(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 12 月 24 日 (24.12.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/252897 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/102497

(22) 国际申请日: 2019 年 8 月 26 日 (26.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910524196.7 2019年6月18日 (18.06.2019) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518033 (CN)。

(72) 发明人: 洪耿杰 (HONG, Gengjie); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518033 (CN)。

(74) 代理人: 北京市京大律师事务所 (BEIJING JINGDA LAW FIRM); 中国北京市海淀区海淀中街16号7层2单元703, Beijing 100080 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(54) **Title:** DISTRIBUTED LINK DATA AUTHENTICATION METHOD, DEVICE AND APPARATUS, AND STORAGE MEDIUM

(54) **发明名称**: 全链路数据鉴权方法、装置、设备及存储介质

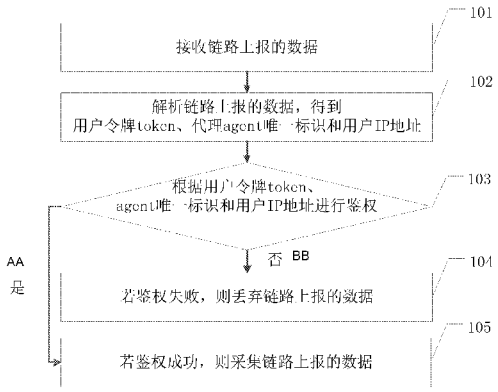


图1

101 Receive data reported on a link
102 Analyze the data reported on the link to obtain a user token, an agent unique identifier and a user IP address
103 Perform authentication according to the user token, the agent unique identifier and the user IP address
104 If the authentication fails, discard the data reported on the link
105 If the authentication is successful, collect the data reported on the link
AA Yes
BB No

(57) **Abstract:** The present application relates to the field of information security. Disclosed are a distributed link data authentication method, device and apparatus, and a storage medium. The distributed link data authentication method comprises: receiving data reported on a link; analyzing the data reported on the link to obtain a user token, an agent unique identifier and a user IP address; performing authentication according to the user token, the agent unique identifier and the user IP address; if the authentication fails, discarding the data reported on the link, and if the authentication is successful, collecting the data reported on the link. The present application performs identity authentication on all data reported on the link on the basis of a JWT protocol to prevent the problem of junk data caused by user information leakage, prevent a distributed link monitoring server from being attacked and ensure the usefulness of data reported on the link.

(57) **摘要**: 本申请涉及信息安全领域，公开了全链路数据鉴权方法、装置、设备及存储介质。全链路数据鉴权方法包括：接收链路上报的数据；解析链路上报的数据，得到用户令牌token、代理agent唯一标识和用户IP地址；根据用户token、agent唯一标识和用户IP地址进行鉴权；若鉴权失败，则丢弃链路上报的数据；若鉴权成功，则采集链路上报的数据。本申请基于JWT协议的方式对全链路上报数据进行身份验证，防止用户信息泄露导致的垃圾数据问题，防止全链路监控服务器受到攻击，确保链路上报数据的有用性。

WO 2020/252897 A1

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

全链路数据鉴权方法、装置、设备及存储介质

本申请要求于2019年6月18日提交中国专利局、申请号为201910524196.7、发明名称为“全链路数据鉴权方法、装置、设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在申请中。

技术领域

本申请涉及信息安全领域，尤其涉及全链路数据鉴权方法、装置、设备及存储介质。

背景技术

在互联网技术高速发展的今天，需要通过集群部署来支撑日益增长的庞大业务量，同时又能根据业务需要进行灵活扩展，形成了分布式系统。

全链路监控组件可以监控分布式系统在不同应用、不同服务器的之间的关联动作。一次用户上报数据通常要调用多个服务节点，在系统运维中，需要对服务链路的用户上报数据进行监控，以便及时发现并处理服务链路中出现的问题。

目前全链路上报数据只是根据用户名和密码进行简单鉴权，或者不进行鉴权，发明人意识到这样会带来各种问题，比如一些重要的用户信息，尤其敏感数据，以明文方式传输，会导致用户的数据容易遭受攻击，也会造成大量的垃圾数据上报。

发明内容

本申请的主要目的在于解决全链路上报数据不鉴权或者简单鉴权导致的用户数据遭受攻击，大量的垃圾数据上报的技术问题。

为实现上述目的，本申请第一方面提供了一种全链路数据鉴权方法，包括：接收链路上报的数据；解析所述链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权；若鉴权失败，则丢弃所述链路上报的数据；若鉴权成功，则采集所述链路上报的数据。

本申请第二方面提供了一种全链路数据鉴权装置，包括：接收单元，用于接收链路上报的数据；解析单元，用于解析所述链路上报的数据，得到所述用户令牌 token、代理 agent 唯一标识和用户 IP 地址；鉴权单元，用于根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权；第一处理单元，若鉴权失败，则用于丢弃所述链路上报的数据；第二处理单元，若鉴权成功，则用于采集所述链路上报的数据。

本申请第三方面提供了一种全链路数据鉴权设备，包括：存储器和至少一个处理器，所述存储器中存储有指令，所述存储器和所述至少一个处理器通过线路互联；所述至少一个处理器调用所述存储器中的所述指令，以使得所述全链路数据鉴权设备执行上述第一方面所述的方法。

本申请的第四方面提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机指令，当所述计算机指令在计算机上运行时，使得计算机执行上述第一方面所述的方法。

本申请提供的技术方案中，接收链路上报的数据；解析所述链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权；若鉴权失败，则丢弃所述链路上报的数据；若鉴权成功，则采集所述链路上报的数据。本申请实施例中，根据用户令牌 token 与代理 agent 唯一标识和用户 IP 地址进行鉴权，得到鉴权结果，根据鉴权结果确定是否采集链路上报的数据，实现过滤链路上报的垃圾数据。

附图说明

图 1 为本申请实施例中全链路数据鉴权方法的一个实施例示意图；

图 2 为本申请实施例中全链路数据鉴权方法的另一个实施例示意图；

图 3 为本申请实施例中全链路数据鉴权装置的一个实施例示意图；

图 4 为本申请实施例中全链路数据鉴权装置的另一个实施例示意图；

图 5 为本申请实施例中全链路数据鉴权设备的一个实施例示意图。

具体实施方式

本申请实施例提供了全链路数据鉴权方法、装置、设备及存储介质，用于根据用户令牌 token 与代理 agent 唯一标识和用户 IP 地址进行鉴权，得到鉴权结果，根据鉴权结果确定是否采集链路上报的数据，实现过滤链路上报的垃圾数据。基于 JWT 协议的方式对全链路上报数据进行身份验证，防止用户信息泄露导致的垃圾数据问题，防止全链路监控服务器受到攻击，确保链路上报数据的有用性。

为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例进行描述。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”或“具有”及其任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

为便于理解，下面对本申请实施例的具体流程进行描述，请参阅图 1，本申请实施例中全链路数据鉴权方法的一个实施例包括：

101、接收链路上报的数据；

服务器接收链路上报的数据。具体的，服务器通过全链路的代理 agent 发送链路上报的数据，通过全链路中的数据收集模块 collector 接收 agent 发送过来的链路上报的数据，链路上报的数据包括用户令牌 token、代理 agent 唯一标识和用户 IP 地址。

需要说明的是，全链路监控系统包括代理 agent，数据收集模块 collector 以及显示终端，每个 agent 都有其唯一的用户 token、agent 唯一标识和用户 IP 地址。agent 部署在全链路分布式系统中，用于监控网络连接情况，并上报数据，collector 用于接收数据并对接收的数据进行鉴权，显示终端用来展示 collector 采集的数据。

102、解析链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；

服务器解析链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址。具体的，服务器按照预置方式解析该链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址，服务器判断用户令牌 token、代理 agent 唯一标识和用户 IP 地址是否为空，若用户令牌 token、代理 agent 唯一标识和用户 IP 地址有一个参数为空，则确定此次链路上报的数据为无效数据，丢弃此次链路上报的数据。

需要说明的是，该用户令牌 token 为根据 JWT 协议生成的，该 JWT 协议是一种基于 JS 对象简谱（javascript object notation，JSON）的开放标准协议，适用场景比如现在流行的分布式环境当中，非常适用跨平台应用程序，根据 JWT 协议生成的链路的用户 token，包括用户 token 的头部 header、用户 token 的载荷 payload 和用户 token 的签名 signature，

三个部分使用分隔符“.”按照先后顺序依次进行连接。该 agent 唯一标识是全局唯一的，服务器使用数据库中具有自动增长标识符类型的字段或者使用通用唯一识别码（universally unique identifier，UUID）的生成库进行设置代理 agent 唯一标识，具体此处不做限定。

103、根据用户 token、agent 唯一标识和用户 IP 地址进行鉴权；

服务器根据用户 token、agent 唯一标识和用户 IP 地址进行鉴权。鉴权是指验证链路上报的数据是否拥有访问系统的权利。具体的，服务器根据 JWT 协议对用户 token 进行分割，进一步地，服务器根据 JWT 协议通过分隔符“.”将该用户 token 进行分割，得到用户 token 的头部、用户 token 的载荷和用户 token 的签名，三个部分都为字符串形式，包括数字和字母等符号；服务器对用户 token 的头部进行 base64 解密，得到头部声明的加密算法；服务器根据头部声明的加密算法对用户 token 的头部和用户 token 的载荷进行组合加密，得到待验证签名；服务器判断待验证签名与用户 token 的签名是否相同；若待验证签名与用户 token 的签名相同，则服务器对用户 token 的载荷进行 base64 解密，得到用户 token 的鉴权信息。

服务器判断用户 token 的鉴权信息是否存在异常；若用户 token 的鉴权信息存在异常，则确定鉴权失败，执行步骤 104，例如，若用户 token 的鉴权信息为空，则确定鉴权失败；若用户 token 的鉴权信息不存在异常，则服务器判断用户 token 的鉴权信息是否包括 agent 唯一标识；若用户 token 的鉴权信息不包括 agent 唯一标识，则服务器确定鉴权失败，执行步骤 104，例如，agent 唯一标识为 1000，用户 token 的鉴权信息中的 agent 唯一标识为 1001，则两者不匹配，确定鉴权失败；若用户 token 的鉴权信息包括 agent 唯一标识，则服务器判断用户 token 的鉴权信息是否包括用户 IP 地址；若用户 token 的鉴权信息不包括用户 IP 地址，则确定鉴权失败，执行步骤 104，例如，用户 IP 地址为 A，用户 token 的鉴权信息中的用户 IP 地址为 B，则两者不匹配，确定鉴权失败，A 与 B 均为符合 IP 地址的格式；若用户 token 的鉴权信息包括用户 IP 地址，则确定鉴权成功，执行步骤 105。

104、若鉴权失败，则丢弃链路上报的数据；

若鉴权失败，则服务器丢弃链路上报的数据。鉴权失败说明通过 agent 发送的数据没有通过链路的身份验证，是无效的垃圾数据，拒绝采集，等待下一个链路上报数据周期，重新进行链路数据的鉴权。

具体的，服务器根据鉴权失败预设鉴权失败的原因值，一旦鉴权失败，服务器发送鉴权失败的原因值；获取鉴权时刻；记录鉴权失败的原因值、agent 唯一标识、用户 IP 地址和鉴权时刻；服务器删除链路上报的数据。例如，若用户令牌 token 的鉴权信息不包括 agent 唯一标识，确定鉴权失败，设置其鉴权失败的原因值为 501；若用户令牌 token 的鉴权信息不包括用户 IP 地址，确定鉴权失败，设置其鉴权失败的原因值为 502，具体此处不做限定。

需要说明的是，记录鉴权失败的原因值、agent 唯一标识、用户 IP 地址和鉴权时刻，以便于查询问题，该记录方式可以通过日志或者数据库表的方式，具体此处不做限定。

105、若鉴权成功，则采集链路上报的数据。

若鉴权成功，则服务器采集上报的数据，具体的，服务器发送鉴权成功的原因值，通知链路上报数据端数据采集成功，例如，设置鉴权成功的原因值为 200，agent 接收到该值，确认上报数据被采集；同时服务器将链路上报的数据记录在 HBase 数据库中。HBase 是一个高可靠性、高性能、面向列和可伸缩的分布式存储系统，利用 HBase 技术可搭建大规模结构化存储集群，HBase 的目标是存储并处理大型的数据，更具体来说是仅需使用普通的硬件配置，就能够处理由成千上万的行和列所组成的大型数据，适用于全链路监控系统。

需要说明的是，全链路通过代理 agent 无侵入式部署，将性能测量与业务逻辑完全分离，用于收集应用端监控数据，在启动命令中设置部分参数，例如，代理 agent 唯一标识以及数据收集模块 collector 的地址，这种方式大大提高了采集效率，并且减少运维成本。

本申请实施例中，根据用户令牌 token 与代理 agent 唯一标识和用户 IP 地址进行鉴权，得到鉴权结果，根据鉴权结果确定是否采集链路上报的数据，实现过滤链路上报的垃圾数据。基于 JWT 协议的方式对全链路上报数据进行身份验证，防止用户信息泄露导致的垃圾数据问题，防止全链路监控服务器受到攻击，确保链路上报数据的有用性。

请参阅图 2，本申请实施例中全链路数据鉴权方法的另一个实施例包括：

201、接收链路上报的数据；

服务器接收链路上报的数据。具体的，服务器通过全链路的代理 agent 发送链路上报的数据，通过全链路中的数据收集模块 collector 接收 agent 发送过来的链路上报的数据，链路上报的数据包括用户令牌 token、代理 agent 唯一标识和用户 IP 地址。

需要说明的是，全链路监控系统包括代理 agent，数据收集模块 collector 以及显示终端，每个 agent 都有其唯一的用户 token、agent 唯一标识和用户 IP 地址。agent 部署在全链路分布式系统中，用于监控网络连接情况，并上报数据，collector 用于接收数据并对接收的数据进行鉴权，显示终端用来展示 collector 采集的数据。

202、解析链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；

服务器解析链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址。具体的，服务器通过预置方式解析该链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址，服务器判断用户令牌 token、代理 agent 唯一标识和用户 IP 地址是否为空，若用户令牌 token、代理 agent 唯一标识和用户 IP 地址有一个参数为空，则确定此次链路上报的数据为无效数据，丢弃此次链路上报的数据。

需要说明的是，该用户令牌 token 为根据 JWT 协议生成的，该 JWT 协议是一种基于 JS 对象简谱（javascript object notation，JSON）的开放标准协议，适用场景比如现在流行的分布式环境当中，非常适用跨平台应用程序，根据 JWT 协议生成的链路的用户 token，包括用户 token 的头部 header、用户 token 的载荷 payload 和用户 token 的签名 signature，三个部分使用分隔符“.”按照先后顺序依次进行连接。该 agent 唯一标识是全局唯一的，服务器使用数据库中具有自动增长标识符类型的字段或者使用通用唯一识别码（universally unique identifier，UUID）的生成库进行设置代理 agent 唯一标识，UUID 包括当前时刻、时钟序列和全局唯一的 IEEE 机器识别号，UUID 是指在一台机器上生成的数字，它保证对在同一时空中的所有机器都是唯一的。

203、根据 JWT 协议对用户 token 进行解析，得到用户 token 的鉴权信息；

服务器根据 JWT 协议对用户 token 进行解析，得到用户 token 的鉴权信息。该用户 token 的鉴权信息包括用户 token 的过期时刻和鉴权参数。

具体的，首先，服务器根据 JWT 协议对用户 token 进行分割，进一步地，服务器根据 JWT 协议通过分隔符“.”对用户 token 进行字符串的分割，得到用户 token 的头部、用户 token 的载荷和用户 token 的签名，三个部分都为字符串形式，包括数字和字母等字符。

其次，服务器对用户 token 的头部进行 base64 解密，得到头部声明的加密算法，例如，服务器根据 base64 解密，base64UrlDecode(用户 token 的头部)，得到的解密结果如下所示，

```
{
  "alg": "HS256",
```

```
  "typ": "JWT"
}
```

其中，参数 typ 为令牌的类型，参数 alg 为常用的加密散列算法，得到头部声明的加密算法为 HS256。

然后，服务器根据头部声明的加密算法对用户 token 的头部和用户 token 的载荷进行组合加密，得到待验证签名，具体的，服务器将用户 token 的头部和用户 token 的载荷使用分隔符“.”连接组成字符串，然后根据头部声明的加密方式 HS256 将字符串与密钥组合加密，得到待验证签名，例如，密钥为 secret，服务器根据头部声明的加密算法 HS256 进行组合加密的流程为，

HMACSHA256(用户 token 的头部 + "." +用户 token 的载荷, secret)，

其中 secret 为用户 token 的密钥，该密钥与用户 token 的加密过程保持一致。

最后，服务器判断待验证签名与用户 token 的签名是否相同；若待验证签名与用户 token 的签名相同，则服务器对用户 token 的载荷进行 base64 解密，得到用户令牌 token 的鉴权信息。

需要说明的是，用户 token 的载荷存放有效信息，包含注册声明、公有声明和私有声明，服务器获取包括 agent 唯一标识和用户 IP 地址的私有声明部分，例如：

```
{
  "agentid": "1234",
  "agentip": "192.168.0.1"
}
```

，服务器还获取到注册声明中的参数，例如过期时刻参数 exp，该参数 exp 为时间戳格式。

204、根据用户 token 的鉴权信息、agent 唯一标识和用户 IP 地址进行鉴权；

服务器根据用户令牌 token 的鉴权信息、agent 唯一标识和用户 IP 地址进行鉴权，具体的，服务器判断用户令牌 token 的鉴权信息是否存在异常，例如，若用户令牌 token 的鉴权信息为空，则确定鉴权失败；若用户令牌 token 的鉴权信息存在异常，则确定鉴权失败，执行步骤 205，例如，用户令牌 token 的鉴权信息为空，则确定鉴权失败；若用户令牌 token 的鉴权信息不存在异常，则服务器判断用户令牌 token 的鉴权信息是否包括代理 agent 唯一标识；若用户令牌 token 的鉴权信息不包括代理 agent 唯一标识，则服务器确定鉴权失败，执行步骤 205，例如，agent 唯一标识为 1000，用户令牌 token 的鉴权信息中的 agent 唯一标识为 1001，则两者不匹配，确定鉴权失败；若用户令牌 token 的鉴权信息包括代理 agent 唯一标识，则服务器判断用户令牌 token 的鉴权信息是否包括用户 IP 地址；若用户令牌 token 的鉴权信息不包括用户 IP 地址，则确定鉴权失败，执行步骤 205，例如，用户 IP 地址为 A，用户令牌 token 的鉴权信息中的用户 IP 地址为 B，则两者不匹配，确定鉴权失败，A 与 B 均为符合 IP 地址的格式。若用户令牌 token 的鉴权信息包括用户 IP 地址，则确定鉴权成功，执行步骤 206。

可选的，服务器读取配置信息，判断预置值是否为目标阈值，目标阈值用于指示根据用户令牌 token 的过期时刻进行鉴权；若预置值为目标阈值，则获取用户 token 的获取用户令牌的过期时刻；判断所述用户令牌 token 的过期时刻是否小于当前时刻，若用户令牌的过期时刻小于当前时刻，则确定鉴权失败，执行步骤 205；若用户 token 的过期时刻大于或等于当前时刻，则确定鉴权成功，执行步骤 206。例如，若获取预置值的目标阈值为 1，则表示根据用户 token 的过期时刻进行鉴权，用户 token 的过期时刻是时间戳格式。该配置信息可通过文件方式或者数据表方式进行存储，具体此处不做限定。

205、若鉴权失败，则丢弃链路上报的数据；

若鉴权失败，则服务器丢弃链路上报的数据。鉴权失败说明通过 agent 发送的链路上报的数据没有通过身份验证，是无效的垃圾数据，拒绝采集，等待下一个链路上报数据周期，重新进行链路数据的鉴权。

具体的，服务器根据鉴权失败预设鉴权失败的原因值，一旦鉴权失败，服务器发送鉴权失败的原因值；获取鉴权时刻；记录鉴权失败的原因值、agent 唯一标识、用户 IP 地址和鉴权时刻；服务器删除链路上报的数据。例如，若用户 token 的鉴权信息不包括 agent 唯一标识，确定鉴权失败，其预设的鉴权失败的原因值为 501；若用户 token 的鉴权信息不包括用户 IP 地址，确定鉴权失败，起预设的鉴权失败的原因值为 502，具体此处不做限定。

需要说明的是，记录鉴权失败的原因值、agent 唯一标识、用户 IP 地址和鉴权时刻，是为了便于查询问题，该记录方式可以通过日志或者数据库表的方式，具体此处不做限定。

206、若鉴权成功，则采集链路上报的数据。

若鉴权成功，则服务器采集链路上报的数据。具体的，用户令牌 token 的鉴权信息不存在异常，同时包括代理 agent 唯一标识和用户 IP 地址服务器，则确定鉴权成功，若鉴权成功，则服务器发送鉴权成功的原因值，通知链路上报数据端，即 agent 数据采集成功，例如，设置鉴权成功的原因值为 200，agent 接收到该值，确认上报数据被采集；同时服务器将链路上报的数据记录在 HBase 数据库中。HBase 是一个高可靠性、高性能、面向列和可伸缩的分布式存储系统，利用 HBase 技术可搭建大规模结构化存储集群，HBase 的目标是存储并处理大型的数据，更具体来说是仅需使用普通的硬件配置，就能够处理由成千上万的行和列所组成的大型数据，适用于全链路监控系统。

需要说明的是，全链路通过代理 agent 无侵入式部署，将性能测量与业务逻辑完全分离，用于收集应用端监控数据，在启动命令中设置部分参数，例如，代理 agent 唯一标识以及数据收集模块 collector 的地址，这种方式大大提高了采集效率，并且减少运维成本。

本申请采用上述的方法，根据用户令牌 token 与代理 agent 唯一标识和用户 IP 地址进行鉴权，得到鉴权结果，根据鉴权结果确定是否采集链路上报的数据，实现过滤链路上报的垃圾数据。基于 JWT 协议的方式对全链路上报数据进行身份验证，防止用户信息泄露导致的垃圾数据问题，防止全链路监控服务器受到攻击，确保链路上报数据的有用性。

上面对本申请实施例中全链路数据鉴权方法进行了描述，下面对本申请实施例中全链路数据鉴权装置进行描述，请参阅图 3，本申请实施例中全链路数据鉴权一个实施例包括：

接收单元 301，用于接收链路上报的数据；

解析单元 302，用于解析链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；

鉴权单元 303，用于根据用户 token、agent 唯一标识和用户 IP 地址进行鉴权；

第一处理单元 304，若鉴权失败，则用于丢弃链路上报的数据；

第二处理单元 305，若鉴权成功，则用于采集链路上报的数据。

本申请根据用户令牌 token 与代理 agent 唯一标识和用户 IP 地址进行鉴权，得到鉴权结果，根据鉴权结果确定是否采集链路上报的数据，实现过滤链路上报的垃圾数据。基于 JWT 协议的方式对全链路上报数据进行身份验证，防止用户信息泄露导致的垃圾数据问题，防止全链路监控服务器受到攻击，确保链路上报数据的有用性。

请参阅图 4，本申请实施例中全链路数据鉴权装置的另一个实施例包括：

接收单元 301，用于接收链路上报的数据；

解析单元 302，用于解析链路上报的数据，得到用户令牌 token、代理 agent 唯一标识

和用户 IP 地址；

鉴权单元 303，用于根据用户 token、agent 唯一标识和用户 IP 地址进行鉴权；

第一处理单元 304，若鉴权失败，则用于丢弃链路上报的数据；

第二处理单元 305，若鉴权成功，则用于采集链路上报的数据。

可选的，鉴权单元 303 可进一步包括：

解析子单元 3031，用于根据 JWT 协议对用户 token 进行解析，得到用户 token 的鉴权信息；

第一判断子单元 3032，用于判断用户 token 的鉴权信息是否存在异常；

第一处理子单元 3033，若用户 token 的鉴权信息存在异常，则用于确定鉴权失败；

第一鉴权子单元 3034，若用户 token 的鉴权信息不存在异常，则用于根据用户 token 的鉴权信息、agent 唯一标识和用户 IP 地址进行鉴权。

可选的，解析子单元 3031 还可以具体用于：

根据 JWT 协议对用户 token 进行分割，得到用户 token 的头部、用户 token 的载荷和用户 token 的签名；

对用户 token 的头部进行 base64 解密，得到头部声明的加密算法；

根据头部声明的加密算法对用户 token 的头部和用户 token 的载荷进行组合加密，得到待验证签名；

判断待验证签名与用户 token 的签名是否相同；

若待验证签名与第用户 token 的签名相同，则对用户 token 的载荷进行 base64 解密，得到用户 token 的鉴权信息。

可选的，第一鉴权子单元 3034 还可以具体用于：

若用户 token 的鉴权信息不存在异常，则判断用户 token 的鉴权信息是否包括 agent 唯一标识；

若用户 token 的鉴权信息不包括 agent 唯一标识，则确定鉴权失败；

若用户 token 的鉴权信息包括代理 agent 唯一标识，则判断用户 token 的鉴权信息是否包括用户 IP 地址；

若用户 token 的鉴权信息不包括用户 IP 地址，则确定鉴权失败；

若用户 token 的鉴权信息包括用户 IP 地址，则确定鉴权成功。

可选的，第一处理单元 304 还可以具体用于：

发送鉴权失败的原因值；

获取鉴权时刻；

记录鉴权失败的原因值、agent 唯一标识、用户 IP 地址和鉴权时刻；

删除所述链路上报的数据。

可选的，第二处理单元 305 还可以具体用于：

发送鉴权成功的原因值；

将链路上报的数据写入数据库。

可选的，鉴权单元 303 还可进一步包括：

读取子单元 3035，用于读取预置值；

第二判断子单元 3036，用于判断预置值是否为目标阈值，目标阈值用于指示根据用户 token 的过期时刻进行鉴权；

第二鉴权子单元 3037，若预置值为目标阈值，则用于获取用户 token 的过期时刻；

第三判断子单元 3038，用于判断用户 token 的过期时刻是否小于当前时刻；

第二处理子单元 3039，若用户令牌 token 的过期时刻小于当前时刻，则用于确定鉴权

失败；

第三处理子单元 30310，若用户 token 的过期时刻大于或等于当前时刻，则用于确定鉴权成功。

本申请根据用户令牌 token 与代理 agent 唯一标识和用户 IP 地址进行鉴权，得到鉴权结果，根据鉴权结果确定是否采集链路上报的数据，实现过滤链路上报的垃圾数据。基于 JWT 协议的方式对全链路上报数据进行身份验证，防止用户信息泄露导致的垃圾数据问题，防止全链路监控服务器受到攻击，确保链路上报数据的有用性。

上面图 3 和图 4 从模块化功能实体的角度对本申请实施例中的全链路数据鉴权装置进行详细描述，下面从硬件处理的角度对本申请实施例中全链路数据鉴权设备进行详细描述。

图 5 是本申请实施例提供的一种全链路数据鉴权设备的结构示意图，该全链路数据鉴权设备 500 可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上处理器（central processing units，CPU）501（例如，一个或一个以上处理器）和存储器 509，一个或一个以上存储应用程序 507 或数据 506 的存储介质 508（例如一个或一个以上海量存储设备）。其中，存储器 509 和存储介质 508 可以是短暂存储或持久存储。存储在存储介质 508 的程序可以包括一个或一个以上模块（图示没标出），每个模块可以包括对全链路数据鉴权中的一系列指令操作。更进一步地，处理器 501 可以设置为与存储介质 508 通信，在全链路数据鉴权设备 500 上执行存储介质 508 中的一系列指令操作。

全链路数据鉴权设备 500 还可以包括一个或一个以上电源 502，一个或一个以上有线或无线网络接口 503，一个或一个以上输入输出接口 504，和/或，一个或一个以上操作系统 505，例如 Windows Serve，Mac OS X，Unix，Linux，FreeBSD 等等。本领域技术人员可以理解，图 5 中示出的全链路数据鉴权设备结构并不构成对全链路数据鉴权设备的限定，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。

本申请还提供一种计算机可读存储介质，该计算机可读存储介质可以为非易失性计算机可读存储介质。计算机可读存储介质存储有计算机指令，当所述计算机指令在计算机上运行时，使得计算机执行如下步骤：

接收链路上报的数据；

解析所述链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；

根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权；

若鉴权失败，则丢弃所述链路上报的数据；

若鉴权成功，则采集所述链路上报的数据。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可

以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或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一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory， ROM）、随机存取存储器（random access memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

权 利 要 求

1、一种全链路数据鉴权方法，包括：

接收链路上报的数据；

解析所述链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；

根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权；

若鉴权失败，则丢弃所述链路上报的数据；

若鉴权成功，则采集所述链路上报的数据。

2、根据权利要求 1 所述的全链路数据鉴权方法，所述根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权包括：

根据 JWT 协议对所述用户 token 进行解析，得到所述用户 token 的鉴权信息；

判断所述用户 token 的鉴权信息是否存在异常；

若所述用户 token 的鉴权信息存在异常，则确定鉴权失败；

若所述用户 token 的鉴权信息不存在异常，则根据所述用户 token 的鉴权信息、所述 agent 唯一标识和所述用户 IP 地址进行鉴权。

3、根据权利要求 2 所述的全链路数据鉴权方法，所述根据 JWT 协议对所述用户 token 进行解析，得到所述用户 token 的鉴权信息包括：

根据所述 JWT 协议对所述用户 token 进行分割，得到所述用户 token 的头部、所述用户 token 的载荷和所述用户 token 的签名；

对所述用户 token 的头部进行 base64 解密，得到所述头部声明的加密算法；

根据所述头部声明的加密算法对所述用户 token 的头部和所述用户 token 的载荷进行组合加密，得到待验证签名；

判断所述待验证签名与所述用户 token 的签名是否相同；

若所述待验证签名与所述用户 token 的签名相同，则对所述用户 token 的载荷进行 base64 解密，得到所述用户 token 的鉴权信息。

4、根据权利要求 2 所述的全链路数据鉴权方法，所述若所述用户 token 的鉴权信息不存在异常，则根据所述用户 token 的鉴权信息、所述 agent 唯一标识和所述用户 IP 地址进

行鉴权包括：

若所述用户 token 的鉴权信息不存在异常，则判断所述用户 token 的鉴权信息是否包括所述 agent 唯一标识；

若所述用户 token 的鉴权信息不包括所述 agent 唯一标识，则确定鉴权失败；

若所述用户 token 的鉴权信息包括所述 agent 唯一标识，则判断所述用户 token 的鉴权信息是否包括所述用户 IP 地址；

若所述用户 token 的鉴权信息不包括所述用户 IP 地址，则确定鉴权失败；

若所述用户 token 的鉴权信息包括所述用户 IP 地址，则确定鉴权成功。

5、根据权利要求 1 所述的全链路数据鉴权方法，所述若鉴权失败，则丢弃所述链路上报的数据包括：

发送鉴权失败的原因值；

获取鉴权时刻；

记录所述鉴权失败的原因值、所述 agent 唯一标识、所述用户 IP 地址和所述鉴权时刻；

删除所述链路上报的数据。

6、根据权利要求 1 所述的全链路数据鉴权方法，所述若鉴权成功，则采集所述链路上报的数据包括：

发送鉴权成功的原因值；

将所述链路上报的数据写入数据库。

7、根据权利要求 1 至 6 中任一项所述的全链路数据鉴权方法，所述若所述用户 token 的鉴权信息不存在异常，则根据所述用户 token 的鉴权信息、所述 agent 唯一标识和所述用户 IP 地址进行鉴权之后，所述全链路数据鉴权方法还包括：

读取预置值；

判断预置值是否为目标阈值，所述目标阈值用于指示根据所述用户 token 的过期时刻进行鉴权；

若所述预置值为所述目标阈值，则获取所述用户 token 的过期时刻；

判断所述用户 token 的过期时刻是否小于当前时刻；

若所述用户 token 的过期时刻小于所述当前时刻，则确定鉴权失败；

若所述用户 token 的过期时刻大于或等于所述当前时刻，则确定鉴权成功。

8、一种全链路数据鉴权装置，所述全链路数据鉴权装置包括：

接收单元，用于接收链路上报的数据；

解析单元，用于解析所述链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；

鉴权单元，用于根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权；

第一处理单元，若鉴权失败，则用于丢弃所述链路上报的数据；

第二处理单元，若鉴权成功，则用于采集所述链路上报的数据。

9、根据权利要求 8 所述的全链路数据鉴权装置，所述鉴权单元包括：

解析子单元，用于根据 JWT 协议对所述用户 token 进行解析，得到所述用户 token 的鉴权信息；

第一判断子单元，用于判断所述用户 token 的鉴权信息是否存在异常；

第一处理子单元，若所述用户 token 的鉴权信息存在异常，则用于确定鉴权失败；

第一鉴权子单元，若所述用户 token 的鉴权信息不存在异常，则用于根据所述用户 token 的鉴权信息、所述 agent 唯一标识和所述用户 IP 地址进行鉴权。

10、根据权利要求 9 所述的全链路数据鉴权装置，所述解析子单元具体用于：

根据所述 JWT 协议对所述用户 token 进行分割，得到所述用户 token 的头部、所述用户 token 的载荷和所述用户 token 的签名；

对所述用户 token 的头部进行 base64 解密，得到所述头部声明的加密算法；

根据所述头部声明的加密算法对所述用户 token 的头部和所述用户 token 的载荷进行组合加密，得到待验证签名；

判断所述待验证签名与所述用户 token 的签名是否相同；

若所述待验证签名与所述用户 token 的签名相同，则对所述用户 token 的载荷进行 base64 解密，得到所述用户 token 的鉴权信息。

11、根据权利要求 9 所述的全链路数据鉴权装置，所述第一鉴权子单元具体用于：

若所述用户 token 的鉴权信息不存在异常，则判断所述用户 token 的鉴权信息是否包括所述 agent 唯一标识；

若所述用户 token 的鉴权信息不包括所述 agent 唯一标识，则确定鉴权失败；

若所述用户 token 的鉴权信息包括所述 agent 唯一标识，则判断所述用户 token 的鉴权信息是否包括所述用户 IP 地址；

若所述用户 token 的鉴权信息不包括所述用户 IP 地址，则确定鉴权失败；

若所述用户 token 的鉴权信息包括所述用户 IP 地址，则确定鉴权成功。

12、根据权利要求 8 所述的全链路数据鉴权装置，所述第一处理单元具体用于：

发送鉴权失败的原因值；

获取鉴权时刻；

记录所述鉴权失败的原因值、所述 agent 唯一标识、所述用户 IP 地址和所述鉴权时刻；

删除所述链路上报的数据。

13、根据权利要求 8 所述的全链路数据鉴权装置，所述第二处理单元具体用于：

发送鉴权成功的原因值；

将所述链路上报的数据写入数据库。

14、根据权利要求 8 至 13 中任一项所述的全链路数据鉴权装置，所述鉴权单元还包括：

读取子单元，用于读取预置值；

第二判断子单元，用于判断所述预置值是否为目标阈值，所述目标阈值指示根据所述用户 token 的过期时刻进行鉴权；

第二鉴权子单元，若所述预置值为根据所述用户 token 的过期时刻进行鉴权，则用于获取所述用户 token 的过期时刻；

第三判断子单元，用于判断所述用户 token 的过期时刻是否小于当前时刻；

第二处理子单元，若所述用户 token 的过期时刻小于所述当前时刻，则用于确定鉴权单元；

第三处理子单元，若所述用户 token 的过期时刻大于或等于所述当前时刻，则用于确定鉴权成功。

15、一种基于全链路数据鉴权设备，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计算机程序，所述处理器执行所述计算机程序时实现如下步骤：

接收链路上报的数据；

解析所述链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；

根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权；

若鉴权失败，则丢弃所述链路上报的数据；

若鉴权成功，则采集所述链路上报的数据。

16、根据权利要求 15 所述的全链路数据鉴权设备，所述处理器执行所述计算机程序实现所述根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权时，包括以下步骤：

根据 JWT 协议对所述用户 token 进行解析，得到所述用户 token 的鉴权信息；

判断所述用户 token 的鉴权信息是否存在异常；

若所述用户 token 的鉴权信息存在异常，则确定鉴权失败；

若所述用户 token 的鉴权信息不存在异常，则根据所述用户 token 的鉴权信息、所述 agent 唯一标识和所述用户 IP 地址进行鉴权。

17、根据权利要求 16 所述的全链路数据鉴权设备，所述处理器执行所述计算机程序实现所述根据 JWT 协议对所述用户 token 进行解析，得到所述用户 token 的鉴权信息时，包括以下步骤：

根据所述 JWT 协议对所述用户 token 进行分割，得到所述用户 token 的头部、所述用户 token 的载荷和所述用户 token 的签名；

对所述用户 token 的头部进行 base64 解密，得到所述头部声明的加密算法；

根据所述头部声明的加密算法对所述用户 token 的头部和所述用户 token 的载荷进行组合加密，得到待验证签名；

判断所述待验证签名与所述用户 token 的签名是否相同；

若所述待验证签名与所述用户 token 的签名相同，则对所述用户 token 的载荷进行 base64 解密，得到所述用户 token 的鉴权信息。

18、根据权利要求 16 所述的全链路数据鉴权设备，所述处理器执行所述计算机程序实现所述若所述用户 token 的鉴权信息不存在异常，则根据所述用户 token 的鉴权信息、所述 agent 唯一标识和所述用户 IP 地址进行鉴权时，包括以下步骤：

若所述用户 token 的鉴权信息不存在异常，则判断所述用户 token 的鉴权信息是否包括所述 agent 唯一标识；

若所述用户 token 的鉴权信息不包括所述 agent 唯一标识，则确定鉴权失败；

若所述用户 token 的鉴权信息包括所述 agent 唯一标识，则判断所述用户 token 的鉴权信息是否包括所述用户 IP 地址；

若所述用户 token 的鉴权信息不包括所述用户 IP 地址，则确定鉴权失败；

若所述用户 token 的鉴权信息包括所述用户 IP 地址，则确定鉴权成功。

19、根据权利要求 15 所述的全链路数据鉴权设备，所述处理器执行所述计算机程序实现所述若鉴权失败，则丢弃所述链路上报的数据时，包括以下步骤：

发送鉴权失败的原因值；

获取鉴权时刻；

记录所述鉴权失败的原因值、所述 agent 唯一标识、所述用户 IP 地址和所述鉴权时刻；

删除所述链路上报的数据。

20、一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机指令，当所述计算机指令在计算机上运行时，使得计算机执行如下步骤：

接收链路上报的数据；

解析所述链路上报的数据，得到用户令牌 token、代理 agent 唯一标识和用户 IP 地址；

根据所述用户 token、所述 agent 唯一标识和所述用户 IP 地址进行鉴权；

若鉴权失败，则丢弃所述链路上报的数据；

若鉴权成功，则采集所述链路上报的数据。

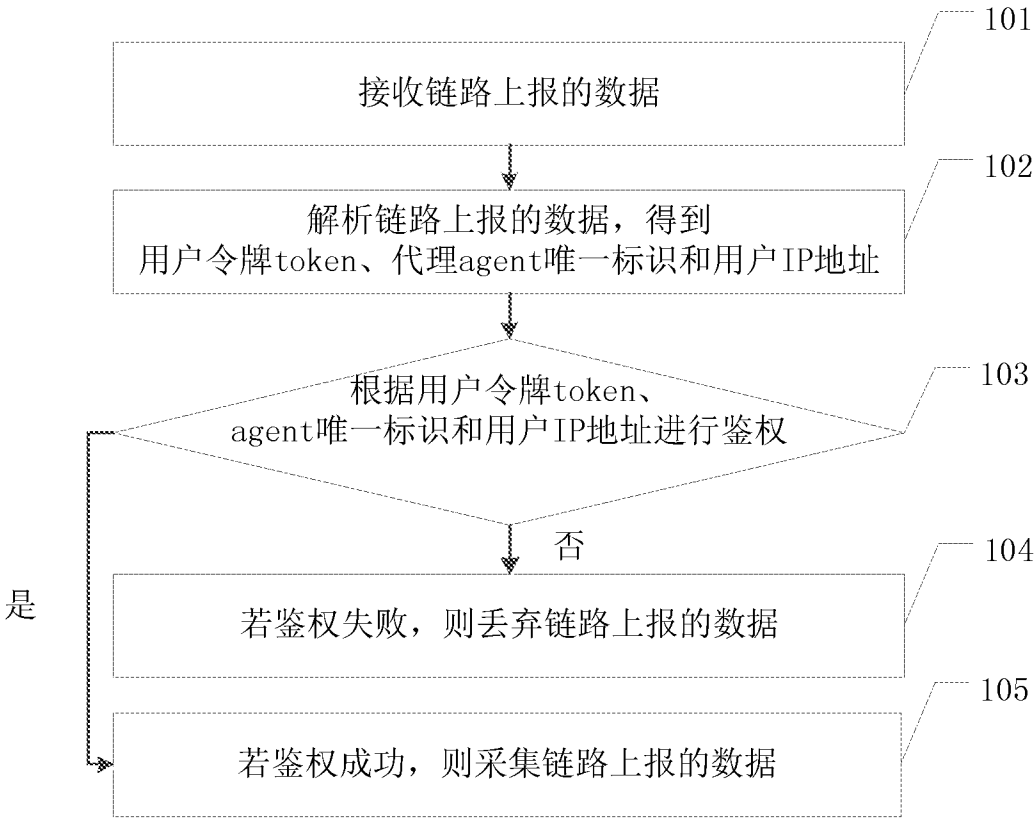

101
接收链路上报的数据
102
解析链路上报的数据，得到
用户令牌token、代理agent唯一标识和用户IP地址
103
根据用户令牌token、
agent唯一标识和用户IP地址进行鉴权
否
是
104
若鉴权失败，则丢弃链路上报的数据
105
若鉴权成功，则采集链路上报的数据

图 1

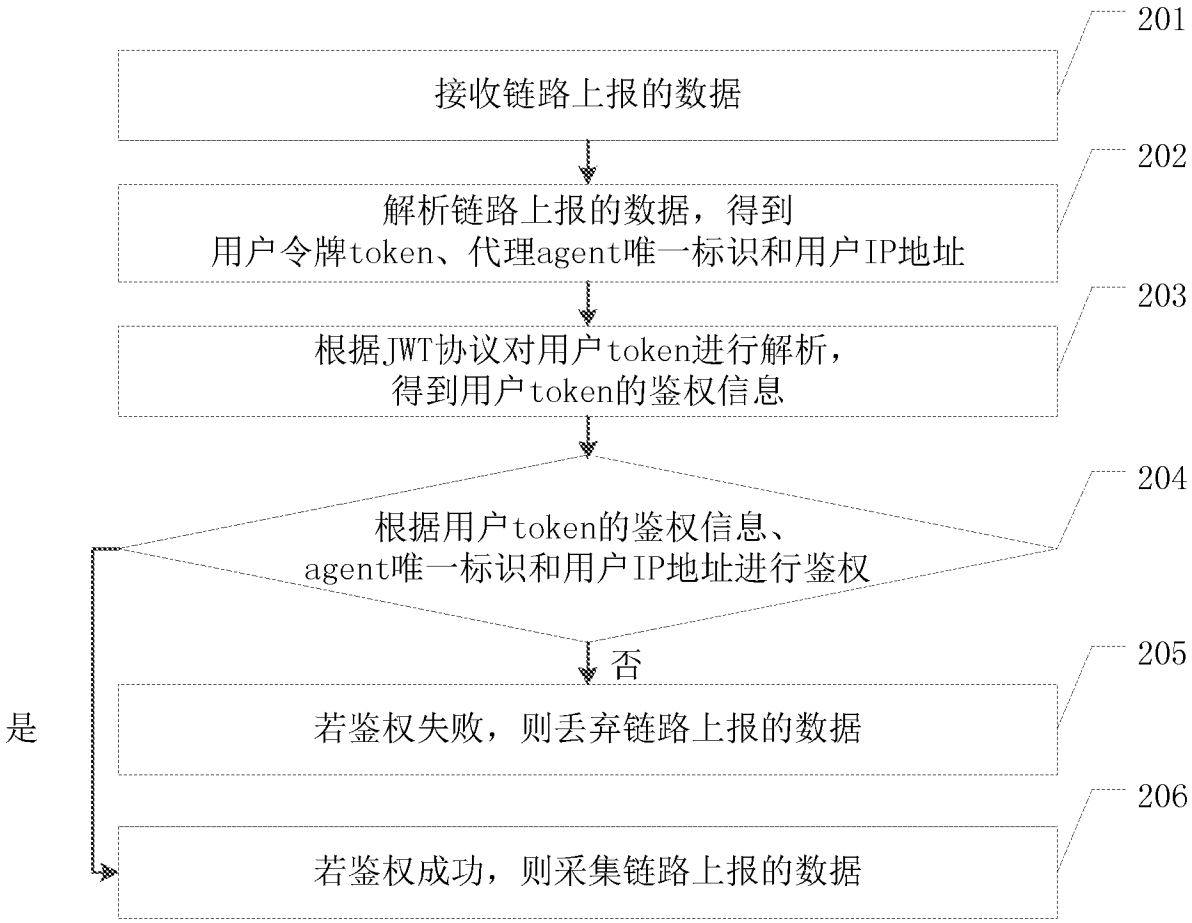

201
接收链路上报的数据
202
解析链路上报的数据，得到
用户令牌token、代理agent唯一标识和用户IP地址
203
根据JWT协议对用户token进行解析，
得到用户token的鉴权信息
204
根据用户token的鉴权信息、
agent唯一标识和用户IP地址进行鉴权
否
205
若鉴权失败，则丢弃链路上报的数据
是
206
若鉴权成功，则采集链路上报的数据

图 2

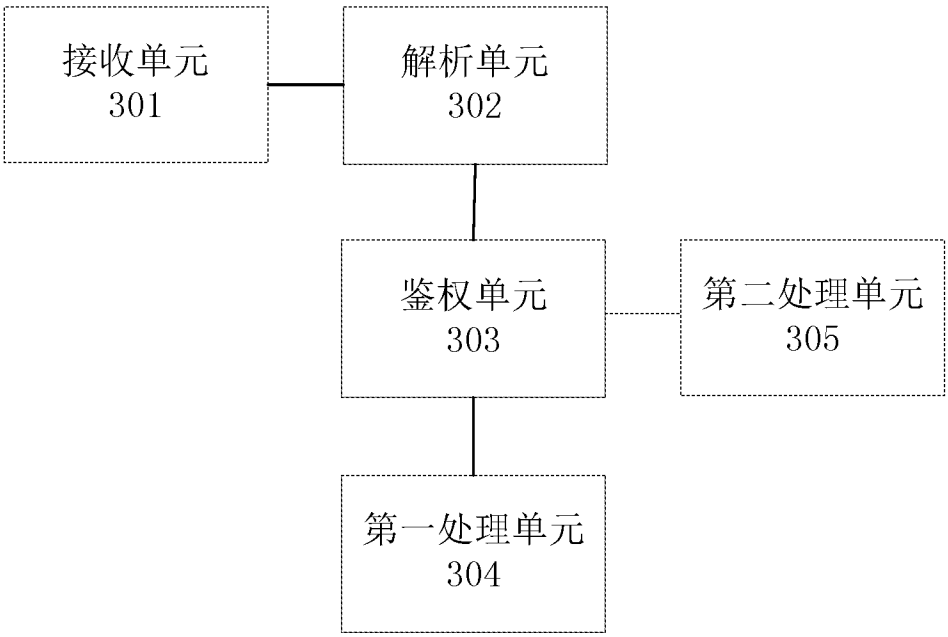


图 3

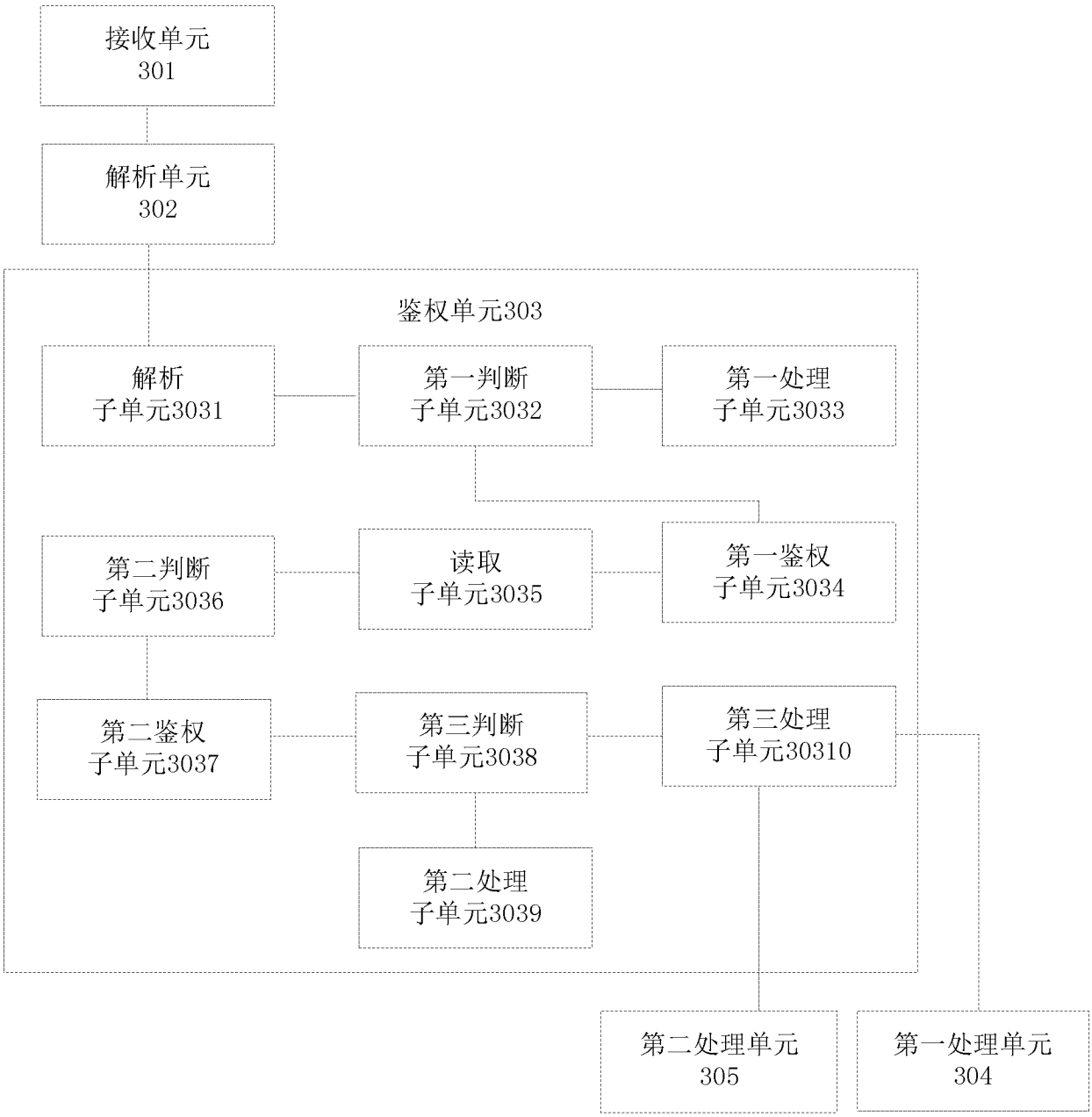

接收单元
301
解析单元
302
鉴权单元303
解析
子单元3031
第一判断
子单元3032
第一处理
子单元3033
第二判断
子单元3036
读取
子单元3035
第一鉴权
子单元3034
第二鉴权
子单元3037
第三判断
子单元3038
第三处理
子单元30310
第二处理
子单元3039
第二处理单元
305
第一处理单元
304

图 4

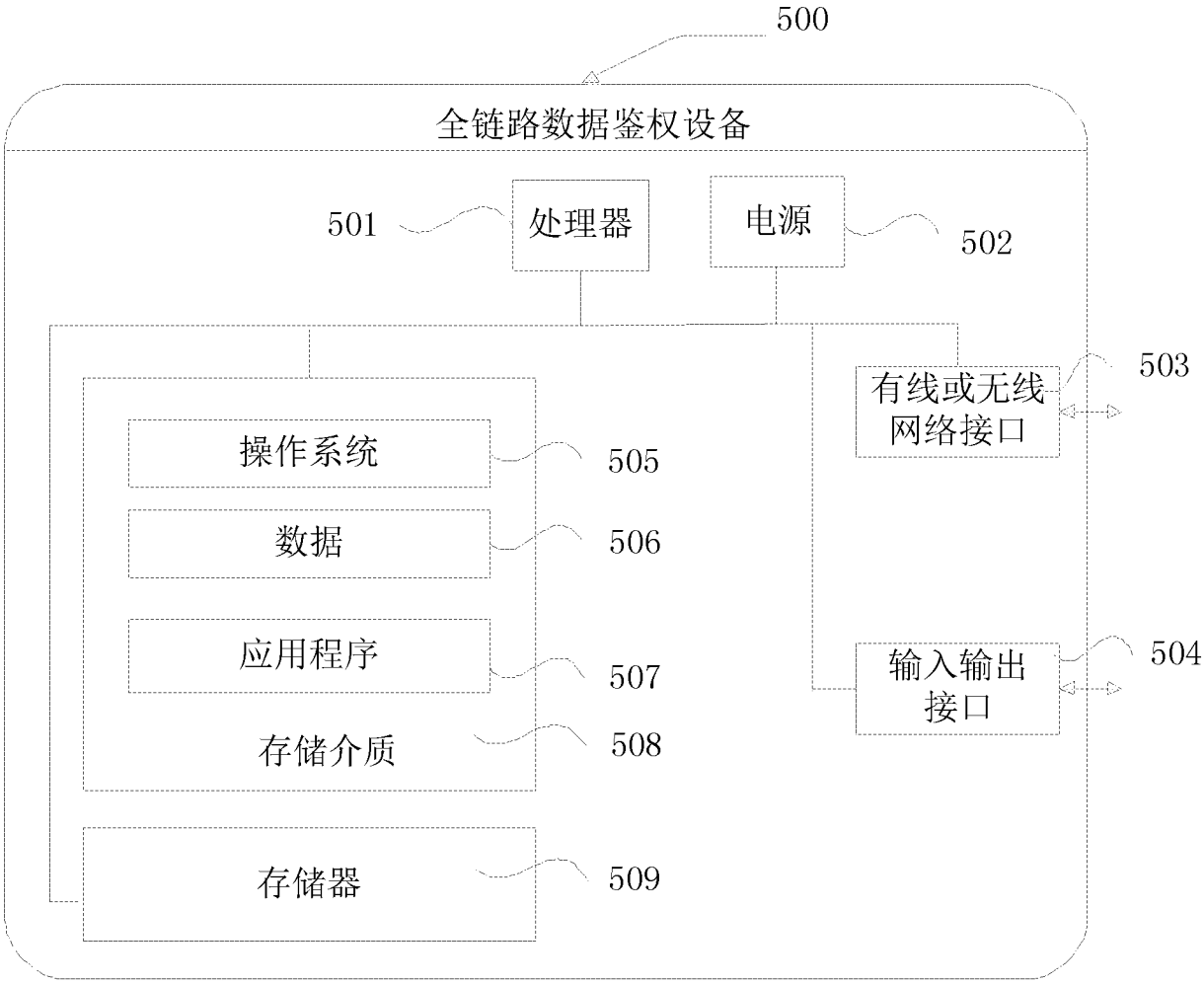

500
全链路数据鉴权设备
501
处理器
电源
502
503
有线或无线
网络接口
操作系统
505
数据
506
应用程序
507
504
输入输出
接口
存储介质
508
存储器
509

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/102497

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 安全, 认证, 鉴权, 代理, 标识, 地址, 链路, 数据, 异常, 头部, 载荷, 签名; JSON WEB Token, JWT, security, authentication, agent, identifier, address, IP, link, data, abnormal, header, payload, signature

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	项武铭 等 (XIANG, Wuming et al.):. ""现代计算机 (Modern Computer)";" *"基于JWT的RESTful API角色权限验证方案设计 (Design of Role Authentication Scheme for RESTful API Based on JWT)";*, 05 December 2018 (2018-12-05), sections 1-2	1-20
A	CN 107925668 A (CONVIDA WIRELESS LLC) 17 April 2018 (2018-04-17) entire document	1-20
A	CN 109104432 A (SHENZHEN ZHUYUN SCIENCE & TECHNOLOGY CO., LTD.) 28 December 2018 (2018-12-28) entire document	1-20
A	CN 109446769 A (BEIJING INSTITUTE OF COMPUTER TECHNOLOGY AND APPLICATION) 08 March 2019 (2019-03-08) entire document	1-20
A	CN 109660343 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 19 April 2019 (2019-04-19) entire document	1-20
A	US 2015341176 A1 (VMWARE, INC.) 26 November 2015 (2015-11-26) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 March 2020	**18 March 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/102497

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107925668	A	17 April 2018	EP	3318036	A1	09 May 2018
				JP	2018525722	A	06 September 2018
				KR	20180026751	A	13 March 2018
				US	2018183802	A1	28 June 2018
				WO	2017004373	A1	05 January 2017
CN	109104432	A	28 December 2018	None			
CN	109446769	A	08 March 2019	None			
CN	109660343	A	19 April 2019	None			
US	2015341176	A1	26 November 2015	None			

国际检索报告

国际申请号
PCT/CN2019/102497

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,CNKI,WPI,EPODOC：安全，认证，鉴权，代理，标识，地址，链路，数据，异常，头部，载荷，签名；JSON WEB Token，JWT，security，authentication，agent，identifier，address，IP，link，data，abnormal，header，payload，signature

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	项武铭 等；. ""现代计算机"；" "基于JWT 的RESTful API 角色权限验证方案设计"；，2018年 12月 5日 (2018-12-05)， 第1-2节	1-20
A	CN 107925668 A (康维达无线有限责任公司) 2018年 4月 17日 (2018-04-17) 全文	1-20
A	CN 109104432 A (深圳竹云科技有限公司) 2018年 12月 28日 (2018-12-28) 全文	1-20
A	CN 109446769 A (北京计算机技术及应用研究所) 2019年 3月 8日 (2019-03-08) 全文	1-20
A	CN 109660343 A (平安科技深圳有限公司) 2019年 4月 19日 (2019-04-19) 全文	1-20
A	US 2015341176 A1 (VMWARE, INC.) 2015年 11月 26日 (2015-11-26) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 3月 6日	2020年 3月 18日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 彭亮 电话号码 86-10-53961652

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/102497

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	107925668	A	2018年 4月 17日	EP	3318036	A1	2018年 5月 9日
				JP	2018525722	A	2018年 9月 6日
				KR	20180026751	A	2018年 3月 13日
				US	2018183802	A1	2018年 6月 28日
				WO	2017004373	A1	2017年 1月 5日
CN	109104432	A	2018年 12月 28日	无			
CN	109446769	A	2019年 3月 8日	无			
CN	109660343	A	2019年 4月 19日	无			
US	2015341176	A1	2015年 11月 26日	无			