(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115242531 A
(43)申请公布日 2022.10.25

(21)申请号 202210889059.5

(22)申请日 2022.07.27

(71)申请人 上海齐屹信息科技有限公司
地址 201824 上海市嘉定区曹安公路1926号1幢

(72)发明人 邱振毅 邓华金 周海军 刘靖

(74)专利代理机构 上海创开专利代理事务所(普通合伙) 31374
专利代理师 汪发成

(51)Int.Cl.
H04L 9/40(2022.01)

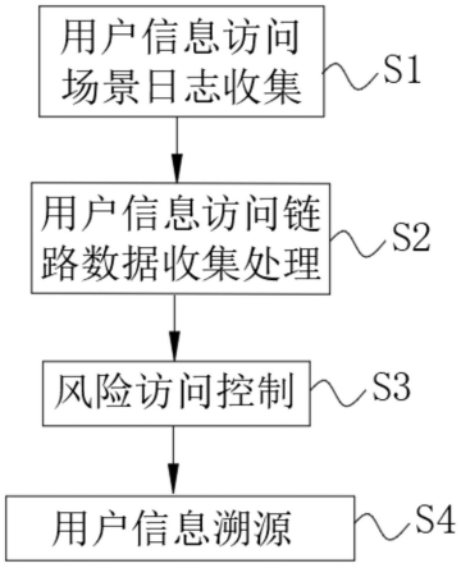
权利要求书2页 说明书7页 附图4页

(54)发明名称

一种跨系统多场景跟踪用户信息的方法

(57)摘要

本发明公开了一种跨系统多场景跟踪用户信息的方法，涉及数据安全技术领域。本发明包括如下步骤：S1、用户信息访问场景日志收集；S2、用户信息访问链路数据收集处理；S3、风险访问控制；S4、用户信息溯源。本发明满足不同场景、不同系统、不同用户角色的信息访问跟踪记录的需求，同时通过对记录数据的集中处理，减少了衍生数据的干扰，实时的风控预警可以及时提醒企业信息安全管理人员对可能存在用户信息的风险访问人和风险用户进行关注，且提供了多维度的用户信息访问记录查询，能够对异常访问进行拦截处理，对可能存在用户信息事件的行为进行预警，可以根据用户及访问者进行溯源。



CN 115242531 A

1.一种跨系统多场景跟踪用户信息的方法,其特征在于,包括如下步骤:

S1、用户信息访问场景日志收集:具体涉及用户信息访问的系统,功能场景进行详细的日志记录,在数据传递过程中调用chain用于记录访问的源信息;所述用户信息访问场景日志收集具体包括用户信息访问场景、系统重点关注的用户信息访问场景、用户信息访问场景日志埋点收集、重点数据chain模型及用户信息访问事件形成四个步骤;

所述用户信息访问场景日志收集是根据公司现有业务系统列出所有访问用户信息场景,其中重点访问场景是对访问者进行重点标记,标记能够定位到具体访问者以及是否访问用户敏感信息;所述系统重点关注的用户信息访问场景包括对应的用户注册、装修活动报名、客户资料新增、查询客户基本信息、客户信息批量查看、进线客户资料查询所涉及到用户敏感信息访问的业务场景需要重点进行标记跟踪;所述用户信息访问场景日志埋点收集是在用户访问场景的关键接口请求日志中,加入chain参数用于记录访问者源数据信息;所述重点数据chain模型及用户信息访问事件形成包括访问者数据模型以及完整信息模型;所述访问者数据模型具体是:调用人→功能→行为→ip链路,在数据的流转衍生过程中,用于记录访问者的信息流转记录,即使数据不断的流转衍生,依然能够在系统中确认访问者的源信息;所述完整信息模型具体是:调用人角色-场景-调用人店铺-调用人-调用人名称-调用来源系统-调用者IP→被查阅服务→服务地址→服务说明→被查阅的信息→查阅的信息类型→查阅信息归属用户→时间,在数据流转日志清洗机解析完毕后,结合上下文数据补全完整的访问信息模型,得到完整的用户信息访问事件;

S2、用户信息访问链路数据收集处理:根据用户信息访问场景的上下文信息建立对应的用户信息访问事件,主要围绕时间、访问者、访问目标、访问行为四点进行延伸;所述用户信息访问链路数据收集处理包括用户信息访问chain数据处理、用户信息访问事件要素补全两个步骤;

S3、风险访问控制:用户信息访问事件生成后,提供不同维度统计,根据对应的风控规则进行风险访问控制和风险预警,具体包括根据访问者的角色设置匹配不同的风控策略、按照固定周期统计用户信息访问事件频率并执行风控策略后生成用户信息访问统计结果、用户信息风险访问管理;

S4、用户信息溯源:用户信息事件发生后,在系统中根据用户ID快速查询用户信息的访问历史记录,进行快速准确的溯源。

2.根据权利要求1所述的一种跨系统多场景跟踪用户信息的方法,其特征在于,所述S1步骤中,访问者源数据信息根据不同的场景记录不同的维度数据,关键的场景明确到包括访问者的角色、来源ip、访问者id在内的详细信息。

3.根据权利要求1所述的一种跨系统多场景跟踪用户信息的方法,其特征在于,所述S2步骤中用户信息访问chain数据处理是指chain数据主要记录了访问者的源信息,需要根据系统、场景并集合上下文进行解析,补全用户信息访问事件数据,具体包括如下步骤:

P1、确认用户信息访问场景,在各个系统的日志进行埋点,对涉及用户信息访问的日志进行标记,接入ELK日志系统中,集中采集各个系统日志;

P2、对原始的日志进行解析、清洗、过滤、合并,根据日志中的标记,提取出涉及用户信息访问的关键日志;

P3、涉及用户信息访问的日志进行解析、拆分、标记处理;

P4、从拆分、解析后的日志中抽取用户信息访问行为的关键信息，所述关键信息包括访问时间、访问者、访问目标、关键行为；

P5、根据场景对解析后的日志进行初步的标注，结合日志上下文补全访问者以及被访问者信息。

4.根据权利要求1所述的一种跨系统多场景跟踪用户信息的方法，其特征在于，所述S2步骤中用户信息访问事件要素补全具体包括如下步骤：

Q1、获取用户信息访问的原始调用链chain数据，根据其中的访问者信息，匹配缓存数据，补全被访问者的详细信息；所述详细信息包括访问归属系统、来源ip、访问者id，最终能够在系统中清晰的描述访问者；

Q2、根据日志上下文，确定访问目标的主体，匹配缓存数据，补全包括被访问者id、被访问的内容在内的被访问者的详细信息；

Q3、根据访问场景、日志标注、确定访问者行为，访问目标内容，确定访问行为是否合理；

Q4、组装用户信息访问行为源数据，组装后的数据进入数据仓库中进行处理，并生成详细的用户访问事件，所述处理包括大数据批量处理以及风控规则。

5.根据权利要求1所述的一种跨系统多场景跟踪用户信息的方法，其特征在于，所述S3步骤中，用户信息风险访问管理具体包括如下步骤：

F1、风险访问者列表支持手动添加，可手动添加风险用户信息，风险访问者信息，实时监控用户信息访问情况；

F2、当经过风控规则过滤，标记为风险访问事件中的访问者，被访问者，添加记录在风险访问表中，相应的用户信息访问时间发生时，进行风险预警。

一种跨系统多场景跟踪用户信息的方法

技术领域

[0001] 本发明属于数据安全技术领域，特别是涉及一种跨系统多场景跟踪用户信息的方法。

背景技术

[0002] 目前市面上用户信息时间屡见不鲜，很多平台对用户信息行为都没有建立有效的反应机制和追溯机制，不能够有效的防止用户信息。在信息事件发生时，企业不能快速有效的察觉。用户信息事件一旦发生，企业不能够及时发现并处理，往往会给企业和用户造成巨大的损失。市面上常见的用户防护主要还是通过安全软件对企业内部的应用、机器等进行扫描查杀，这种方式仍然处于一个初级的保护阶段，只能防范部分病毒感染系统漏洞造成的个人信息。对于生产管理的信息安全问题，虽然不少企业都有设置信息安全规章制度，但是这些管理制度通常不能够及时启动并发挥作用，有些规定也并没有量化，存在管理的灰色地带。当用户信息事件发生时，企业不能够有效的察觉，往往在用户遭受骚扰并主动投诉后，企业才感知到用户信息事件的发生。由于很多企业没有完善的用户信息访问记录系统，也难以对用户信息时间进行追溯。

[0003] 因此，现有的技术中对应处理信息问题具有以下缺点与不足：(1)防护依赖于安全扫描，信息具有延迟性：以往用户信息事件的预防主要还是通过定期对系统进行安全扫描，及时更新安全软件，普及信息安全知识等方式，虽然市面上的安全产品众多，但是大部分都是依赖于公开的漏洞、病毒信息库；一旦最新的漏洞出现时，企业依然遭受黑客的供给，被窃取用户信息，用户信息发生时，企业也不能及时的感知，通常都是在用户遭到骚扰投诉后，企业才会知晓用户的信息遭受了窃取，但已经给企业造成了损失，用户也受到了骚扰，为时已晚；(2)用户信息途径追查困难：用户信息事件发生后，大多数企业还是采用的传统的静态信息资源追溯，查看系统访问日志等方式处理；但是在目前的环境下用户信息调用链路数据经过层层调用传递，数据的生成规模、设计系统错综复杂以及干扰数据的衍生，给传统的用户信息溯源带来了巨大挑战；如果不对源数据的访问信息进行系统性的记录，将在很大程度上降低数据的真实性和有效性，对用户信息访问记录溯源造成了巨大的干扰；传统的数据溯源是一种溯本追源的技术，根据追溯路径重现数据的历史状态和调用过程，实现数据历史档案的追溯；当用户信息发生时，可通过追溯对溯源对数据的处理阶段进行定位，但很难定位到具体的访问源；因此，针对以上问题，提供一种跨系统多场景跟踪用户信息的方法具有重要实际意义。

发明内容

[0004] 本发明提供了一种跨系统多场景跟踪用户信息的方法，解决了以上问题。

[0005] 为解决上述技术问题，本发明是通过以下技术方案实现的：

[0006] 本发明的一种跨系统多场景跟踪用户信息的方法，包括如下步骤：

[0007] S1、用户信息访问场景日志收集：具体涉及用户信息访问的系统，功能场景进行详

细的日志记录，在数据传递过程中调用chain用于记录访问的源信息；所述用户信息访问场景日志收集具体包括用户信息访问场景、系统重点关注的用户信息访问场景、用户信息访问场景日志埋点收集、重点数据chain模型及用户信息访问事件形成四个步骤；

[0008] 所述用户信息访问场景日志收集是根据公司现有业务系统列出所有访问用户信息场景，其中重点访问场景是对访问者进行重点标记，标记能够定位到具体访问者以及是否访问用户敏感信息；所述系统重点关注的用户信息访问场景包括对应的用户注册、装修活动报名、客户资料新增、查询客户基本信息、客户信息批量查看、进线客户资料查询所涉及到用户敏感信息访问的业务场景需要重点进行标记跟踪；所述用户信息访问场景日志埋点收集是在用户访问场景的关键接口请求日志中，加入chain参数用于记录访问者源数据信息；所述重点数据chain模型及用户信息访问事件形成包括访问者数据模型以及完整信息模型；所述访问者数据模型具体是：调用人→功能→行为→ip链路，在数据的流转衍生过程中，用于记录访问者的信息流转记录，即使数据不断的流转衍生，依然能够在系统中确认访问者的源信息；所述完整信息模型具体是：调用人角色-场景-调用人店铺-调用人-调用人名称-调用来源系统-调用者IP→被查阅服务→服务地址→服务说明→被查阅的信息→查阅的信息类型→查阅信息归属用户→时间，在数据流转日志清洗机解析完毕后，结合上下文数据补全完整的访问信息模型，得到完整的用户信息访问事件；

[0009] S2、用户信息访问链路数据收集处理：根据用户信息访问场景的上下文信息建立对应的用户信息访问事件，主要围绕时间、访问者、访问目标、访问行为四点进行延伸；所述用户信息访问链路数据收集处理包括用户信息访问chain数据处理、用户信息访问事件要素补全两个步骤；

[0010] S3、风险访问控制：用户信息访问事件生成后，提供不同维度统计，根据对应的风控规则进行风险访问控制和风险预警，具体包括根据访问者的角色设置匹配不同的风控策略、按照固定周期统计用户信息访问事件频率并执行风控策略后生成用户信息访问统计结果、用户信息风险访问管理；

[0011] S4、用户信息溯源：用户信息事件发生后，在系统中根据用户ID快速查询用户信息的访问历史记录，进行快速准确的溯源。

[0012] 进一步地，所述S1步骤中，访问者源数据信息根据不同的场景记录不同的维度数据，关键的场景明确到包括访问者的角色、来源ip、访问者id在内的详细信息。

[0013] 进一步地，所述S2步骤中用户信息访问chain数据处理是指chain数据主要记录了访问者的源信息，需要根据系统、场景并集合上下文进行解析，补全用户信息访问事件数据，具体包括如下步骤：

[0014] P1、确认用户信息访问场景，在各个系统的日志进行埋点，对涉及用户信息访问的日志进行标记，接入ELK日志系统中，集中采集各个系统日志；

[0015] P2、对原始的日志进行解析、清洗、过滤、合并，根据日志中的标记，提取出涉及用户信息访问的关键日志；

[0016] P3、涉及用户信息访问的日志进行解析、拆分、标记处理；

[0017] P4、从拆分、解析后的日志中抽取用户信息访问行为的关键信息，所述关键信息包括访问时间、访问者、访问目标、关键行为；

[0018] P5、根据场景对解析后的日志进行初步的标注，结合日志上下文补全访问者以及

被访问者信息。

[0019] 进一步地,所述S2步骤中用户信息访问事件要素补全具体包括如下步骤:

[0020] Q1、获取用户信息访问的原始调用链chain数据,根据其中的访问者信息,匹配缓存数据,补全被访问者的详细信息;所述详细信息包括访问归属系统、来源ip、访问者id,最终能够在系统中清晰的描述访问者;

[0021] Q2、根据日志上下文,确定访问目标的主体,匹配缓存数据,补全包括被访问者id、被访问的内容在内的被访问者的详细信息;

[0022] Q3、根据访问场景、日志标注、确定访问者行为,访问目标内容,确定访问行为是否合理;

[0023] Q4、组装用户信息访问行为源数据,组装后的数据进入数据仓库中进行处理,并生成详细的用户访问事件,所述处理包括大数据批量处理以及风控规则。

[0024] 进一步地,所述S3步骤中,用户信息风险访问管理具体包括如下步骤:

[0025] F1、风险访问者列表支持手动添加,可手动添加风险用户信息,风险访问者信息,实时监控用户信息访问情况;

[0026] F2、当经过风控规则过滤,标记为风险访问事件中的访问者,被访问者,添加记录在风险访问表中,相应的用户信息访问时间发生时,进行风险预警。

[0027] 本发明相对于现有技术包括有以下有益效果:

[0028] 1、本发明提供了多个场景的数据模型,满足不同场景、不同系统、不同用户角色的信息访问跟踪记录的需求,同时通过对记录数据的集中处理,减少了衍生数据的干扰,实时的风控预警可以及时提醒企业信息安全管理人员对可能存在用户信息的风险访问人和风险用户进行关注,且提供了多维度的用户信息访问记录查询,可以根据用户及访问者进行溯源;

[0029] 2、本发明解决不能及时发现用户信息事件以及用户信息访问溯源困难的问题,对比以往的技术,构建了一个用户信息访问跟踪系统,汇集了用户信息访问场景,访问者根据角色维度进行分类标记,并且对访问源头进行了访问链路标记,根据用户信息访问场景和上下游日志批注出此次访问涉及到的访问者和被访问用户的具体信息,能够定位到每个用户信息访问行为的具体人,同时根据风控规则标注此次访问是否合理,实现一个用户信息访问行为进行准确跟踪和信息预警的功能;收集用户信息相关日志数据,用于收集分析用户信息访问行为源数据,同时根据分析结果进行用户信息访问行为进行多维度审计,同时可根据用户访问记录不断的优化调整风控规则,对异常访问进行拦截处理,对可能存在用户信息事件的行为进行预警,当用户信息事件发生时,可通过用户信息访问记录查询,快速的实现溯源。

[0030] 当然,实施本发明的任一产品并不一定需要同时达到以上所述的所有优点。

附图说明

[0031] 为了更清楚地说明本发明实施例的技术方案,下面将对实施例描述所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅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。

[0032] 图1为本发明一种跨系统多场景跟踪用户信息的方法的步骤图；

[0033] 图2为使用本技术方法对应的系统的结构原理图；

[0034] 图3为具体实施例中S2步骤所形成的根据用户信息访问场景上下文信息建立对应的用户信息访问事件的软件系统界面截图；

[0035] 图4为具体实施例中S3步骤所生成的用户信息访问统计结果的软件系统界面截图；

[0036] 图5为具体实施例中S4步骤根据用户ID快速查询用户信息的访问历史记录并进行快速准确溯源的软件系统界面截图。

具体实施方式

[0037] 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前提下所获得的所有其它实施例，都属于本发明保护的范围。

[0038] 随着信息化和移动互联网的迅速发展，人们的生活体验更加便捷舒适，但与此同时，用户信息安全问题也逐步凸显。用户信息非法，倒卖用户信息等行为，导致用户接二连三的接到骚扰电话、垃圾短信，严重的干扰了用户生活。同时发生用户信息的企业，更是面临着用户投诉，监管审查，给企业造成了难以挽回的损失。互联网时代下的用户信息溯源也是困难重重。

[0039] 本发明方法及系统构建了基于用户信息访问场景，调用链路数据模型，用户信息风控预警规则，用户信息访问黑名单四方面的维度标准库，提供了实时用户信息访问行为跟踪以及用户信息预警规则，实现用户信息访问行为的实时追踪。对于黑名单中的访问进行拦截处理，在发生用户信息时进行预警，同时提供对用户信息访问行为的溯源功能。

[0040] 如图2所示，为本技术方案的跨系统多场景跟踪用户信息的方法对应的系统的结构原理示意图，由图中可知，其具体是获取包括商家中心、装修报名、ip地址等在内的行为原始数据，然后通过日志ES集群获得原始ELK数据，行为原始数据分别经过kafka行为队列、logstash数据预处理、Kaflka行为队列、logstash数据预处理、kaflka用户信息访问行为队列，半结构化数据、stom、hive大数据处理以及缓存数据、PG、页面展示查询、风控规则，黑名单以及行为预警等；对应的基于该系统，为了解决背景技术中的问题，本发明提出了如下技术方案：

[0041] 请参阅图1以及图3-5所示，本发明的一种跨系统多场景跟踪用户信息的方法，该技术方案主要有用户信息访问场景日志收集即场景库、用户信息访问场景调用链路模型数据集中处理即数据模型、风险访问控制规则即场景+执行，本技术方案的跨系统多场景跟踪用户信息的方法包括如下步骤：

[0042] S1、用户信息访问场景日志收集：具体涉及用户信息访问的系统，功能场景进行详细的日志记录，在数据传递过程中调用chain用于记录访问的源信息；用户信息访问场景日志收集具体包括用户信息访问场景、系统重点关注的用户信息访问场景、用户信息访问场景日志埋点收集、重点数据chain模型及用户信息访问事件形成四个步骤；

[0043] 用户信息访问场景日志收集是根据公司现有业务系统列出所有访问用户信息场

景,其中重点访问场景是对访问者进行重点标记,标记能够定位到具体访问者以及是否访问用户敏感信息;

[0044] 系统重点关注的用户信息访问场景包括对应的用户注册、装修活动报名、客户资料新增、查询客户基本信息、客户信息批量查看、进线客户资料查询所涉及到用户敏感信息访问的业务场景需要重点进行标记跟踪;

[0045] 用户信息访问场景日志埋点收集是在用户访问场景的关键接口请求日志中,加入chain参数用于记录访问者源数据信息,关键的场景明确到包括访问者的角色、来源ip、访问者id在内的详细信息;

[0046] 重点数据chain模型及用户信息访问事件形成包括访问者数据模型以及完整信息模型;访问者数据模型具体是:调用人→功能→行为→ip链路,在数据的流转衍生过程中,用于记录访问者的信息流转记录,即使数据不断的流转衍生,依然能够在系统中确认访问者的源信息;

[0047] 完整信息模型具体是:调用人角色-场景-调用人店铺-调用人-调用人名称-调用来源系统-调用者IP→被查阅服务→服务地址→服务说明→被查阅的信息→查阅的信息类型→查阅信息归属用户→时间,在数据流转日志清洗机解析完毕后,结合上下文数据补全完整的访问信息模型,得到完整的用户信息访问事件;

[0048] S2、用户信息访问链路数据收集处理:根据用户信息访问场景的上下文信息建立对应的用户信息访问事件,主要围绕时间、访问者、访问目标、访问行为四点进行延伸;用户信息访问链路数据收集处理包括用户信息访问chain数据处理、用户信息访问事件要素补全两个步骤;

[0049] 用户信息访问chain数据处理是指chain数据主要记录了访问者的源信息,需要根据系统、场景并集合上下文进行解析,补全用户信息访问事件数据,具体包括如下步骤:

[0050] P1、确认用户信息访问场景,在各个系统的日志进行埋点,对涉及用户信息访问的日志进行标记,接入ELK日志系统中,集中采集各个系统日志;

[0051] P2、对原始的日志进行解析、清洗、过滤、合并,根据日志中的标记,提取出涉及用户信息访问的关键日志;

[0052] P3、涉及用户信息访问的日志进行解析、拆分、标记处理;

[0053] P4、从拆分、解析后的日志中抽取用户信息访问行为的关键信息,关键信息包括访问时间、访问者、访问目标、关键行为;

[0054] P5、根据场景对解析后的日志进行初步的标注,结合日志上下文补全访问者以及被访问者信息;

[0055] 用户信息访问事件要素补全具体包括如下步骤:

[0056] Q1、获取用户信息访问的原始调用链chain数据,根据其中的访问者信息,匹配缓存数据,补全被访问者的详细信息;详细信息包括访问归属系统、来源ip、访问者id,最终能够在系统中清晰的描述访问者;

[0057] Q2、根据日志上下文,确定访问目标的主体,匹配缓存数据,补全包括被访问者id、被访问的内容在内的被访问者的详细信息;该详细信息包括被访问者id、被访问的内容,最终能够在系统中清晰的描述访问者访问了具体用户的哪些信息;

[0058] Q3、根据访问场景、日志标注、确定访问者行为,访问目标内容,确定访问行为是否

合理；

[0059] Q4、组装用户信息访问行为源数据，组装后的数据进入数据仓库中进行处理，并生成详细的用户访问事件，处理包括大数据批量处理以及风控规则；

[0060] S3、风险访问控制：用户信息访问事件生成后，提供不同维度统计，根据对应的风控规则进行风险访问控制和风险预警，具体包括根据访问者的角色设置匹配不同的风控策略、按照固定周期统计用户信息访问事件频率并执行风控策略后生成用户信息访问统计结果、用户信息风险访问管理；根据访问者的角色设置匹配不同的风控策略包括如角色及对应的风控策略：

[0061]

角色	风控策略
用户	访问频率过高
系统	不明的访问来源系统
运营	访问频率过高
商户	跨城市访问获取用户信息
商户	访问频率过高
商户	用户访问频率过高
运营	访问时间异常
系统	系统证书不匹配
....	.....

[0062] 表1.根据访问者的角色设置匹配不同的风控策略表；

[0063] 按照固定周期是指以小时、日、月为周期，进行统计用户信息访问的事件频率，执行风控策略，并生成用户信息访问统计结果；本具体实施例中

[0064] 用户信息风险访问管理具体包括如下步骤：

[0065] F1、风险访问者列表支持手动添加，可手动添加风险用户信息，风险访问者信息，实时监控用户信息访问情况；

[0066] F2、当经过风控规则过滤，标记为风险访问事件中的访问者，被访问者，添加记录在风险访问表中，相应的用户信息访问时间发生时，进行风险预警；

[0067] S4、用户信息溯源：用户信息事件发生后，在系统中根据用户ID快速查询用户信息的访问历史记录，进行快速准确的溯源。

[0068] 本发明的主要目的在于克服现有技术的不足，解决不能及时发现用户信息事件以及用户信息访问溯源困难的问题，对比以往的技术，构建了一个用户信息访问跟踪系统，汇集了用户信息访问场景，访问者根据角色维度按商户、用户、运营、系统服务进行分类标记，并且对访问源头进行了访问链路标记，根据用户信息访问场景和上下游日志批注出此次访问涉及到的访问者和被访问用户的具体信息，能够定位到每个用户信息访问行为的具体人，同时根据风控规则标注此次访问是否合理，实现一个用户信息访问行为进行准确跟踪和信息预警的功能；收集用户信息相关日志数据，用于收集分析用户信息访问行为源数据，同时根据分析结果进行用户信息访问行为进行多维度审计，同时可根据用户访问记录不断的优化调整风控规则，对异常访问进行拦截处理，对可能存在用户信息事件的行为进行预警，当用户信息事件发生时，可通过用户信息访问记录查询，快速的实现溯源。

[0069] 以上公开的本发明优选实施例只是用于帮助阐述本发明。优选实施例并没有详尽

叙述所有的细节，也不限制该发明仅为所述的具体实施方式。显然，根据本说明书的内容，可作很多的修改和变化。本说明书选取并具体描述这些实施例，是为了更好地解释本发明的原理和实际应用，从而使所属技术领域技术人员能很好地理解和利用本发明。本发明仅受权利要求书及其全部范围和等效物的限制。

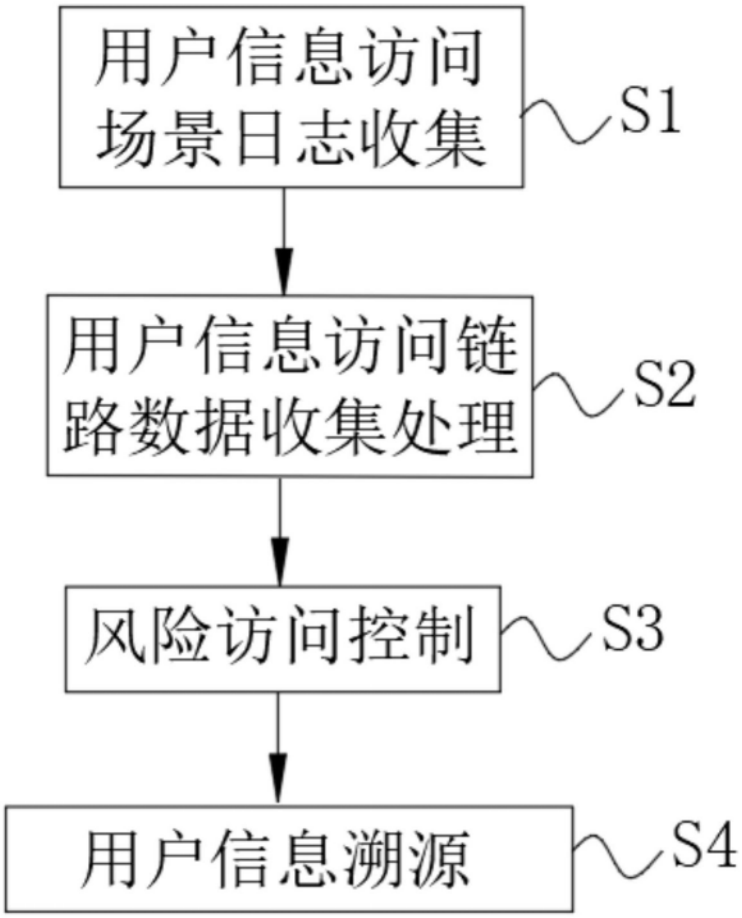


图1

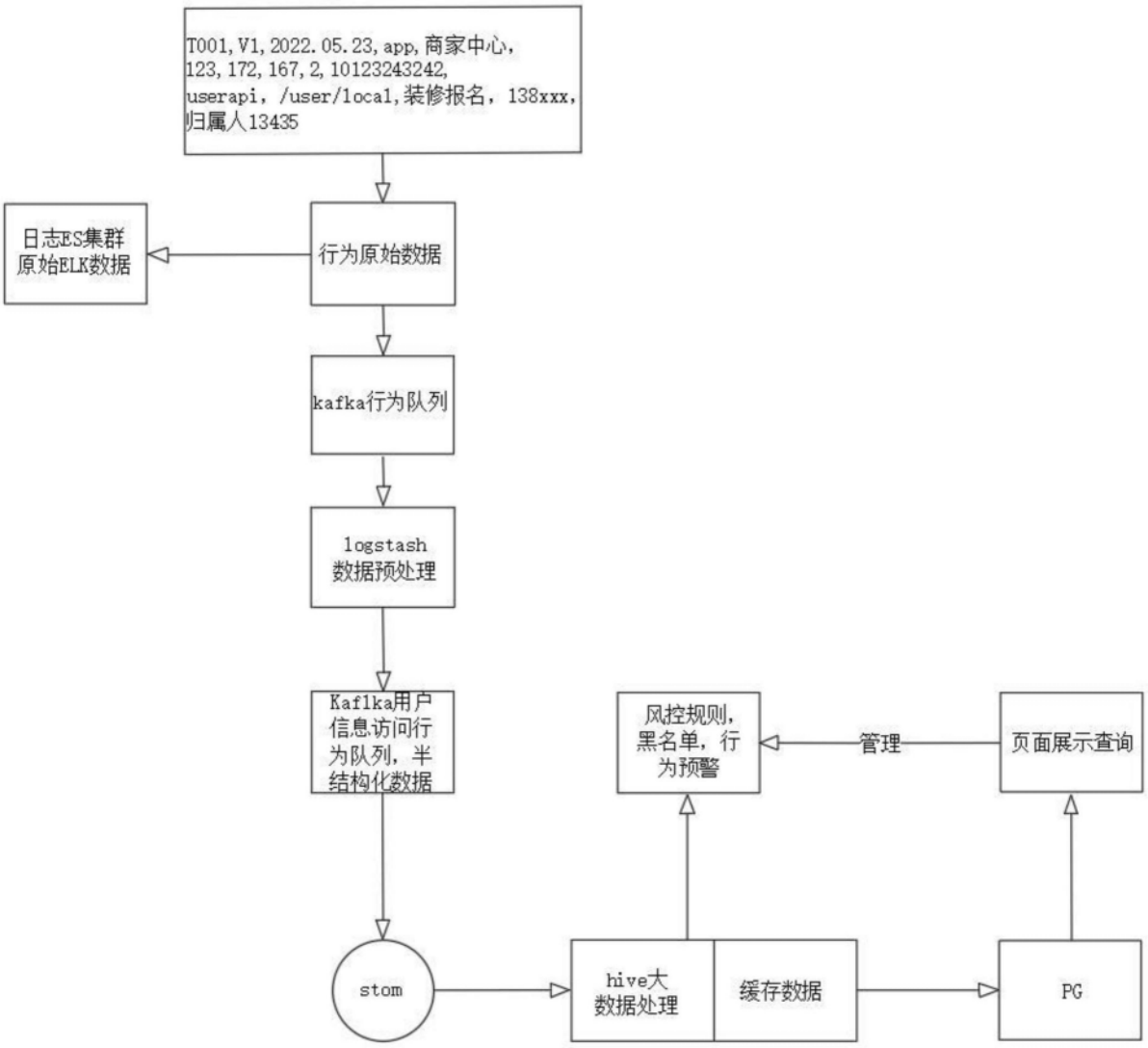
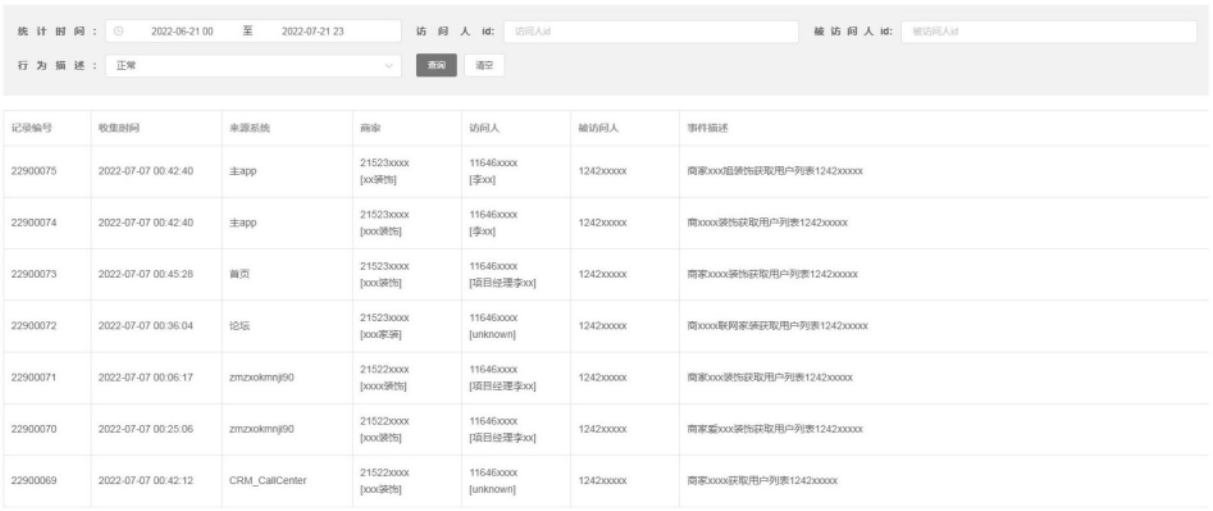

T001,V1,2022.05.23,app,商家中心,
123,172,167,2,10123243242,
userapi，/user/local,装修报名，138xxx,
归属人13435
日志ES集群
原始ELK数据
行为原始数据
kafka行为队列
logstash
数据预处理
Kaflka用户
信息访问行
为队列，半
结构化数据
风控规则,
黑名单，行
为预警
管理
页面展示查询
stom
hive大
数据处理
缓存数据
PG

图2



记录编号	收集时间	来源系统	商家	访问人	被访问人	事件描述
22900075	2022-07-07 00:42:40	主app	21523xxxx [xx装饰]	11646xxxx [李xx]	1242xxxxx	商家xxx担装饰获取用户列表1242xxxxx
22900074	2022-07-07 00:42:40	主app	21523xxxx [xxx装饰]	11646xxxx [李xx]	1242xxxxx	商xxxx装饰获取用户列表1242xxxxx
22900073	2022-07-07 00:45:28	首页	21523xxxx [xxx装饰]	11646xxxx [项目经理李xx]	1242xxxxx	商家xxxx装饰获取用户列表1242xxxxx
22900072	2022-07-07 00:36:04	论坛	21523xxxx [xxx家装]	11646xxxx [unknown]	1242xxxxx	商xxxx联网家装获取用户列表1242xxxxx
22900071	2022-07-07 00:06:17	zmzxokmnjl90	21522xxxx [xxxx装饰]	11646xxxx [项目经理李xx]	1242xxxxx	商家xxx装饰获取用户列表1242xxxxx
22900070	2022-07-07 00:25:06	zmzxokmnjl90	21522xxxx [xxx装饰]	11646xxxx [项目经理李xx]	1242xxxxx	商家爱xxx装饰获取用户列表1242xxxxx
22900069	2022-07-07 00:42:12	CRM_CallCenter	21522xxxx [xxx装饰]	11646xxxx [unknown]	1242xxxxx	商家xxxx获取用户列表1242xxxxx

图3

记录编号	收集时间	访问人类型	访问人来源系统	访问人id	访问人名称	目标用户id	行为场景	行为次数	异常类型
45	20220624	用户	商家中心	11126xxxx	测试01	132027xxxx	数据解密	321	行为正常
44	20220625	用户	商家中心	11126xxxx	测试01	132027xxxx	数据解密	12	行为正常
43	20220626	用户	商家中心	11126xxxx	测试01	132027xxxx	CRM获取用户手机号	1	行为正常
42	20220627	用户	商家中心	11126xxxx	测试01	132027xxxx	CRM获取用户手机号	233	行为正常
40	20220629	用户	商家中心	11126xxxx	测试01	132027xxxx	获取用户手机号	500	行为正常
33	20220629	用户	商家中心	11126xxxx	测试01	132027xxxx	数据解密	123	行为正常
28	20220627	用户	商家中心	11126xxxx	测试01	132027xxxx	CRM获取用户手机号	10	行为正常
23	20220625	用户	商家中心	11126xxxx	测试01	132027xxxx	获取用户手机号	150	行为正常

图4

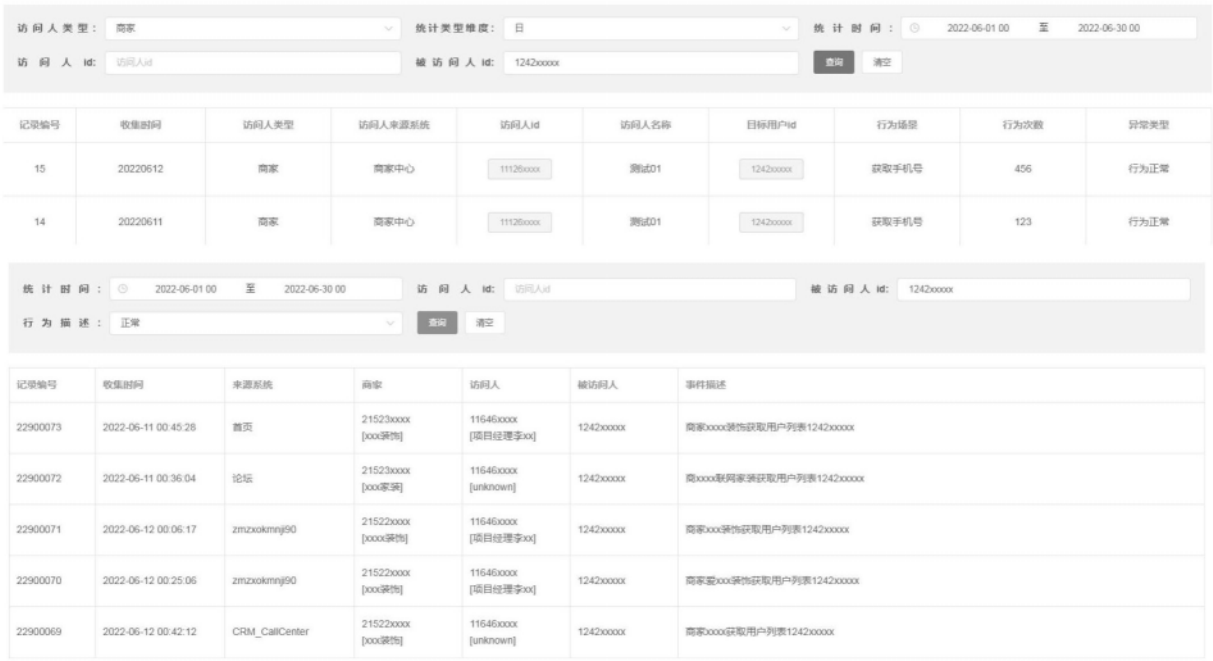

访问人类型：
商家
统计类型维度：
日
统计时间：
2022-06-01 00
至
2022-06-30 00
访问人id:
被访问人id:
1242xxxxx
查询
清空
记录编号
收集时间
访问人类型
访问人来源系统
访问人id
访问人名称
目标用户id
行为场景
行为次数
异常类型
15
20220612
商家
商家中心
测试01
获取手机号
456
行为正常
14
20220611
商家
商家中心
测试01
获取手机号
123
行为正常
统计时间：
2022-06-01 00
至
2022-06-30 00
访问人id:
被访问人id:
1242xxxxx
行为描述：
正常
查询
清空
记录编号
收集时间
来源系统
商家
访问人
被访问人
事件描述
22900073
2022-06-11 00:45:28
首页
21523xxxx
[xxx装饰]
11646xxxx
[项目经理李xx]
1242xxxxx
商家xxxx装饰获取用户列表1242xxxxx
22900072
2022-06-11 00:36:04
论坛
21523xxxx
[xxx家装]
11646xxxx
[unknown]
1242xxxxx
商xxxx联网家装获取用户列表1242xxxxx
22900071
2022-06-12 00:06:17
zmzxokmnji90
21522xxxx
[xxxx装饰]
11646xxxx
[项目经理李xx]
1242xxxxx
商家xxx装饰获取用户列表1242xxxxx
22900070
2022-06-12 00:25:06
zmzxokmnji90
21522xxxx
[xxx装饰]
11646xxxx
[项目经理李xx]
1242xxxxx
商家爱xxx装饰获取用户列表1242xxxxx
22900069
2022-06-12 00:42:12
CRM_CallCenter
21522xxxx
[xxx装饰]
11646xxxx
[unknown]
1242xxxxx
商家xxxx获取用户列表1242xxxxx

图5