14:64via eth1:network eth1:no free leases

[0055] 网络滤波器53检测在客户端系统10与其它方之间经由网络12到14的电子通信期间发生的一组网络事件。由网络滤波器53检测的示范性事件包含形成在客户端系统10与另一网络实体之间建立连接的部分的事件(例如请求网络地址、发射网络地址、握手事件等)、配置经加密连接的事件(安全套接字层-SSL、虚拟私有网络-VPN)、发射数据、及接收数据等。在一些实施例中,网络滤波器53从经拦截网络业务收集元数据。此类元数据可包含例如始发网络地址(例如因特网协议-IP地址)、目的地地址、数据分组的时间戳、通信协议类型的指示符、及数据分组的大小。其它示范性元数据可包含传输相应通信/数据分组的超文本传输协议(HTTP)用户代理的类型。一些实施例将通信元数据组织成专门的数据结构,在所属领域中称为网络流量(例如来自思科系统有限公司(Cisco Systems, Inc.)的NetFlow®)。表1展示根据本发明的一些实施例表示为流量的通信元数据的实例。

[0056] 表1

[0057]	流量	目的地		源		协议	字节数	分组数	TCP 旗标
	#	地址	端口	地址	端口				
	1	10.10.12.71	443	192.168.127.10	54321	TCP	12300	21	SA
	2	192.168.127.10	54321	10.10.12.71	443	TCP	2156980	413	FSPA

[0058] 在一些实施例中,安全应用程序50根据由采集器52及网络滤波器53检测的硬件、软件、及/或网络事件制定事件指示符。应用程序50可进一步管理与安全服务器16的通信,以发射事件指示符及/或接收安全通知等。

[0059] 在替代实施例中,代替如上文所展示那样在客户端处处理网络通信,网络滤波器53及/或路由器15可经配置以将传入及/或传出客户端系统10的电子通信的至少一部分重新路由到安全服务器16。例如,客户端系统10的网络配置参数可经设置以将服务器16指示为默认网络网关。接着,一些实施例采用安全服务器16来从相应经重新路由的业务提取事件指示符。

[0060] 图5展示根据本发明的一些实施例的在安全服务器16上执行的示范性软件。所说明的软件包含分析引擎60及进一步连接到警告管理器64的异常检测器62。技术人员将了解,并非所说明的所有组件都需要在同一机器/处理器上执行;例如,分析引擎60可在专用处理器集群上执行,而异常检测器62的例子可在其它机器/处理器上运行。

[0061] 在一些实施例中,分析引擎60经配置以分析在一组客户端系统(例如图1中的客户端10a到h的子集)上发生的事件及构建表示操作相应客户端系统的基线、正常、及/或合法方式的多个客户端配置文件。从客户端接收的事件指示符20a到b的子集可用于组装训练事件语料库,在图1、5、及6中标示为语料库18。接着,根据事件语料库18确定配置文件。确定客户端配置文件可尤其包含在抽象多维事件空间中表示事件及实施数据聚类过程,如在下文更详细展示。接着,所构建的配置文件可经存储为配置文件数据库19中的条目。示范性配置文件数据库条目包括一组配置文件参数,例如集群质心的一组坐标、集群的直径及/或离心率的量度等。

[0062] 图6说明分析引擎60的示范性组件及操作。在一些实施例中,引擎60包括事件编码器70、事件聚类引擎72、及连接到事件编码器70及事件聚类引擎72的客户端聚类引擎74。由分析引擎执行的示范性步骤序列在图7中说明。

[0063] 在步骤202到204到206的序列中,分析引擎60可根据从所选择的客户端系统及/或路由器接收的事件指示符组装训练事件语料库18。一些实施例积累事件指示符直到一些积累条件被满足为止。积累条件可根据事件的计数(收集1百万个事件的事件语料库)、根据时间条件(例如,记录在1h间隔内接收的所有事件等)、根据客户端系统及/或用户的身份(例如,记录从企业X、IP范围Y、订阅账户Z等接收的所有事件)、或根据所属领域中已知的任何其它方法来确定。个别事件可根据其起源进行标记且可包括表征相应事件已经发生、或已经被检测到、或已经在安全服务器16处接收到等的时刻的时间戳。在一些实施例中,事件语料库18通过并入最新接收的事件指示符周期性地及/或按需进行刷新。

[0064] 在一些实施例中,事件编码器70(图6)经配置以输入包括表征在客户端系统上已经发生的事件(例如,在客户端机器上发起进程)的数据的事件记录26,且作为响应,输出包括相应事件的表示的事件向量28a作为在所属领域中通常被认为是嵌入空间的抽象多维空间中的向量。示范性嵌入空间通过一组轴展开,其中每一轴表示相异事件特征。在网络事件

的情况中,示范性特征可包含源IP地址、源端口、目的地IP地址、目的地端口、及传输协议的指示符等。在另一实例中,嵌入空间的每一轴对应于事件特征的线性组合(例如,在主成分/奇异值分解实施例)。在优选实施例中,在相应事件前面及/或后面的其它事件的上下文中分析事件。在此类情况中,编码器70经配置以将事件表示为上下文的嵌入空间中的向量,其中主要发生于类似上下文中的两个事件相对紧密地定位在一起。一些实施例根据事件词汇N的大小(即,相应安全系统正监测的相异事件类型的计数)选取嵌入空间的维度(有关事件词汇的更多信息,请参见下文)。例如,事件空间的维度可约为N的平方根、或约为N的对数。本发明的典型实施例使用具有数百到数千个维度的嵌入上下文空间。

[0065] 事件编码器70可使用自动化数据处理领域中已知的任何方法构建。在优选实施例中,编码器70包括人工智能系统,例如多层人工神经网络(例如递归及/或前馈神经网络)。为了实现事件向量的所期望表示,编码器70的参数可经调谐直到一些性能条件被满足为止。此调谐在本文中称为训练且由图7中的步骤208表示。在神经网络实施例中,事件编码器70的示范性可调谐参数包含一组突触权重等。在一些实施例中,训练编码器70相当于构建嵌入空间本身。换种方式来说,嵌入空间并非是预定的,而是取决于事件语料库18的组成及所选择的训练过程。

[0066] 示范性训练过程在图8-A到B中展示且包括word2vec算法版本,例如连续跳跃元语法算法及连续词袋算法。在此类实施例中,事件并非是孤立地进行分析,而是作为由根据发生或检测时间排序的多个事件组成的事件序列25的成分进行分析。在一些实施例中,相应序列的所有事件都经选择使得其在同一客户端系统上发生。事件序列25包括中心事件 E_0 及由中心事件前面的事件 $E_{-k} \cdots E_{-1}$ ($k \geq 0$)的子集及/或中心事件后面的事件 $E_1 \cdots E_p$ ($p \geq 0$)的子集组成的事件上下文。典型实施例使用对称事件上下文 ($p=k$), 其中p在2到5的范围内。每一个别事件 E_i ($-k \leq i \leq p$) 可被表示为N乘1数字向量,其中每一行表示相异事件类型(例如打开浏览器、启动文件下载、将数据写入到磁盘等),N表示事件类型的“词汇”的大小,且非零元素指示相应事件具有相应事件类型。此表示在所属领域中通常称为独热编码。事件词汇的示范性大小N的范围从数百到数千个相异事件类型,但针对特定应用可增加到高达数百万。技术人员将了解,独热编码在本文中仅用作实例,且决不限制本发明的范围。

[0067] 在示范性训练过程中,事件编码器与事件解码器成对且与事件解码器一起训练,其中两者都可包括前馈及/或递归神经网络的部分。一般来说,编码器-解码器对可经配置以输入训练序列的第一子集(例如,中心事件 E_0)及输出相应序列的第二子集(例如,某上下文事件 E_i , $i \neq 0$)的“预测”。在图8-A到B的实例中,预测被说明为独热向量;替代实施例可使用不同表示。例如,预测可经表示为N维数字向量,每一数字指示对应事件类型存在于第二子集中的可能性。

[0068] 在图8-A中说明的连续跳跃元语法训练过程中,编码器-解码器对经训练以在给定中心事件 E_0 的情况下产生正确的事件上下文。针对从事件语料库18取得的每一事件序列,编码器70a经配置以输入中心事件 E_0 的独热编码及产生包括嵌入上下文空间中中心事件 E_0 的表示的事件向量28c。解码器76a又经配置以输入事件向量28c及输出多个猜测向量,每一者表示相应事件序列的“经预测”上下文事件 E_i ($i \neq 0$)。接着,编码器-解码器对可通过调整编码器70a及/或解码器76a的参数来进行训练以便减小预测误差,即校正相应训练序列的“经预测”上下文与实际上下文之间的失配。

[0069] 替代训练过程使用连续词袋训练算法且目的是在给定相应事件上下文的情况下产生训练序列的正确中心事件 E_0 。在图8-B中说明的一个此实例中,事件编码器70b经配置以输入表示序列25的上下文事件 E_i ($i \neq 0$)的一组独热向量,及输出针对每一相应上下文事件确定的嵌入事件向量28d到f。与图8-A中说明的连续跳跃元语法实施例相反,编码器70b现在与经配置以输入多个事件向量28d到f及产生对序列25的中心事件 E_0 的预测或“猜测”的事件解码器76b成对。接着,编码器-解码器对可通过调整编码器70b及/或解码器76b的参数来进行训练以便减小预测误差,即相应训练序列的“经预测”中心事件与实际中心事件之间的失配。

[0070] 实施事件编码器的训练的示范性步骤序列在图9中说明。步骤222从事件语料库18检索一组事件记录且根据事件时间戳且根据相应事件的源(即,已经发生相应事件的客户端系统)识别事件序列25。在连续跳跃元语法实施例中,接着,步骤224执行事件编码器70a以产生事件 E_0 的嵌入空间表示(图8-A中的事件向量28c)。在步骤226中,分析引擎60执行事件解码器76a以产生针对在序列25内的中心事件 E_0 前面及/或后面的事件的一组预测或“猜测”。步骤228比较序列25的每一经预测上下文事件与相应实际上下文事件 E_i ($i \neq 0$),从而确定数值预测误差。可被解译为成本函数或目标函数的预测误差可根据人工智能领域中已知的任何方法进行计算。此类计算可包括确定经预测事件与实际事件之间的距离,例如编辑距离、欧几里得距离、或余弦距离。一些实施例根据交叉熵量度确定目标函数。在步骤230中,分析引擎可在最小化计算得到的预测误差的方向上调整编码器70a的参数。用于训练的一些示范性算法包含使用梯度下降的反向传播、模拟退火及遗传算法等。接着,一些实施例重复步骤222到230直到终止条件被满足为止,例如直到事件语料库18的平均预测误差下降到低于预定阈值为止。在另一实施例中,训练进行达预定时间量或预定迭代计数。技术人员将了解图9中说明的步骤序列在稍作改动的情况下同样也适用于词袋实施例(图8-B)。

[0071] 响应于如上文展示那样训练事件编码器,一些实施例进一步变换所生成的嵌入空间以降低其维度。此操作可包括任何数据降维算法,例如主成分分析(PCA)或奇异值分解(SVD)。

[0072] 在训练及任选的降维(图7中的步骤208)之后,事件编码器70能够将每一事件表示为事件上下文的多维嵌入空间中的向量,其中频繁发生于同一事件上下文内的两个事件占据类似位置。换种方式来说,两个此类事件在嵌入空间中分开小于主要发生于不同上下文中的两个事件之间的距离的距离。

[0073] 返回到分析引擎60(图6)的组件,事件聚类引擎74经配置以根据每一事件向量在嵌入空间内的位置将由经训练事件编码器70产生且表示训练语料库18的成员的事件向量组织成集群(也参见图7中的步骤207)。在一些实施例中,集群包括在嵌入空间中相对靠近地在一起的多个事件,或换种方式来说,包括由嵌入空间中相对较小的事件间距离表征的多个事件。在替代实施例中,集群由占据嵌入空间的集群特定区的事件组成。此类区可为互斥的或部分重叠的。图10说明根据本发明的一些实施例的示范性嵌入空间及一组事件集群80a到b。所说明的轴可包括例如所说明的事件向量(向量28g到h到k)的第一及第二主成分。在使用事件上下文的嵌入空间的实施例中,集群可选择性地含有主要发生于类似事件上下文内的事件。此外,同一集群可包含发生于各个客户端系统上及/或表示各种用户的活动的事件。

[0074] 为了构建事件集群,分析引擎60可采用所属领域中已知的任何数据聚类算法,例如k均值算法的变体。另一示范性实施例可训练一组感知机以将嵌入空间划分为相异区且将定位于每一区内的事件向量指派到相异事件集群。集群及/或区的数目可为预定的(例如根据受保护的客户端系统及/或被监测的事件类型的计数)或可通过聚类算法本身动态地确定。事件聚类的结果包括一组事件集群参数54(图6),其可针对每一集群包含集群的质心的坐标及集群的范围的量度,例如直径及/或离心率。其它示范性集群参数54可尤其包含相应集群的成员列表,且相应集群的所选择的成员被视作相应集群的代表/原型。集群参数可被传递到客户端聚类引擎74上。

[0075] 客户端聚类引擎74(图6)经配置以根据由事件聚类引擎72计算的事件集群确定一组客户端配置文件。此类客户端配置文件在图11中说明。在一些实施例中,每一客户端配置文件包括受保护的客户端系统10a到h的所选择的子集(集群)。一些客户端配置文件可包含多个客户端集群。在一些实施例中,客户端配置文件可包括配置文件原型,其可为相应客户端集群的实际成员、或由配置文件空间中的特定位置表征的虚构客户端系统。例如,配置文件原型可包括由客户端聚类引擎74确定的客户端集群的质心。

[0076] 为了比较客户端配置文件,客户端聚类引擎74的一些实施例根据指示在相应客户端系统上发生的事件的典型分布的事件配置文件将客户端系统10a到h指派到集群。在一个示范性实施例中,客户端系统的事件配置文件包括数字向量,每一者根据在相应客户端系统上发生且属于先前由事件聚类引擎72确定的相异事件集群的事件计数进行确定。在图12中说明的实例中,事件配置文件的每一成分是根据指示属于相应事件集群 C_i 的事件的比例的集群忠诚量度确定,所述比例被确定为可从相应客户端系统得到的总事件计数的分数。例如,当事件聚类引擎72已经识别了三个事件集群 C_1 、 C_2 、及 C_3 时,事件配置文件向量 $[0.1, 0.75, 0.15]$ 可表示一种客户端系统,其中在相应客户端系统上发生的事件的10%属于事件集群 C_1 ,而事件的75%属于事件集群 C_2 且事件的15%属于事件集群 C_3 。

[0077] 在图11中说明的示范性实施例中,每一客户端系统根据相应事件配置文件表示于多维配置文件空间中。换种方式来说,客户端系统的每一坐标表示相应客户端的事件配置文件的成分。图11展示三个示范性客户端集群/配置文件82a到c。技术人员可使用机器学习或数据挖掘领域中已知的任何方法来构建此类配置文件;示范性方法包含k均值聚类算法及神经网络的变体等。替代实施例可使用将客户端系统指派到集群的其它准则,或除了相应客户端的事件配置文件之外还使用此准则。示范性额外客户端聚类准则尤其包含相应客户端系统的拥有者及/或用户、相应客户端系统的网络地址、相应客户端系统的装置类型等。例如,属于相同家庭、相同企业、或相同网络域的客户端可被一起分组在同一集群中。

[0078] 在客户端聚类之后,分析引擎60可将集群参数保存到配置文件数据库19,所述集群参数例如指派到每一集群/配置文件的客户端系统列表、集群原型的坐标(例如质心)、集群直径等。

[0079] 图13说明根据本发明的一些实施例的异常检测器62的示范性组件及操作(还参见图5)。异常检测器62经配置以接收包括指示在各个客户端系统上发生的事件的事件指示符的事件流24及作为响应输出指示相应事件是否指示安全威胁(例如恶意软件的入侵或执行)的安全标记88。在一些实施例中,异常检测器62包括配置文件管理器84,其经配置以响应于接收指示在受保护的客户端系统上发生的事件的事件通知根据相应事件选择客户端

配置文件。配置文件管理器84进一步经连接到经配置以确定相应事件是否拟合由相应配置文件表示的正常/基线行为的模式的行为模型86。当不拟合时,相应事件可被视为异常,从而指示对相应客户端系统的可能攻击。

[0080] 在准备如下文展示那样执行异常检测时,异常检测器62的一些实施例首先使用分析引擎60的输出在事件语料库上进行训练。训练异常检测器62的一个用途是确定由分析引擎60识别的每一客户端配置文件的正常/基线用户行为。训练包括调整行为模型86的一组参数直到终止准则被满足为止。用于训练异常检测器62的事件语料库可不同于用于训练分析引擎60的组件的训练语料库18。

[0081] 图14展示根据本发明的一些实施例的在训练过程期间由异常检测器62执行的示范性步骤序列。响应于异常引擎60构建一组客户端配置文件,步骤242从配置文件数据库19选择一个此客户端配置文件。在一些实施例中,每一此客户端配置文件包括一组客户端集群,例如图11中的集群82a。每一客户端集群进一步包含受保护的客户端系统的所选择的子集。步骤244可选择登记为在与相应配置文件/集群相关联的任何客户端系统上发生的一组训练事件。在一些实施例中,步骤244可包括从已用于如上文展示那样构建客户端配置文件的训练语料库18选择一组训练事件。另一步骤246可使用相应的事件训练集作为训练语料库来训练行为模型86。

[0082] 在一些实施例中,行为模型86包括结构及功能类似于分析引擎60的一些组件的组件。例如,模型86的一些实施例包含如图15中所说明的编码器-解码器对,其可使用神经网络技术构建且根据word2vec系列算法的成员进行训练(参见上文关于图8-A到B的描述)。接着,训练行为模型86可相当于调整编码器70c及/或解码器76c的参数(例如一组突触权重),目的是将来自相应客户端集群/配置文件的每一事件都表示为事件嵌入空间中的向量。在优选实施例中,编码器70c在事件序列的上下文中分析每一事件且产生嵌入空间,其中主要发生于类似上下文中的事件分开相较于发生于其它上下文中的事件更小的距离。然而,由训练编码器70c产生的事件嵌入空间(即轴的含义、事件间距离的大小等)可与由训练事件编码器70产生的事件嵌入空间显著不同,这是因为用于所述两个编码器的训练语料库是相异的。

[0083] 在优选实施例中,步骤246包括使用某一版本的词袋算法训练编码器-解码器对(参见图8-B)。在一个此实例中,编码器-解码器对(图15)经配置以接收表示当前分析的事件序列的事件上下文的多个事件 $E_{-k} \cdots E_{-1}$ 、 $E_1 \cdots E_p$ 及产生N维预测分数向量90,其中每一元素与相异事件类型相关联,每一元素表示相应事件序列的中心事件具有相应事件类型的可能性。例如,较高分数值可指示相应事件类型比具有较低分数的事件类型更有可能作为相应事件序列的中心事件发生。在此类实施例中,模型86的示范性训练可包括从在步骤244中识别的事件的子集选择事件序列(图14),将相应序列的事件上下文输入到编码器70c,执行解码器76c以产生相应事件序列的中心事件 E_0 的预测、及通过反向传播预测误差通过形成编码器70c及/或解码器76c的神经网络来惩罚不正确的预测。响应于成功训练,步骤248可保存经训练行为模型的参数值。可针对由分析引擎60识别的每一客户端配置文件重复所述训练过程。

[0084] 图16说明根据本发明的一些实施例的由异常检测器62执行以保护目标客户端系统(例如图1中的客户端10a到h)是其免受计算机安全威胁的示范性步骤序列。目标客户端

系统可为或可不为提供如上文展示那样产生行为模型及/或客户端配置文件的事件的训练语料库的客户端的子集的成员。为了保护目标客户端系统,事件可在目标客户端系统及/或其它装置(例如路由器15a到b(参见图1))处进行检测,且可以事件指示符的形式传达到安全服务器16。接着,此类事件指示符可根据其源、事件类型、时序、服务账户设置等进行预处理,且被组织为事件流24。事件可个别地或分批进行处理。响应于从目标客户端系统接收到事件指示符,在步骤254中,异常检测器62可根据相应事件指示符组装事件序列以进行分析。步骤254可包含识别事件源(即,已经发生相应事件的客户端系统),从事件流24选择多个其它事件以形成事件序列。在一些实施例中,序列的成员经选取使得其全都源于同一目标客户端系统。在另一实例中,序列的所有成员必须发生于客户端系统的预定子集上,例如(举例来说)网络子域、或共同IP地址。所选取的事件还可根据其发生及/或检测时间进行排序,例如使用与传入事件指示符一起提供的时间戳。事件序列可进一步分成若干部分,例如从而识别中心事件及事件上下文(参见例如图8-A)。

[0085] 在步骤256中,配置文件管理器84可根据相应事件指示符,例如根据已经发生相应事件的目标客户端系统的身份,选择客户端配置文件。当相应目标客户端系统已经提供用于开发客户端配置文件及/或用于训练行为模型的训练事件时,步骤256可包括选择具有相应目标客户端系统的客户端配置文件/集群作为成员。还可使用其它配置文件选择准则。例如,步骤256可包括根据目标客户端系统在客户端配置文件空间内的位置选择客户端配置文件(参见图11),例如通过比较目标客户端系统的位置与一组集群原型或质心及选择其质心离目标客户端系统最近的集群/配置文件。在一个此实例中,客户端配置文件可根据针对目标客户端系统确定的事件配置文件进行选择(例如根据从目标客户端系统接收的拟合到特定事件类别/集群中的事件的计数)。其它客户端配置文件选择准则可包含根据目标客户端系统的网络地址选择客户端配置文件(例如选择含有具有与目标客户端系统相同的IP地址的客户端的客户端配置文件)、根据目标客户端系统的所有者/用户选择客户端配置文件(例如选择含有与目标客户端系统相同的家庭的成员的配置文件)等。

[0086] 在另一步骤258中,异常检测器可使用特定于相应所选择的客户端配置文件的参数值实例化行为模型86。在一些实施例中,在配置文件特定的实例化之后,执行模型86(步骤260)包括在与相应客户端配置文件相关联的事件嵌入空间中投射相应事件序列的事件。

[0087] 步骤262现在可确定相应事件序列的事件是否表示与相应客户端配置文件相关联的正常/基线用户行为。在一个实施例中,步骤260包括将相应序列的事件上下文($E_i, i \neq 0$)馈送到行为模型86及计算相应序列的预测分数向量90。接着,步骤262可包括识别对应于序列的实际中心事件 E_0 的事件类型的向量90的元素,及比较相应分数与预定阈值(例如0.95)。在一些实施例中,低于阈值的分数值指示相应事件 E_0 基本上不可能在相应事件上下文中发生,且因此指示与潜在计算机安全威胁一致的异常。在一些实施例中,安全服务器16的用户或管理员可通过调整阈值的值来调谐方法的灵敏度。在一个此实例中,不同阈值与不同群组的客户端系统相关联。

[0088] 在替代实施例中,步骤260可包括使用模型86确定序列的事件 E_i 在特定于相应客户端配置文件的事件嵌入空间中的表示。接着,步骤262可包括根据相应事件在嵌入空间内的位置确定事件 E_i 是否拟合相应客户端配置文件的正常行为的模式。例如,当事件定位于训练事件的集群内(例如,比预定阈值更靠近集群质心)时其可被认为是正常的。在另一实

例中,当定位于嵌入空间的特定区中时事件可被认为是正常/良性的,且当定位于其它区中时被认为是异常的。

[0089] 当序列的事件(例如 E_0)被认为是异常的时,或换句话说来说,不拟合通过相应客户端配置文件的训练建立的常态模式,步骤264可标记相应事件以进行进一步分析。在一些实施例中,异常可触发安全服务器16的警告管理器64发射安全警告(参见图5)。安全警告可去向已经发生异常事件的客户端系统及/或去向相应客户端系统的管理员。异常事件的事发也可被收集及报告给计算机安全实验室以进行进一步分析。

[0090] 上文描述的示范性系统及方法允许高效地检测计算机安全威胁,例如恶意软件及入侵。所揭示的系统及方法实施用于计算机安全的行为方法,其中正常/基线用户行为由系统根据事件的训练语料库自动推断,且其中违背基线行为模式可指示威胁。

[0091] 一些实施例检测在多个客户端系统(例如计算机、移动电话、网络设备、及虚拟机)处发生的各种事件。示范性事件包含特定进程发起、试图存取特定文件或网络位置、及如存取特定端口及地址的网络业务事件等。技术人员应理解,本文中描述的系统及方法可适于其它种类的事件,例如与用户在社交媒体上的活动、用户的浏览历史、及用户的游戏活动等相关的事件。事件通知在安全服务器处聚合。此类事件的集合可作用于构建一组客户端配置文件的训练语料库,其中每一客户端配置文件可表示单个用户、单个机器、或多个用户/机器。在一些实施例中,每一客户端配置文件包括客户端系统的子集及/或已经发生于客户端系统的相应子集上的事件的子集。每一客户端配置文件可表示相应客户端系统的正常及/或良性使用模式。接着,此类客户端配置文件可用于检测异常行为的事发,其可指示计算机安全威胁。

[0092] 一些常规计算机安全根据一组量化指示恶意行为的行为的规则进行操作。由于开发人员通常对向各种各样的客户端提供此类解决方案感兴趣,因此行为规则通常是通用的,而不是针对特定用户定制的。然而,实际上,用户是非常多样化的。即使在同一公司或家族中,每一成员使用计算机的方式也可能有很大的不同。对软件开发人员或工程师来说可能被认为是正常的一组动作当在会计部门中的计算机上被检测到时可能会非常不寻常。此外,同一用户在工作中与在家中可能具有显著不同的行为。因此,通用的行为规则可能无法捕获真实用户的多样性及特异性。与此类常规系统相对照,在本发明的一些实施例中,对照捕获每一客户端系统本身及/或类似客户端的正常/基线行为的模型选择性地检视及分析在相应客户端系统上发生的事件。换种方式来说,行为“正常性”的边界可使用实质特异性进行定义:特定客户端机器、特定的用户群组(例如,公司的特定部门、家族成员、特定年龄段)等。

[0093] 由于软件及因特网使用的激增,开发高度特定的行为配置文件(例如,附加到每一个别用户的配置文件)的尝试可能需要不合理的计算资源,且因此可能是不切实际的。此外,从个别用户/机器收集事件可能无法提供足够的数据来开发统计上稳健的行为模型。与此方法相对照,本发明的一些实施例将多个用户及/或机器分组到单个客户端配置文件中,从而确保了特异性、稳健性与计算成本之间的有用折衷。此外,将用户及机器分组为配置文件的方式本身就是基于行为准则的,以确保此类分组保留特异性。在一些实施例中,每一客户端配置文件群组将具有基本上类似的事件配置文件的用户/机器分组在一起。换种方式来说,就在成员机器上发生的事件的统计而言,客户端配置文件的所有成员都显示类似的

基线行为。

[0094] 一些常规的计算机安全系统及方法主要分析个体事件。在计算机系统的操作期间发生的许多事件(例如,打开文件、访问网页)在孤立进行时可能并不指示恶意。然而,当其在其它事件的上下文中发生时(例如,作为特定的动作序列),其可能是恶意的。与更常规的解决方案相对照,本发明的一些实施例在上下文中显式地分析事件,且因此更适合于此类事件相关情况。优选实施例将个别事件表示为多维嵌入空间中的向量,其具有独特的性质,使得在相同事件上下文中以相对较高的频率发生的一对事件比在同一事件上下文中发生频率较低的另一对事件分开的距离更小。

[0095] 成功的行为建模可能需要检测大量(例如,数百或数千)相异事件类型,但并非所有事件类型在行为建模中都可同等重要的。收集及分析从大量来源接收到的关于此类众多事件类型的统计数据可能是不切实际的。为了解决此问题,一些实施例根据事件之间的相似度将事件分组为事件类别或集群,从而创建更稳健及/或相关的统计。此有意义的降维可显著促进客户端配置文件的构建。可根据若干准则来确定事件相似性,例如,根据在事件嵌入空间中两个事件分开的距离。在优选实施例中,如果两个事件主要发生在相同的上下文中,那么可认为它们是相似的(例如,当事件A及B两者经常在事件X后面及/或在事件Y前面时,即,如在示范性序列XAY及XBY中,事件A与B被认为是相似的)。

[0096] 图17-A到B说明将上文描述的一些系统及方法应用于计算机安全威胁的检测的实验。从多个被监测的客户端收集的事件的事件语料库用于如上文展示那样训练分析引擎的组件,从而导致将被监测的客户端分为11个客户端集群/配置文件。根据每一事件在15维嵌入空间中的表示,将事件分为几个事件类别。针对每一相应客户端集群开发了配置文件特定的行为模型。接着,在测试机上发起特定类型的攻击。从测试机收集的事件序列被馈送到异常检测器,所述异常检测器又使用特定于行为模型中的每一者的参数实例化。一些此类事件序列被检测为异常。

[0097] 图17-A展示集群特定的异常分数,以等级表示,其中分数1表示异常的100%确定性(例如,从测试机接收到的事件序列中的至少一个事件在训练中尚未被看到)。曲线图表示在异常事件序列上求平均的分数值及相关联的标准差。所述图展示,可将相同序列视为具有集群特定的确定性级别的异常。换种方式来说,与在其它客户端上相比,在某些客户端上,同一事件序列被认为“异常程度更低”。例如,与集群1、2及7相关联的行为模型不仅比其它模型检测到攻击的效率要高,而且与攻击相关联的所有事件序列都被认为“同样异常”。相比之下,与集群0及9相关联的模型指示同一攻击的一些事件序列比其它事件序列“异常程度更低”。

[0098] 图17-B展示针对三种相异类型的攻击实现的配置文件特定的平均检测率。使用11种配置文件特定的经训练行为模型中的每一者分析在每一类型的攻击期间从测试机收集的事件序列。检测率在模型及攻击类型之间不同,此进一步证实了本文中描述的一些系统及方法的特异性。

[0099] 此类实验结果指示本发明一些实施例的另一潜在应用。集中式计算机安全解决方案可为由客户端配置文件识别的每一组客户端及/或与每一客户端集群的原型具有相似性的其它客户端选择性地开发保护策略。一些实施例可识别本文中描述的方法为其提供令人满意的安全程度的客户端集群,以及需要额外安全措施的其它客户端集群。为每一客户端

集群定制保护可改善用户体验并减少不必要的计算费用。

[0100] 对于所属领域的技术人员将显而易见的是,在不脱离本发明的范围的情况下,可以许多方式改变上述实施例。因此,本发明的范围应由所附权利要求书及其合法等效物确定。

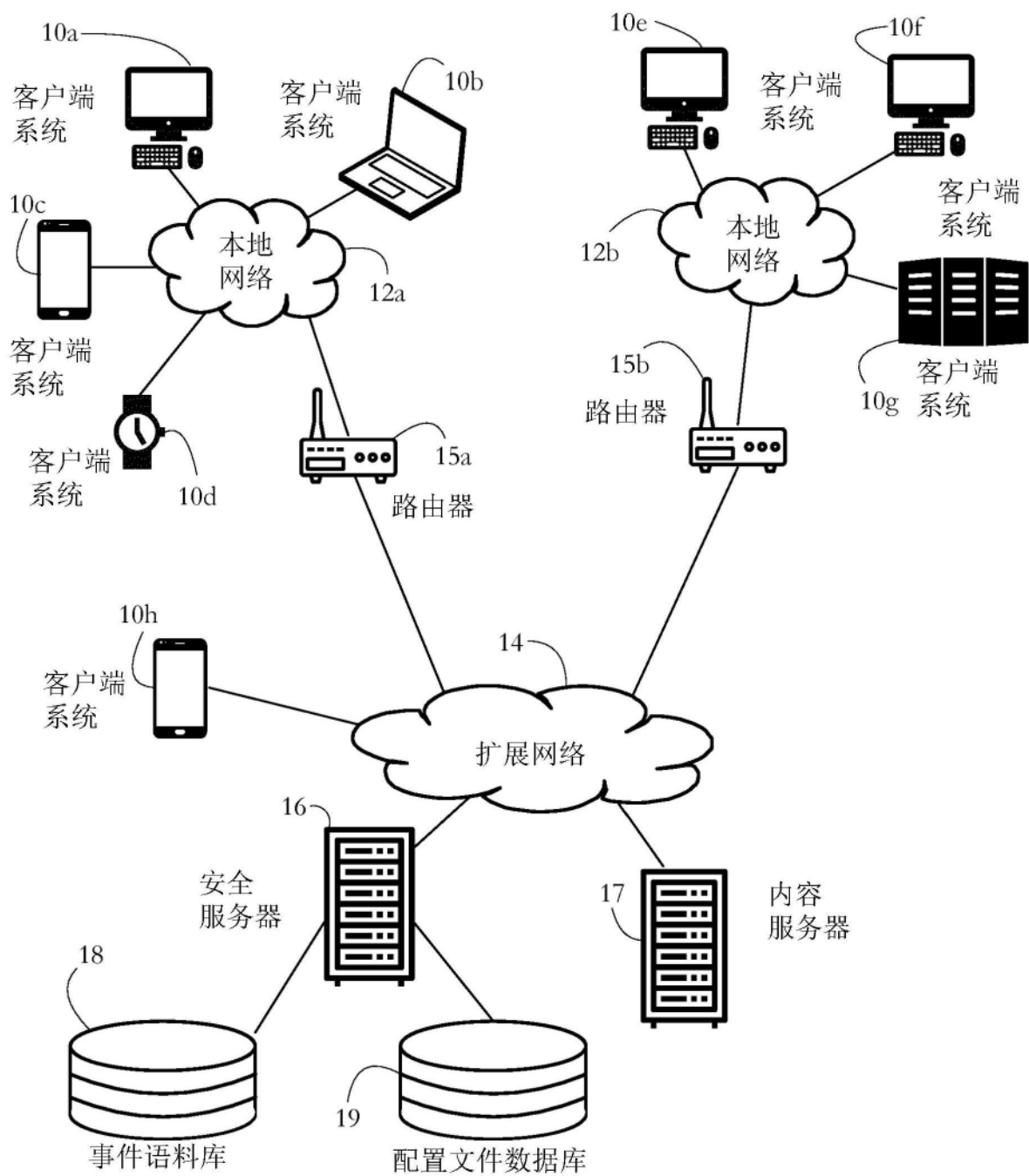


图1

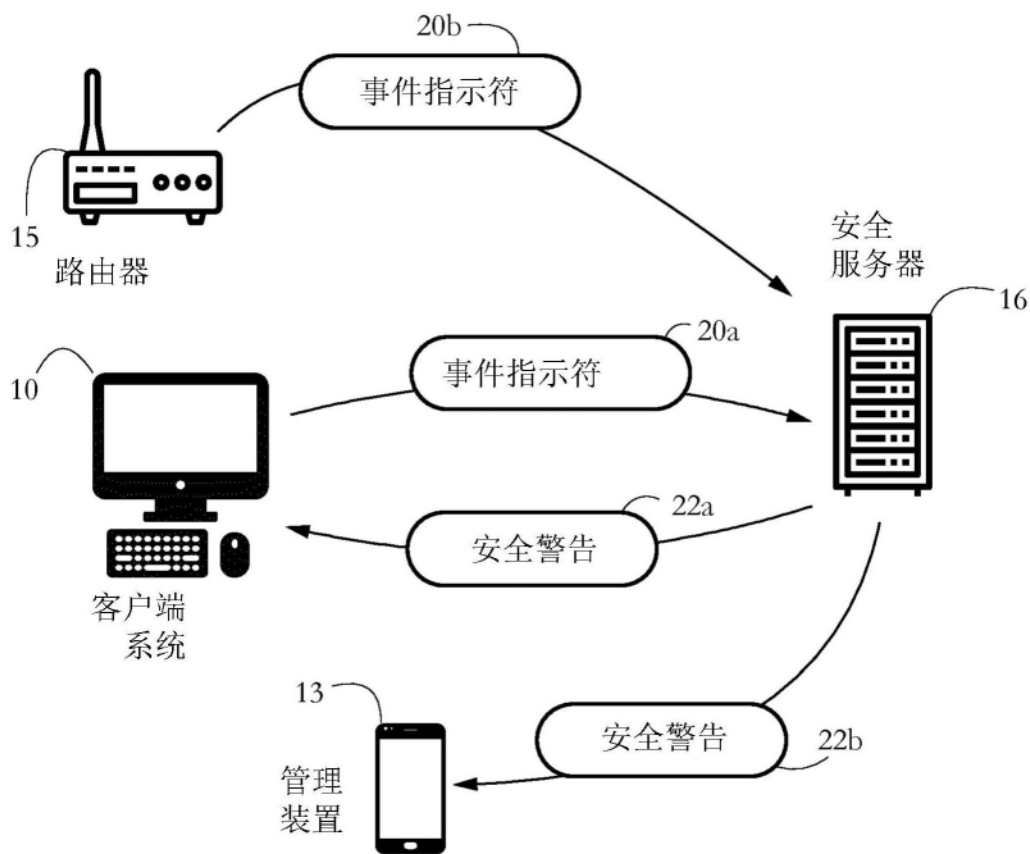


图2

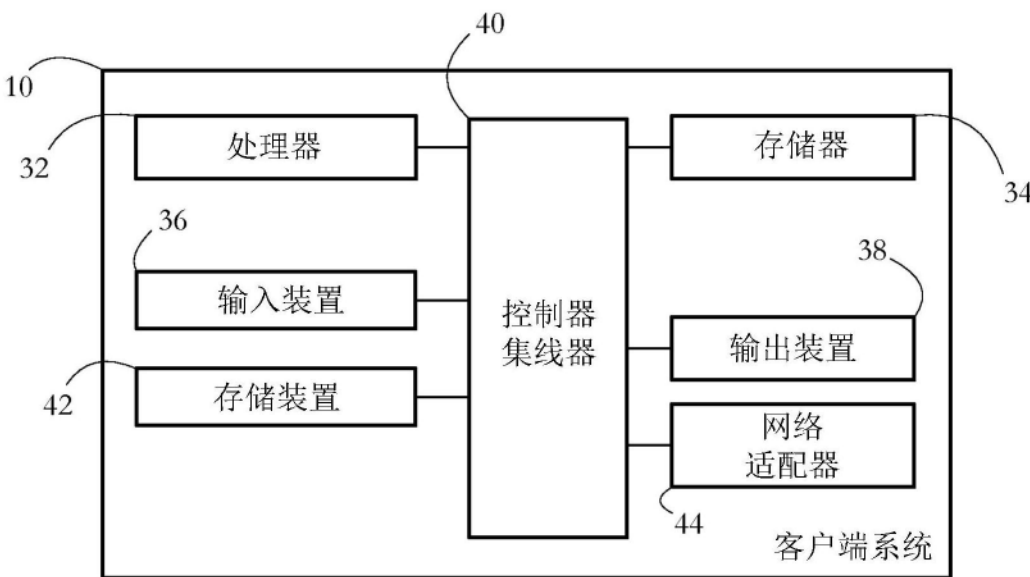


图3-A

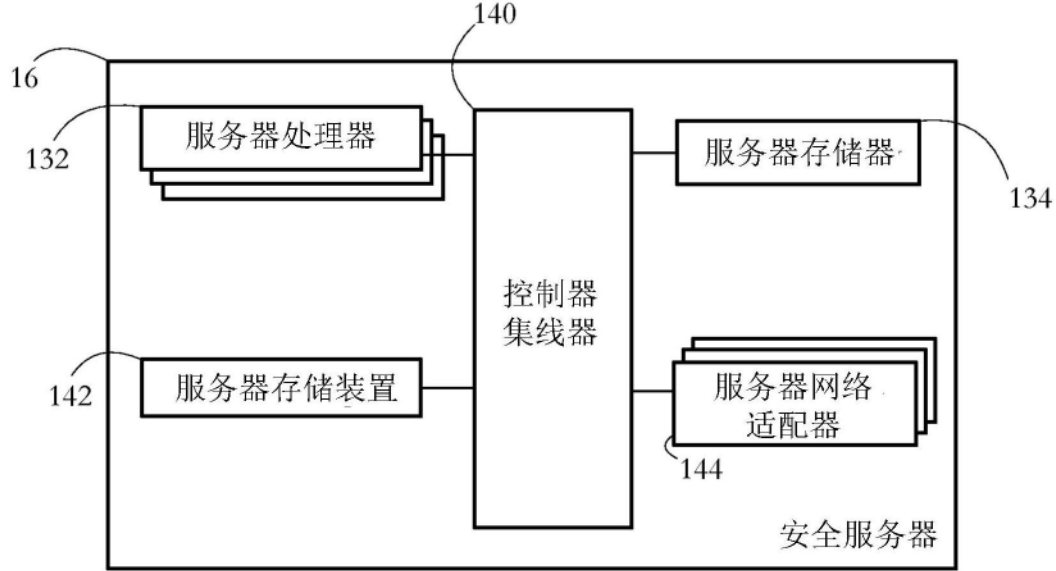


图3-B

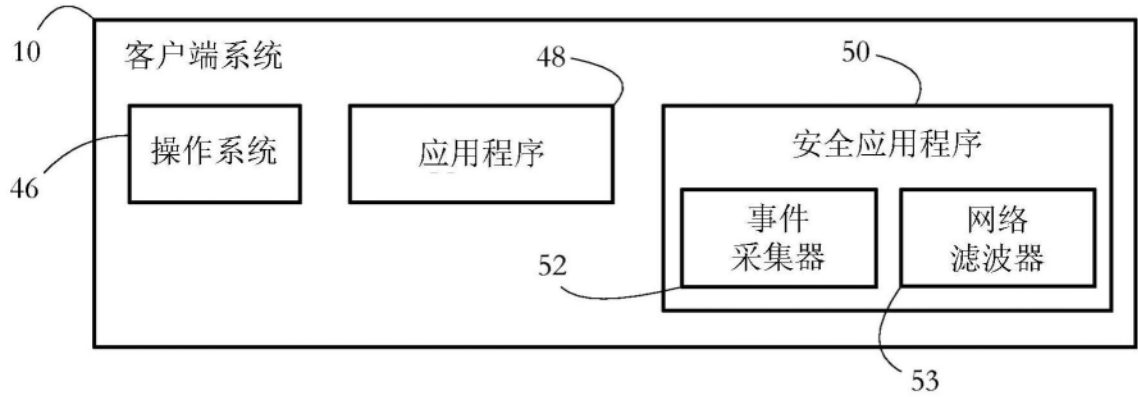


图4

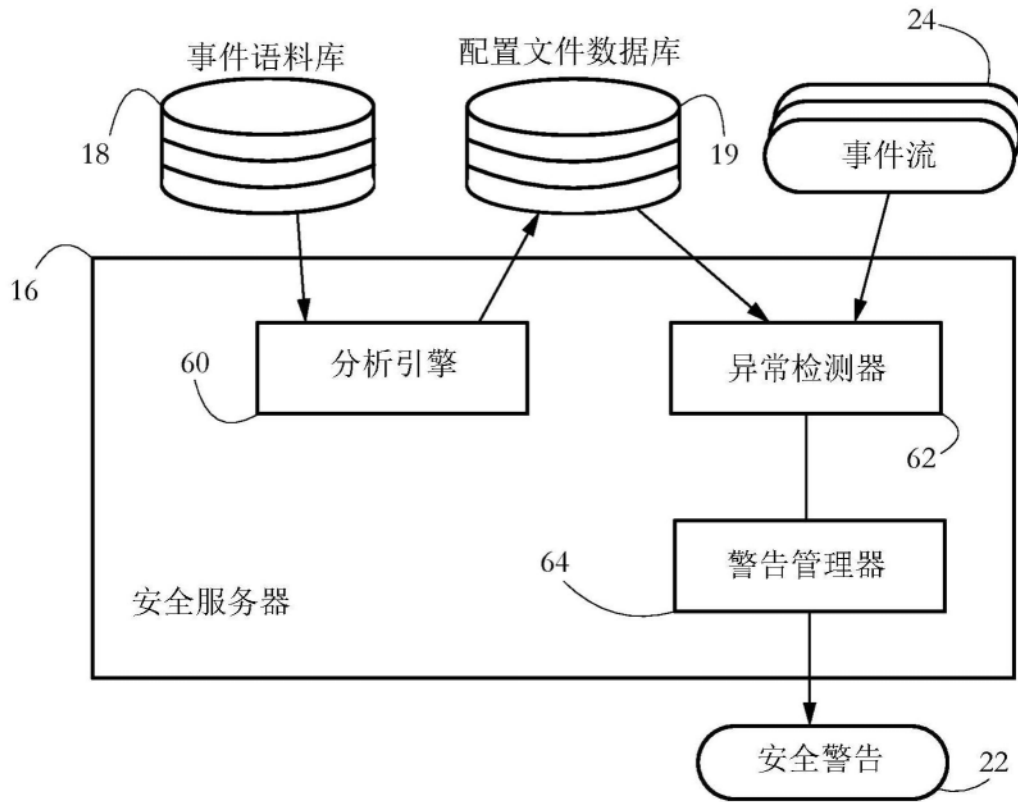


图5

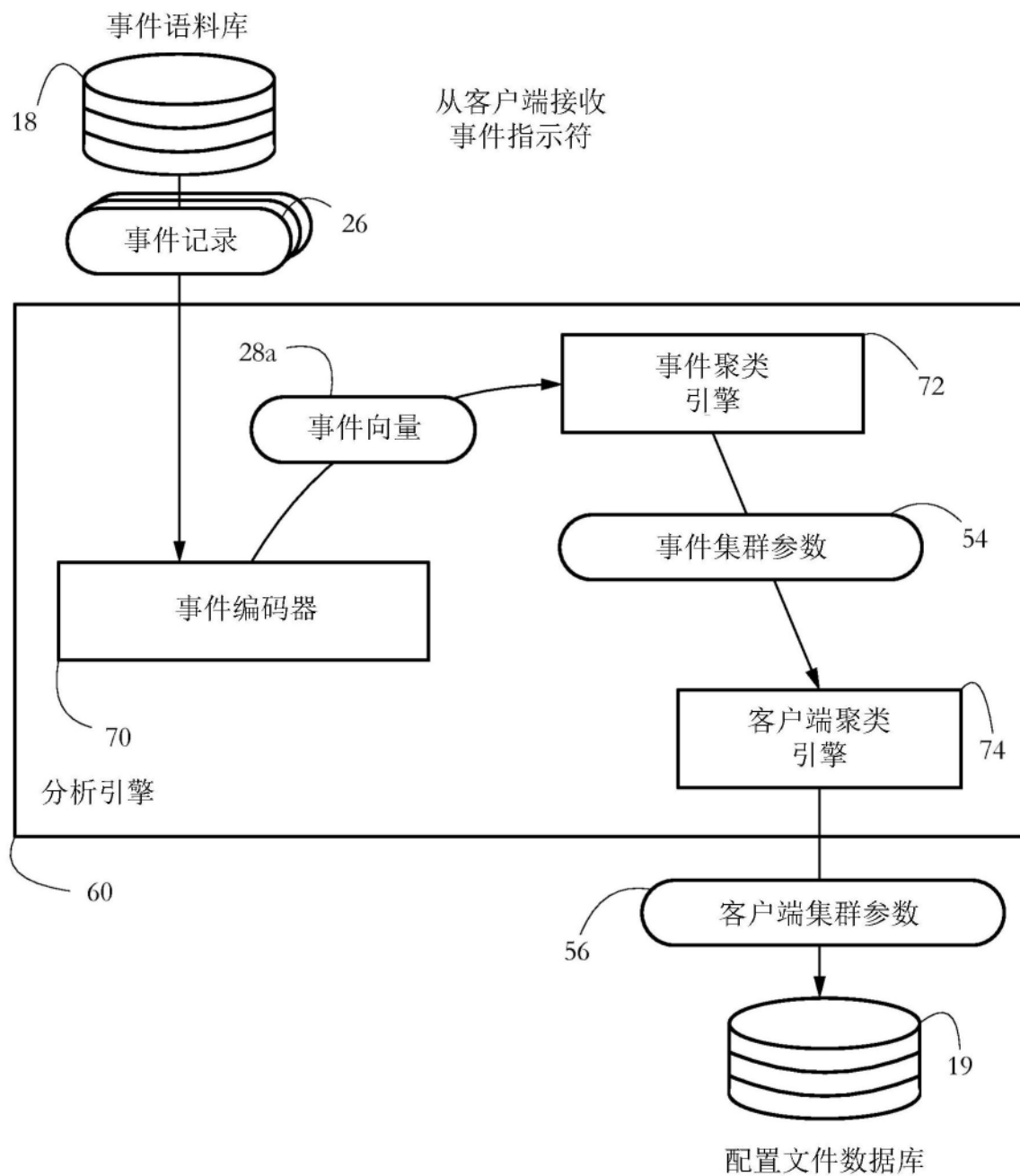


图6

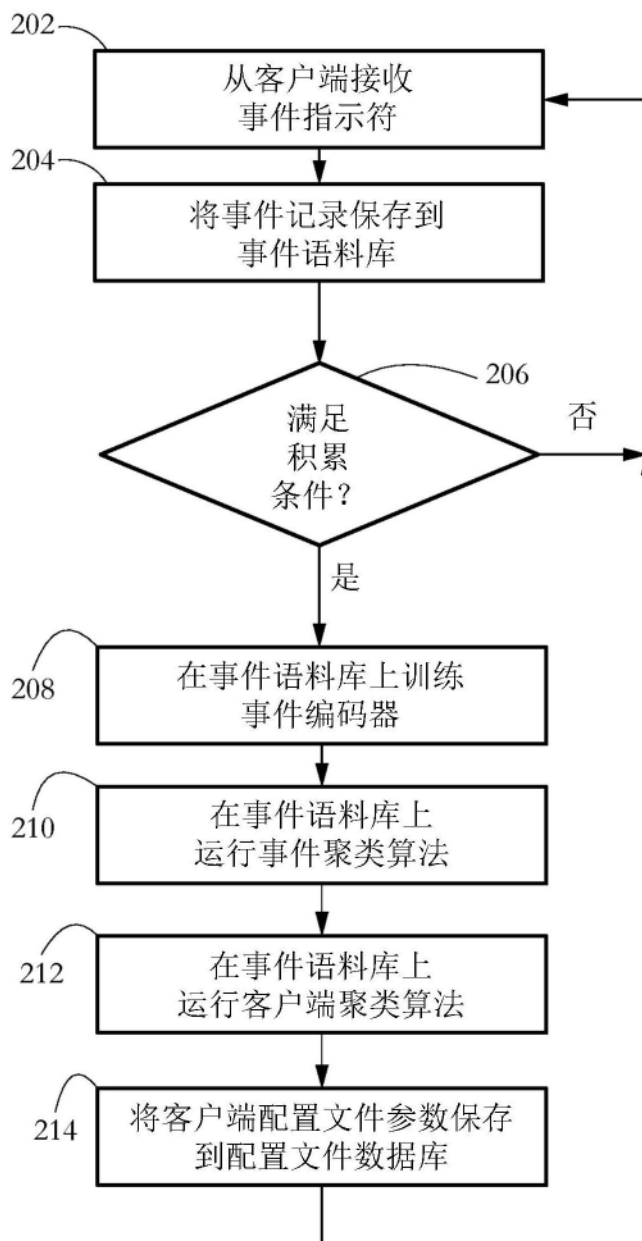


图7

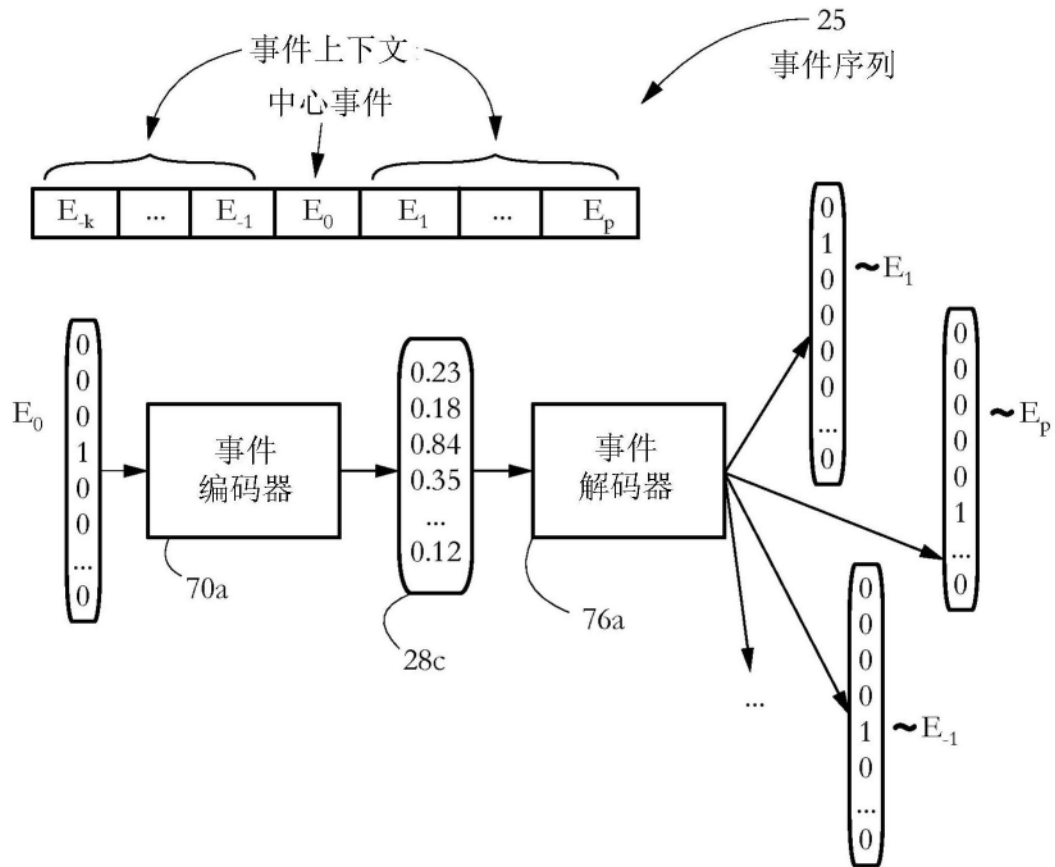


图8-A

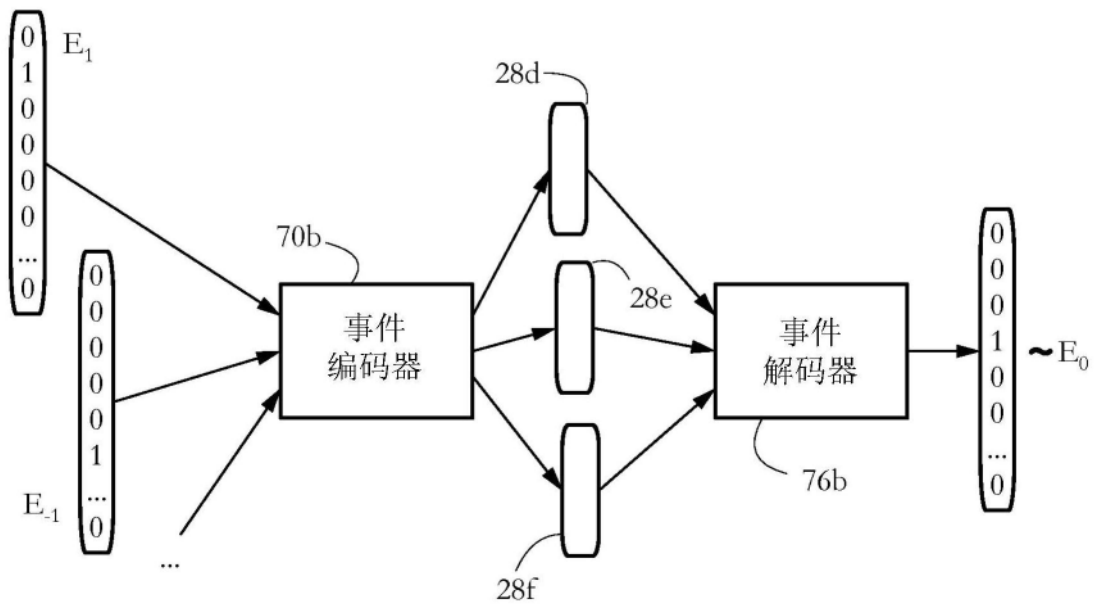


图8-B

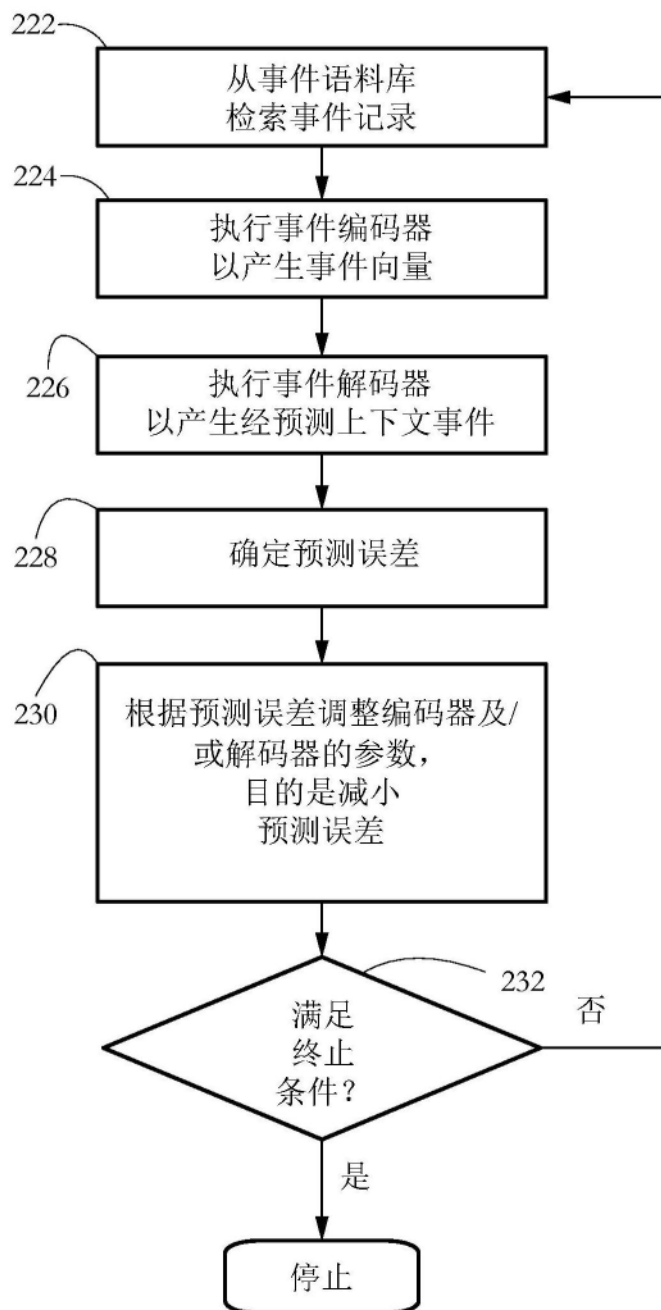


图9

嵌入维度2

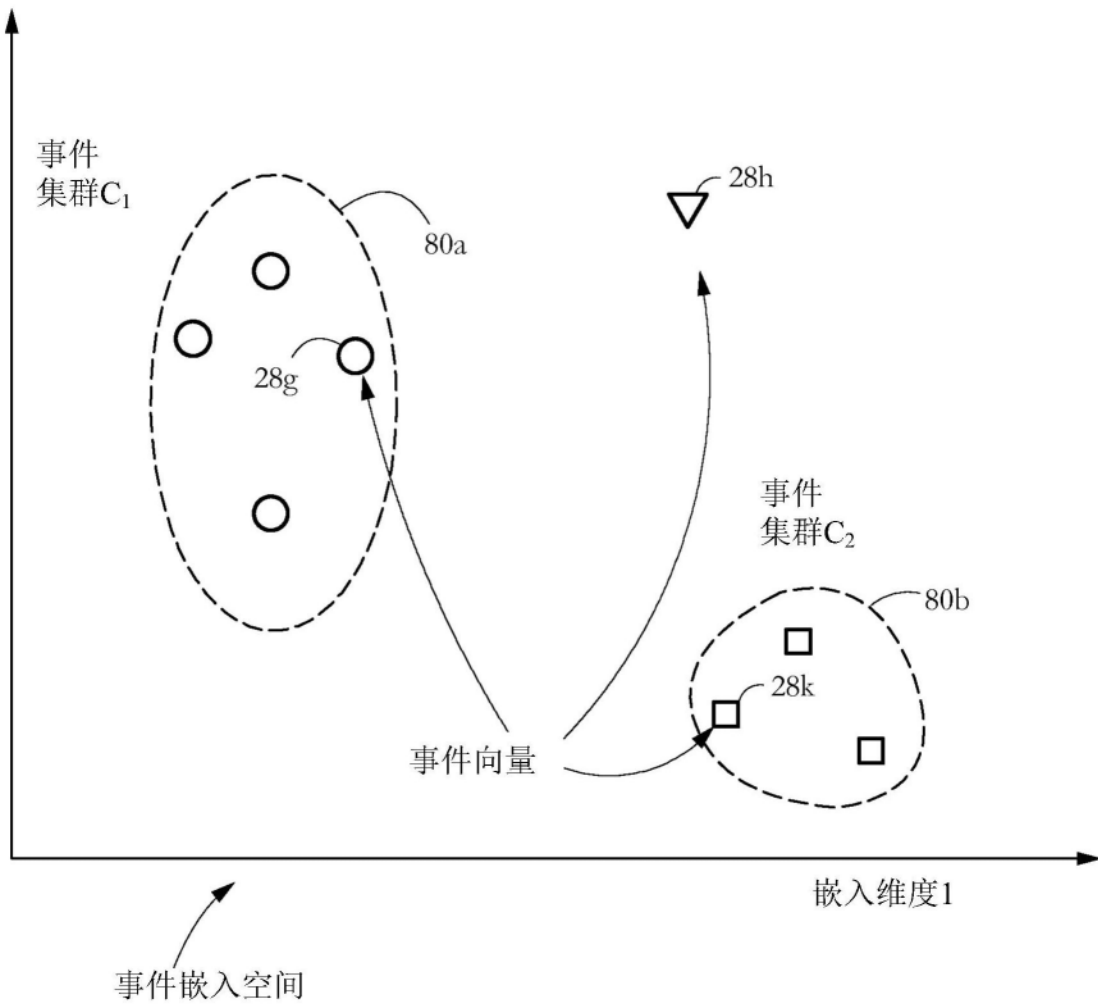


图10

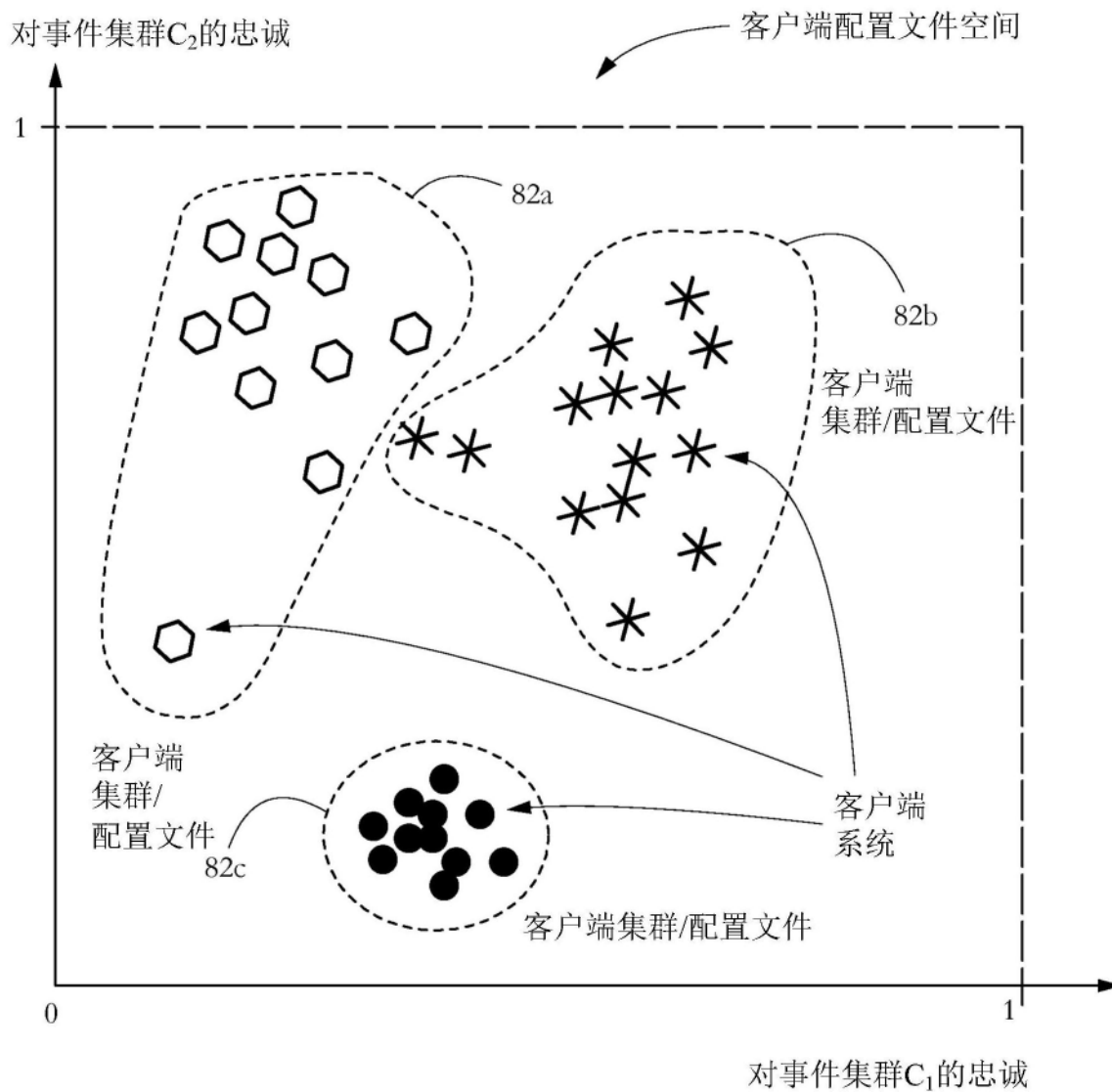


图11

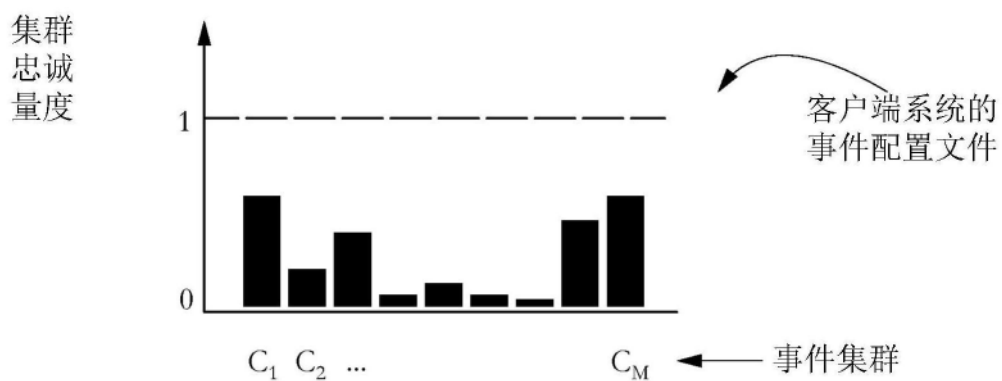


图12

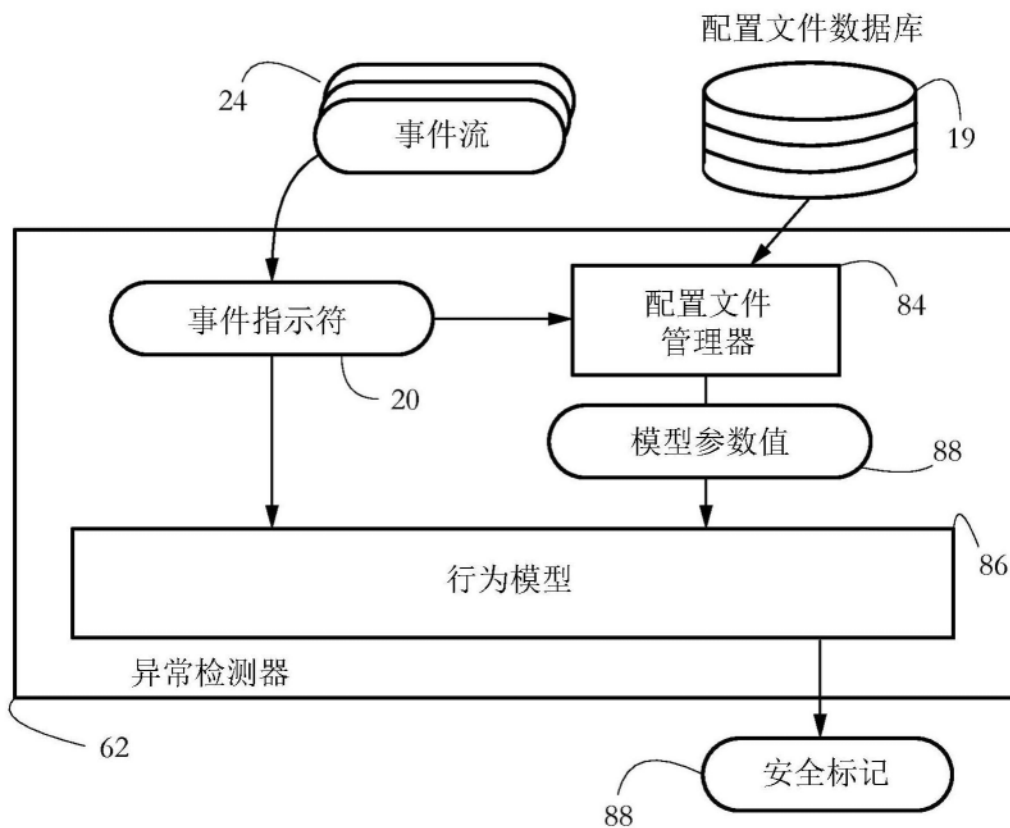


图13

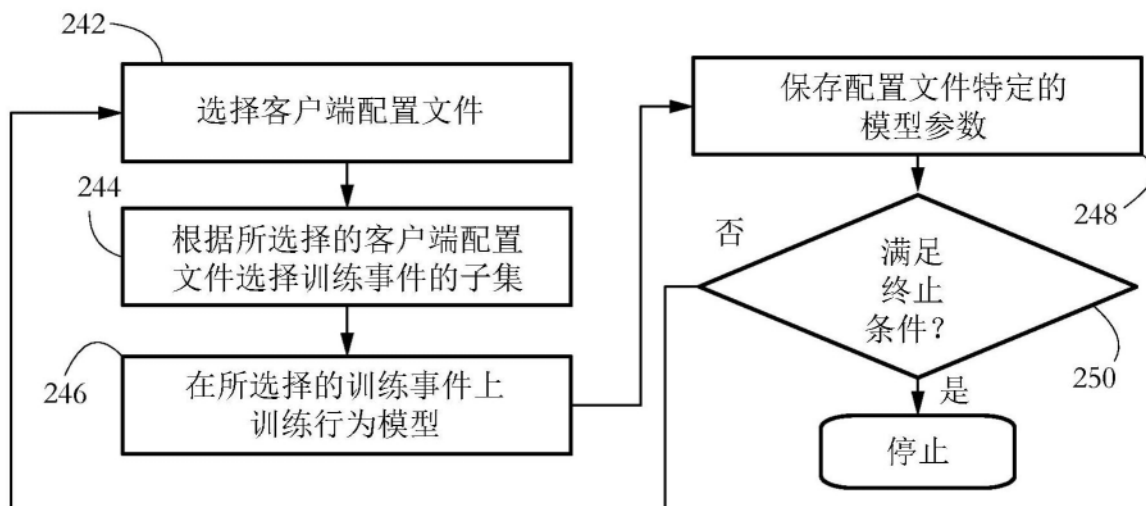


图14

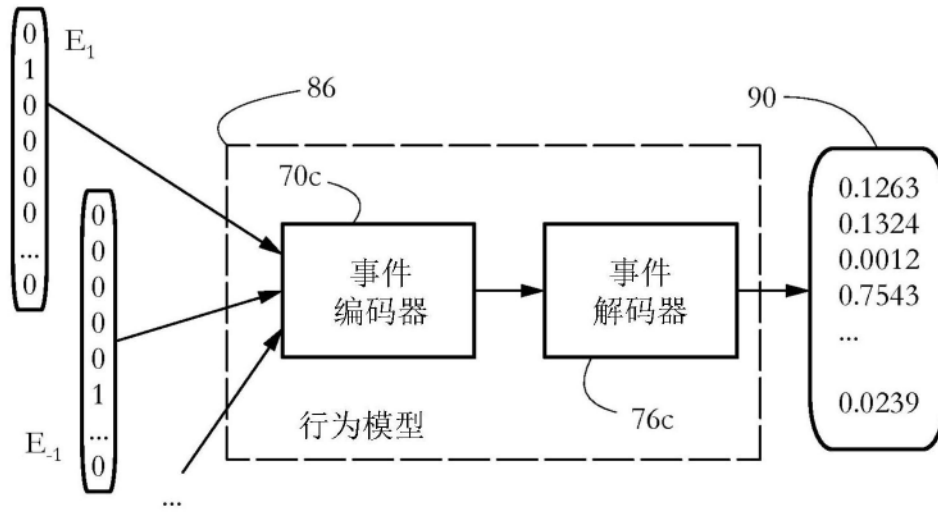


图15

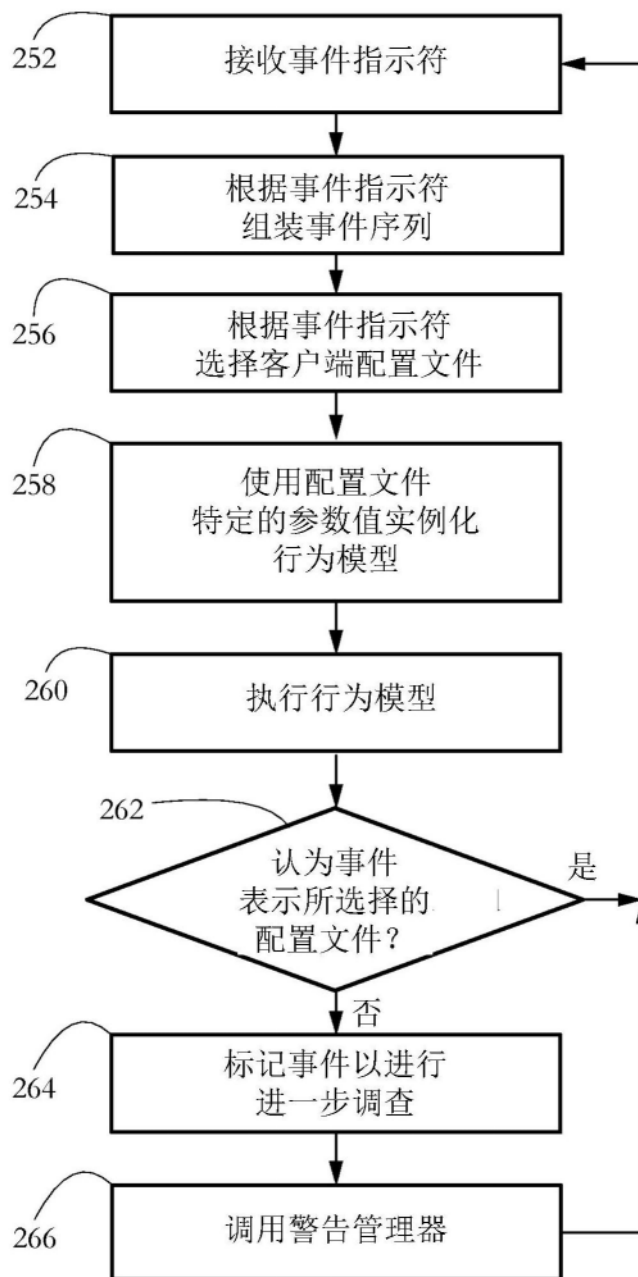


图16

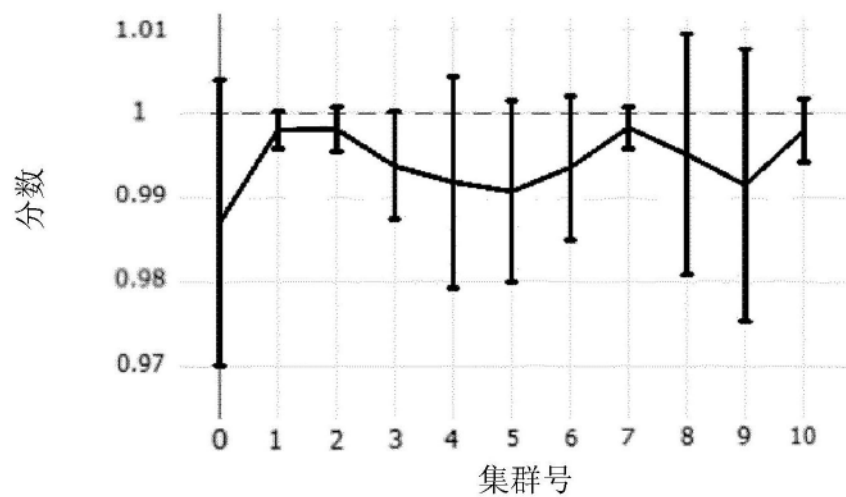


图17-A

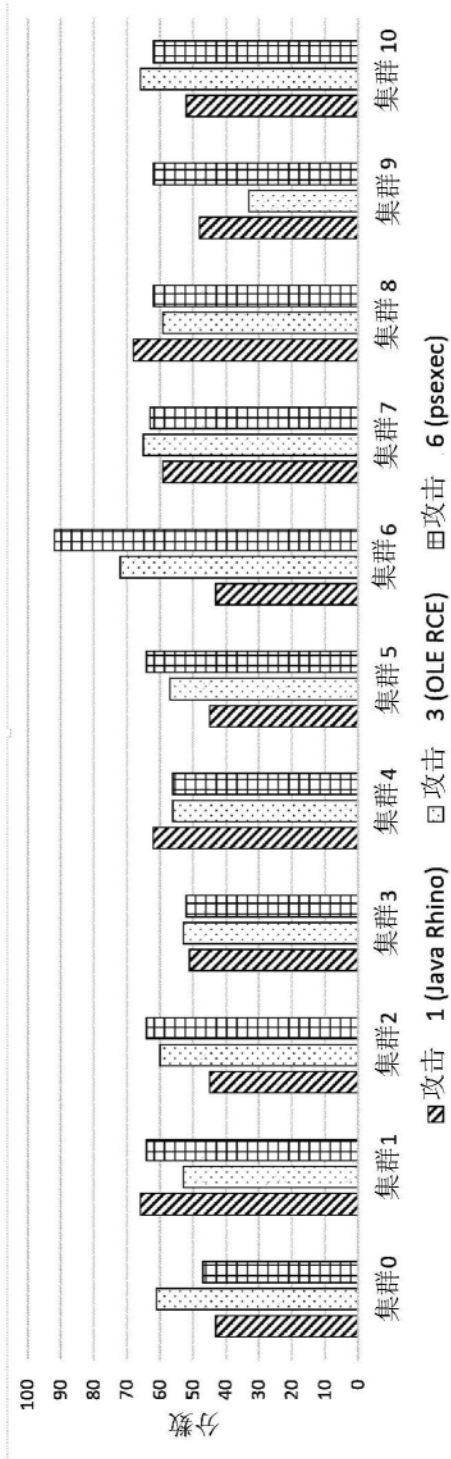


图17-B