(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114726547 A
(43)申请公布日 2022.07.08

(21)申请号 202210525522.8

(22)申请日 2022.05.16

(71)申请人 中国信息通信研究院
地址 100191 北京市海淀区学院路40号

(72)发明人 谢滨 田娟 刘阳 朱斯语 程彤彤

(74)专利代理机构 北京思源智汇知识产权代理有限公司 11657
专利代理师 杜毅

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 67/125(2022.01)

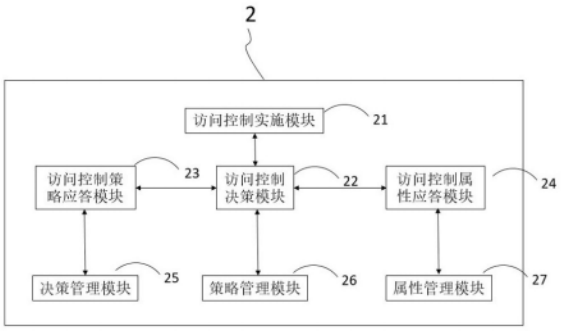
权利要求书2页 说明书10页 附图3页

(54)发明名称

基于数据交换中间件工业互联网访问控制方法和可读介质

(57)摘要

本发明实施例公开了一种基于数据交换中间件工业互联网访问控制方法和可读介质，其中，所述数据交换中间件接收来自发起者(1)的访问请求，根据固定交互模式对来自不同代理方式的访问请求进行一致化处理获得决策请求；所述数据交换中间件依据访问控制策略与访问控制属性完成决策评估，发送最终决策结果；所述数据交换中间件根据所述最终决策结果拒绝或允许发起者对目标的访问。本发明实施例通过将多种访问控制策略与多种访问控制属性相结合完成决策评估对数据滥用、隐私泄露等威胁提供安全防护。



CN 114726547 A

1.一种基于数据交换中间件工业互联网访问控制方法,所述数据交换中间件(2)包括访问控制实施模块(21)、访问控制决策模块(22)、访问控制策略应答模块(23)、访问控制属性应答模块(24);

其特征在于,包括:

所述访问控制实施模块(21)接收来自发起者(1)的访问请求,根据固定交互模式对来自不同代理方式的所述发起者(1)的访问请求进行一致化处理获得决策请求,并向所述访问控制决策模块(22)发送所述决策请求;

所述访问控制决策模块(22)根据获取的所述决策请求为参数,向所述访问控制策略应答模块(23)发出策略查询请求;所述访问控制策略应答模块(23)检索适用策略后,向所述访问控制决策模块(22)返回包括访问控制策略的访问控制策略消息;

所述访问控制决策模块(22)对返回所述访问控制策略进行评估;当在评估过程中发现缺乏访问目标的属性时,向所述访问控制属性应答模块(24)发出属性查询请求;所述访问控制属性应答模块(24)查询并验证属性发布点存储在本地数据库中的属性信息,生成包括访问控制属性的访问控制属性消息返回至所述访问控制决策模块(22);

当所述访问控制属性应答模块(24)查询的属性是外部安全域中的属性,则向外部安全域的外域访问控制属性应答模块(4)进行查询,以获得外部安全域中的访问控制属性,并通过属性映射关系确定属性的可信性,生成访问控制属性消息返回至所述访问控制决策模块(22);

所述访问控制决策模块(22)依据所述访问控制策略与所述访问控制属性完成决策评估,向所述访问控制实施模块(21)发送最终决策结果;

所述访问控制实施模块(21)根据返回的所述最终决策结果拒绝或允许发起者对目标的访问。

2.权利要求1中所述的方法,其特征在于,所述访问控制实施模块(21)能够收集发起者辅助性信息;

所述访问控制决策模块(22)进一步包括,依据所述发起者(1)辅助性信息、所述访问控制策略与所述访问控制属性完成决策评估,向所述访问控制实施模块(21)发送最终决策结果。

3.权利要求1或2中所述的方法,其特征在于,所述访问控制决策模块(22)进一步包括访问控制决策,

所述访问控制决策进一步包括:开放式策略、或保守式策略;

其中,

所述开放式策略的决策逻辑为,如果没有提供显式策略明确禁止访问行为,则认为允许访问进行;

所述保守式策略的决策逻辑为,如果没有提供显式策略明确允许访问行为,则认为禁止访问进行。

4.权利要求3中所述的方法,其特征在于,

所述访问控制决策模块(22)在多条访问控制策略同时给出明确决策结果且所述决策结果之间存在冲突,指定冲突消解策略;

所述冲突消解策略包括:肯定判定优先、否定判定优先、首次判定优先任一项。

5.权利要求4中所述的方法,其特征在于,

所述访问控制策略应答模块(23)中存储的策略具体包括:

所述发起者(1)设置的白名单和黑名单;

访问目标(3)设置的白名单和黑名单。

6.权利要求5中所述的方法,其特征在于,所述访问目标(3)的属性具体包括:

主体标识、主体类型或名称、主体属性值、主体地域、主体制造商、主体使用商、主体属性信息摘要的签名。

7.权利要求6中所述的方法,其特征在于,所述主体属性信息摘要的计算方式包括:

主体属性信息摘要=HASH256(a1 || a2 || a3) and HASH256(b1 || b2 || b3);

其中HASH256为哈希256算法,a1为主体标识,a2为主体类型编码或名称编码,a3为主体属性值,b1为主体地域编码,b2为主体制造商编码,b3为主体使用商编码,||为连接符号,and代表按位与运算。

8.权利要求6中所述的方法,其特征在于,所述访问控制决策模块(22)依据所述访问控制策略与所述访问控制属性完成决策评估具体包括:

根据所述发起者(1)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3);

根据所述访问目标(3)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3);

根据所述访问控制属性确定所述访问目标(3)是否允许访问;

根据所述访问控制决策决定所述访问目标(3)是否允许访问。

9.权利要求6中所述的方法,其特征在于,所述访问控制决策模块(22)依据所述发起者辅助性信息、所述访问控制策略与所述访问控制属性完成决策评估具体包括:

根据所述发起者辅助性信息确定所述发起者(1)是否有权允许访问所述访问目标(3);

根据所述发起者(1)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3);

根据所述访问目标(3)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3);

根据所述访问控制属性确定所述访问目标(3)是否允许访问;

根据所述访问控制决策决定所述访问目标(3)是否允许访问。

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,实现上述权利要求1-9任一所述的方法。

基于数据交换中间件工业互联网访问控制方法和可读介质

技术领域

[0001] 本发明涉及访问控制技术，尤其涉及基于数据交换中间件的工业互联网访问控制方法和可读介质。

背景技术

[0002] 国际主流工业大国都在大力推进工业互联网建设，并以工业互联网平台为引擎，探索工业制造业数字化、智能化转型发展新模式。工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的工业云平台。

[0003] 伴随工业互联网平台开放性的提升，工业应用研发创新能力增强，呈现开放定制的特征。工业互联网平台上存在大量的接入设备，通过工业互联网可以实现企业之间、工业设备之间的快速有效通信，各企业之间可以通过中间媒介进行数据交互，例如各企业设置了边缘侧中间件，通过边缘侧中间件可以在企业之间进行数据采集、协议转换和数据处理。

[0004] 当前工业应用层的软件重视功能、性能设计，对鉴别及访问控制等安全机制设计简单且粒度较粗，攻击者可通过IP欺骗、端口扫描、数据包嗅探等通用手段发现平台应用存在的安全缺陷，进而发起深度攻击。现有网络安全机制，没有考虑到工业互联网网络特性和接入设备属性，如何保证接入工业互联网中企业之间进行数据交互时的数据安全性，是一个亟待解决的问题。

[0005] 海量异构工业设备接入工业互联网平台时，连接条件和连接方式多样，存在大量不安全的接口。当前工业互联网平台边缘层缺乏对异构工业设备接入的安全管理，接口安全防护也有所欠缺。

发明内容

[0006] 本发明实施例提供一种基于数据交换中间件工业互联网访问控制方法和可读介质，以克服工业互联网边缘层能突破异构工业设备的对接限制、互操作限制和管控限制，提供统一的安全接口自动部署及安全策略。

[0007] 根据本发明实施例的一个方面，提供的一种基于数据交换中间件的工业互联网访问控制方法，所述数据交换中间件(2)包括访问控制实施模块(21)、访问控制决策模块(22)、访问控制策略应答模块(23)、访问控制属性应答模块(24)；具体包括：

所述访问控制实施模块(21)接收来自发起者(1)的访问请求，根据固定交互模式对来自不同代理方式的所述发起者(1)的访问请求进行一致化处理获得决策请求，并向所述访问控制决策模块(22)发送所述决策请求；

所述访问控制决策模块(22)根据获取的所述决策请求为参数，向所述访问控制策略应答模块(23)发出策略查询请求；所述访问控制策略应答模块(23)检索适用策略后，向所述访问控制决策模块(22)返回包括访问控制策略的访问控制策略消息；

所述访问控制决策模块(22)对返回所述访问控制策略进行评估；当在评估过程中

发现缺乏访问目标的属性时，向所述访问控制属性应答模块(24)发出属性查询请求；所述访问控制属性应答模块(24)查询并验证属性发布点存储在本地数据库中的属性信息，生成包括访问控制属性的访问控制属性消息返回至所述访问控制决策模块(22)；

当所述访问控制属性应答模块(24)查询的属性是外部安全域中的属性，则向外部安全域的外域访问控制属性应答模块(4)进行查询，以获得外部安全域中的访问控制属性，并通过属性映射关系确定属性的可信性，生成访问控制属性消息返回至所述访问控制决策模块(22)；

所述访问控制决策模块(22)依据所述访问控制策略与所述访问控制属性完成决策评估，向所述访问控制实施模块(21)发送最终决策结果；

所述访问控制实施模块(21)根据返回的所述最终决策结果拒绝或允许发起者对目标的访问。

[0008] 可选地，所述访问控制决策模块(22)进一步包括，依据所述发起者辅助性信息、所述访问控制策略与所述访问控制属性完成决策评估，向所述访问控制实施模块(21)发送最终决策结果。

[0009] 可选地，所述访问控制决策进一步包括：开放式策略、或保守式策略；

其中，

开放式策略的决策逻辑为，如果没有提供显式策略明确禁止某访问行为，则认为允许该类访问进行；

保守式策略的决策逻辑为，如果没有提供显式策略明确允许某访问行为，则认为禁止该类访问进行。

[0010] 可选地，所述访问控制决策模块(22)在多条访问控制策略同时给出明确决策结果且决策结果存在冲突时，指定冲突消解策略；

消解策略包括：肯定判定优先、否定判定优先、首次判定优先任一项。

[0011] 可选地，所述访问控制策略应答模块(23)中存储的策略具体包括：

所述发起者(1)设置的白名单和黑名单；

访问目标(3)设置的白名单和黑名单。

[0012] 可选地，主体标识、主体类型或名称、主体属性值、主体地域、主体制造商、主体使用商、主体属性信息摘要的签名。

[0013] 可选地，主体属性信息摘要=HASH256(a1 || a2 || a3) and HASH256(b1 || b2 || b3)；

其中HASH256为哈希256算法，a1为主体标识，a2为主体类型编码或名称编码，a3为主体属性值，b1为主体地域编码，b2为主体制造商编码，b3为主体使用商编码，||为连接符号。

[0014] 可选地，根据所述发起者(1)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3)；

根据所述访问目标(3)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3)；

根据所述访问控制属性确定所述访问目标(3)是否允许访问；

根据所述访问控制决策决定所述访问目标(3)是否允许访问。

[0015] 可选地，根据所述发起者辅助性信息确定所述发起者(1)是否有权允许访问所述访问目标(3)；

根据所述发起者(1)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3)；

根据所述访问目标(3)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3)；

根据所述访问控制属性确定所述访问目标(3)是否允许访问；

根据所述访问控制决策决定所述访问目标(3)是否允许访问。

[0016] 根据本发明实施例的第二个方面，提供的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，实现本公开上述任一实施例所述的方法。

[0017] 基于本发明上述实施例提供的基于数据交换中间件的工业互联网访问控制方法和可读介质，可以实现如下有益效果：

工业互联网平台上，不同业务流程中存在多样化的工业应用，存在大量应用间数据安全共享与协同处理的场景，通过将多种访问控制策略与多种访问控制属性相结合完成决策评估实现了根据数据共享需求对各应用、用户进行细粒度访问控制。另一方面，为保证应用之间鉴权的合理性，防止出现跨应用的攻击，在中间件明确区分访问控制策略和访问控制属性，保证平台的应用安全。

[0018] 伴随工业互联网平台开放性的提升，工业应用研发创新能力增强，呈现开放定制的特征，工业互联网平台上存在大量未知的应用发布者，应用发布者使用不同协议或者不同标准，为保证工业应用来源的安全、可靠，在中间件对应用开发者各种信息进行一致化处理，提高了系统间的兼容性。

[0019] 工业数据包括研发设计、开发测试、系统设备资产信息、控制信息、工况状态、工艺参数、系统日志、物流、产品售后服务等产品全生命周期各环节所产生的各类数据，其中往往包含工业企业的商业秘密。工业互联网平台上数据的流通与共享将扩大数据安全管理的范围，通过将多种访问控制策略与多种访问控制属性相结合完成决策评估对数据滥用、隐私泄露等威胁提供安全防护。

[0020] 下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

附图说明

[0021] 构成说明书的一部分的附图描述了本发明的实施例，并且连同描述一起用于解释本发明的原理。

[0022] 参照附图，根据下面的详细描述，可以更加清楚地理解本发明，其中：

图1为本发明数据交换中间件的结构示意图；

图2为本发明访问控制决策模块的结构示意图；

图3为本发明访问控制策略应答模块的结构示意图；

图4为本发明访问控制属性应答模块的结构示意图；

图5为本发明基于数据交换中间件的工业互联网访问控制方法的流程图。

具体实施方式

[0023] 现在将参照附图来详细描述本发明的各种示例性实施例。应注意到:除非另外具体说明,否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本发明的范围。

[0024] 请参考图1,数据交换中间件(2)包括访问控制实施模块(21)、访问控制决策模块(22)、访问控制策略应答模块(23)、访问控制属性应答模块(24)、决策管理模块(25)、策略管理模块(26)、属性管理模块(27)。

[0025] 其中,所述访问控制实施模块(21),接收来自发起者(1)的访问请求,根据固定交互模式对来自不同代理方式的所述发起者(1)的访问请求进行一致化处理获得决策请求,并向所述访问控制决策模块(22)发送所述决策请求。

[0026] 所述访问控制实施模块(21)接收来自发起者的访问请求,根据固定交互模式对来自不同代理方式(如:“浏览器/服务器”结构、“客户端/服务器”结构等)用户代理的请求进行一致化处理。访问请求信息的传递不限制具体的传输协议,满足访问实施控制要求的传输协议都可以负责处理信息传递。所述访问控制实施模块(21)能够收集其他对访问决策提供帮助的发起者辅助性信息,例如用户的属性信息,可以感知的若干系统信息等。管理者通过配置的方式指定优先附加的辅助信息,辅助信息的添加并不一定限制在访问控制实施中,其他根据需要也可以具备该功能。所述访问控制实施模块(21)应能够传递决策请求至所述访问控制决策模块(22)并接收决策结果。访问请求的决策结果可能表示为某种抽象形式,访问实施应根据所在的应用场景和技术背景将其转换为具体的应用程序执行逻辑,保证高层抽象安全约束和底层程序逻辑的一致性。

[0027] 发起者可以是工业互联网中接入的企业节点、个人移动终端、工业APP等。

[0028] 所述访问控制实施模块(21)够对请求格式进行标准形式的转换,宜采用基于属性的描述机制对访问请求进行统一描述,进行一致化处理获得决策请求。

[0029] 图2是所述访问控制决策模块(22)的结构示意图,所述访问控制决策模块(22)进一步包括策略检索子单元(221)、属性检索子单元(222)和控制决策模块(223)。所述控制决策模块(223)是所述访问控制决策模块(22)决策和执行单元;所述策略检索子单元(221)用于和访问控制策略应答模块(23)进行通信,获得策略信息;所述属性检索子单元(222)用于和访问控制属性应答模块(24)进行通信,获得属性信息。

[0030] 所述访问控制决策模块(22)负责从所述访问控制实施模块(21)接受决策请求,通过查找适用策略和相对应的访问控制属性,依据访问判定逻辑产生一个决策结果,并将该决策结果返回给所述访问控制实施模块(21)。

[0031] 所述访问控制决策模块(22)接收决策请求,并对请求内的信息进行解析分类。

[0032] 所述访问控制决策模块(22)用于实现访问决策逻辑执行功能。决策逻辑可以采用已有的多种访问控制模型和访问控制机制,尽可能提高其兼容性。所述访问控制决策模块(22)在多条策略同时给出明确决策结果且决策结果存在冲突时,指定冲突消解策略,以处理可能产生的决策结果不一致性,常用的消解策略包括:肯定判定优先、否定判定优先、首次判定优先等。

[0033] 访问控制决策应从宏观角度制定最基本的资源安全策略,以提供最低限度的安全保障。访问控制决策通过开放式策略和保守式策略实现这种可预知的和最低限度的安全保

障。开放式策略的决策逻辑为:如果没有提供显式策略明确禁止某访问行为,则认为允许该类访问进行。保守式策略的决策逻辑为,如果没有提供显式策略明确允许某访问行为,则认为禁止该类访问进行。采用何种策略取决于具体应用的资源对象敏感性和资源对象使用目的。

[0034] 所述访问控制决策模块(22)也可以内部进行访问控制策略检索收集。例如,在运行决策逻辑前,将所有策略一次性导入临时存储区,之后所有的匹配操作都针对存储区内的策略进行。当策略数目较大时,可以根据某些属性特征或者策略标识从策略库中获取规模较小的策略子集,减少实际匹配的策略数量,提高匹配效率。例如,以某个属性类型或者具体的属性值为关键字,或者以某种特定的策略类型为关键字对策略库进行检索。

[0035] 所述访问控制决策模块(22)应具有相关属性信息的检索功能。属性检索过程可以兼容处理不同的属性格式,例如X.509格式的属性证书、SAMI格式的安全断言以及LDAP目录中的属性条目等。考虑到和其他安全组件的集成性,例如为安全审计提供历史访问的相关数据等。访问控制决策在完成请求决策的同时,可以对整个过程涉及的信息进行分类记录。以上信息应保证存储的安全性和与历史记录的一致性,并且可根据特殊的审计需要增加相应的记录信息类型,本标准不对数据存储的形式和方案进行规定。

[0036] 所述访问控制决策模块(22)依据所述访问控制策略应答模块(23)返回的访问控制策略与访问控制属性应答模块(24)返回的访问控制属性完成决策评估,向所述访问控制实施模块(21)发送最终决策结果。所述访问控制决策模块(22)也可以再结合所述发起者辅助性信息完成决策评估。

[0037] 图3为本发明访问控制策略应答模块的结构示意图,所述访问控制策略应答模块(23)具备包括策略应答模块(231)和策略数据库(232)。所述策略数据库(232)用于存储策略管理模块(24)配置的策略;策略应答模块(231)接收到所述访问控制决策模块(22)发送的策略查询请求,在所述策略数据库(232)中检索策略,并向所述访问控制决策模块(22)返回查询到的策略。

[0038] 所述访问控制决策模块(22)根据获取的所述决策请求为参数,向所述访问控制策略应答模块(23)发出策略查询请求;所述访问控制策略应答模块(23)检索适用策略后,向所述访问控制决策模块(22)返回包括访问控制策略的访问控制策略消息。

[0039] 所述访问控制策略应答模块(23)负责响应所述访问控制决策模块(22)的策略查询请求,负责整个中间件访问控制策略的底层处理,对不同形式的策略表达进行一致性转化,完成对适用策略的检索并以安全的方式传输至访问控制决策组件。

[0040] 所述访问控制策略应答模块(23)对不同形式的策略表达进行一致性转化,使决策逻辑所依赖的策略集具有统一的格式和语义。策略转化过程可能需要界定不同策略特征间的转换规则,但应保证策略转化不影响最终的安全目标。所述访问控制策略应答模块(23)应能够处理来自决策带有多种查询参数的策略检索请求,并获取满足要求的策略集合。所述访问控制策略应答模块(23)与所述访问控制决策模块(22)传输的方式和格式进行统一制定,应答完成策略检索后,将响应策略集合以安全可靠的传输协议传输至决策。例如,通过网络层的socket通信协议直接对策略条目进行编码传输,或针对XML类型的策略格式采用类似SOAP协议的XML.RPC方式进行传输。

[0041] 所述访问控制决策模块(22)通过策略管理模块(24)提供对策略的一般性管理功

能，例如策略的添加、修改、删除、更新等，以方便中间件对系统安全策略的控制和掌握。策略管理模块(24)宜提供策略优先级机制，制定策略冲突消解规则，便于访问控制决策执行具体的决策逻辑。策略管理模块(24)宜提供策略一致性检测功能，在策略实体和高层安全目标间进行一致性验证和测试，保证策略实体符合系统的安全管理初衷。

[0042] 常见的策略有设置黑白名单。黑白名单包括地址信息、产品信息等。

[0043] 图4为本发明访问控制属性应答模块的结构示意图，所述访问控制属性应答模块(24)具备包括属性应答模块(241)和属性数据库(242)。所述属性数据库(242)用于存储属性发布点发布的属性信息；所述属性应答模块(241)接收到所述访问控制决策模块(22)发送的属性查询请求，优先在所述属性数据库(242)中检索属性，并向所述访问控制决策模块(22)返回查询到的属性；如果没有在所述属性数据库(242)中检索到对应的属性信息，则向外部安全域的外域访问控制属性应答模块(4)进行查询。

[0044] 所述访问控制决策模块(22)向所述访问控制属性应答模块(24)发出属性查询请求；所述访问控制属性应答模块(24)查询并验证属性发布点存储在本地数据库中的属性信息，生成包括访问控制属性的访问控制属性消息返回至所述访问控制决策模块(22)。

[0045] 所述访问控制属性应答模块(24)负责对访问判定过程中需要的各种类型属性信息进行收集，生成并发布属性断言，并将属性信息集合以安全的方式传输至所述访问控制决策模块(22)。所述访问控制属性应答模块(24)主要负责访问决策可能触发的属性信息收集，辅助访问控制决策完成最终的请求决策。属性信息一般应包含属性的主体标识、属性类型或名称、具体的属性值、应答及对属性信息摘要的签名等。

[0046] 当决策请求中包含的用户属性信息不足以使决策逻辑给出决策结果时，决策需要向访问控制属性应答发送属性查询请求。所述访问控制属性应答模块(24)能根据用户标识对属性信息进行集成检索，形成统一的属性表达语义。在对检索后获取的用户属性进行确认前，所述访问控制属性应答模块(24)对这些属性信息的有效性进行验证。验证过程可能是针对属性实体的数字签名验证，也可能涉及对属性颁发实体的数字身份验证，验证能否通过取决于对验证信息的可信性。

[0047] 当所述访问控制属性应答模块(24)查询的属性是外部安全域中的属性，则向外部安全域的外域访问控制属性应答模块(4)进行查询，以获得外域的用户属性信息。针对来自外域的用户属性信息，所述访问控制属性应答模块(24)应实现域间属性转译，根据外域用户属性检索适用的属性映射规则，推导出外域属性对应的本域属性信息，以决策可理解的域内属性信息格式进行发布。应答宜实现对来自信息系统自身状态、上下文环境、网络状况等一些可以描述访问进行时的外界信息感应点的属性进行接收和主动查询。在获取这些属性后，所述访问控制属性应答模块(24)将这些属性信息转换为决策可理解的语义及格式并以属性断言的格式进行转发。

[0048] 所述访问控制属性应答模块(24)在获取到查询的属性信息后，以决策可验证的属性断言方式发布属性信息。属性断言应包含属性的主体标识，属性类型或名称、具体的属性值、应答及对属性信息摘要的签名等。

[0049] 所述访问控制属性应答模块(24)与所述访问控制决策模块(22)就属性传输的方式和格式进行统一制定，应答完成属性检索后，将属性信息集合以交全可靠的传输协议传输至决策。

[0050] 所述访问控制决策模块(22)应通过所述属性管理模块(26)提供对属性信息的一般性管理功能,例如属性的颁发、撤销、更新等,以方便中间件对属性信息的控制和掌握。

[0051] 为了支持跨域访问控制等多域应用场景,所述属性管理模块(26)应提供域间属性映射功能,制定属性映射规则,可发布映射断言供外域的属性发布进行查询。所述属性管理模块(26)应提供属性一致性检测功能,限制用户同时拥有违反安全约束的多个属性。

[0052] 图5为本发明基于数据交换中间件的工业互联网访问控制方法的流程图,所述工业互联网包括发起者(1)、数据交换中间件(2)、访问目标(3)和外域访问控制属性应答模块(4),具体方法如图5所示:

步骤一、所述访问控制实施模块(21)接收来自发起者(1)的访问请求,根据固定交互模式对来自不同代理方式的所述发起者(1)的访问请求进行一致化处理获得决策请求,并向所述访问控制决策模块(22)发送所述决策请求。

[0053] 所述访问控制实施模块(21)能够收集发起者辅助性信息,将发起者辅助性信息发送给所述访问控制决策模块(22)。

[0054] 发起者可以是工业互联网中接入的企业节点、个人移动终端、工业APP等。发起者辅助性信息可以是发起者地址、发起者信用、发起者属性、发起者权限等。

[0055] 所述访问控制实施模块(21)够对请求格式进行标准形式的转换,采用基于属性的描述机制对访问请求进行统一描述,进行一致化处理获得决策请求。

[0056] 步骤二、所述访问控制决策模块(22)根据获取的所述决策请求为参数,向所述访问控制策略应答模块(23)发出策略查询请求;所述访问控制策略应答模块(23)检索适用策略后,向所述访问控制决策模块(22)返回包括访问控制策略的访问控制策略消息。

[0057] 所述访问控制策略应答模块(23)中存储的策略具体包括:所述发起者(1)设置的白名单和黑名单,以及访问目标(3)设置的白名单和黑名单。其中所述发起者(1)设置的白名单中存储发起者可以访问的访问目标(3),黑名单中存储发起者不能访问的访问目标(3)。当然所述发起者(1)设置的白名单和黑名单可以为空白项,对所述发起者就没有访问限制。所述访问目标(3)设置的白名单中存储可以访问所述访问目标(3)的名单,黑名单中存储不能访问所述访问目标(3)的名单。当然所述访问目标(3)设置的白名单和黑名单可以为空白项,对所述访问目标(3)就没有访问限制。黑白名单包括地址信息、产品信息等。

[0058] 步骤三、所述访问控制决策模块(22)对返回所述访问控制策略进行评估;当在评估过程中发现缺乏访问目标的属性时,向所述访问控制属性应答模块(24)发出属性查询请求。

[0059] 步骤四、所述访问控制属性应答模块(24)查询并验证属性发布点存储在本地数据库中的属性信息,如果本地数据库中存在访问目标属性信息,则生成包括访问控制属性的访问控制属性消息返回至所述访问控制决策模块(22)。

[0060] 当所述访问控制属性应答模块(24)查询的属性是外部安全域中的属性,则向外部安全域的外域访问控制属性应答模块(4)进行查询,以获得外部安全域中的访问控制属性,并通过属性映射关系确定属性的可信性,生成访问控制属性消息返回至所述访问控制决策模块(22)。

[0061] 所述访问目标的属性信息为主体标识、主体类型或名称、主体属性值、主体地域、主体制造商、主体使用商、主体属性信息摘要的签名。

[0062] 主体属性信息摘要=HASH256(a1 || a2 || a3) and HASH256(b1 || b2 || b3)；

其中HASH256为哈希256算法，a1为主体标识，a2为主体类型编码或名称编码，a3为主体属性值，b1为主体地域编码，b2为主体制造商编码，b3为主体使用商编码，||为连接符号。

[0063] 由于工业互联网设备的标签数据能够通过表示解析体系查询到设备的属性信息，因此所述访问控制属性应答模块(24)可以通过对比设备上报信息和通过标识解析体系获取的信息通过属性映射关系确定属性的可信性。

[0064] 步骤五、所述访问控制决策模块(22)依据所述访问控制策略与所述访问控制属性完成决策评估，向所述访问控制实施模块(21)发送最终决策结果。

[0065] 所述访问控制决策模块(22)进一步存储访问控制决策，用于实现访问决策逻辑执行功能。决策逻辑可以采用已有的多种访问控制模型和访问控制机制，尽可能提高其兼容性。所述访问控制决策模块(22)在多条策略同时给出明确决策结果，且决策结果存在冲突时指定冲突消解策略，以处理可能产生的决策结果不一致性，常用的消解策略包括：肯定判定优先、否定判定优先、首次判定优先等。

[0066] 访问控制决策应从宏观角度制定最基本的资源安全策略，以提供最低限度的安全保障。访问控制决策通过开放式策略和保守式策略实现这种可预知的和最低限度的安全保障。开放式策略的决策逻辑为：如果没有提供显式策略明确禁止某访问行为，则认为允许该类访问进行。保守式策略的决策逻辑为，如果没有提供显式策略明确允许某访问行为，则认为禁止该类访问进行。采用何种策略取决于具体应用的资源对象敏感性和资源对象使用目的。

[0067] 所述访问控制决策模块(22)依据所述访问控制策略与所述访问控制属性完成决策评估具体为：

S601，根据所述发起者(1)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3)；

S602，根据所述访问目标(3)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3)；

S603，根据所述访问控制属性确定所述访问目标(3)是否允许访问；

其中，在工业互联网中存在多种设备，包括主动标识载体和被动标识载体两类，其中被动标识载体无法被直接访问，因此通过设置所述访问控制属性可以防止所述发起者(1)浪费网络资源和功耗，发起无意义访问。并且通过设置所述访问控制属性可以所述访问控制决策模块(22)有效的验证所述访问目标(3)的真实性，以防止所述发起者(1)获得失真数据。所述访问目标(3)也可以通过所述访问控制属性提高设备的安全性，例如可以设置永久不被外部网络或者处于特定地理位置的设备访问。

[0068] S604，根据所述访问控制决策决定所述访问目标(3)是否允许访问。

[0069] 通过步骤S601至S603，可能得到所述发起者(1)即可以访问所述访问目标(3)的结果，也可能得到不能访问所述访问目标(3)的结果。这时，需要设置所述访问控制决策。如果没有提供显式策略明确禁止某访问行为，则认为允许该类访问进行。保守式策略的决策逻辑为，如果没有提供显式策略明确允许某访问行为，则认为禁止该类访问进行。采用何种策略取决于具体应用的资源对象敏感性和资源对象使用目的。

[0070] 所述访问控制决策模块(22)进一步可以依据所述发起者辅助性信息、所述访问控制策略与所述访问控制属性完成决策评估,向所述访问控制实施模块(21)发送最终决策结果。

[0071] 依据所述发起者辅助性信息、所述访问控制策略与所述访问控制属性完成决策评估具体为:

S701,根据所述发起者辅助性信息确定所述发起者(1)是否有权允许访问所述访问目标(3);

S702,根据所述发起者(1)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3);

S703,根据所述访问目标(3)设置的白名单和黑名单确定所述发起者(1)是否允许访问所述访问目标(3);

S704,根据所述访问控制属性确定所述访问目标(3)是否允许访问;

S705,根据所述访问控制决策决定所述访问目标(3)是否允许访问。

[0072] 步骤六、所述访问控制实施模块(21)根据返回的所述最终决策结果拒绝或允许发起者对目标的访问。

[0073] 示例性计算机程序产品和计算机可读存储介质:

除了上述方法和设备以外,本公开的实施例还可以是计算机程序产品,其包括计算机程序指令,所述计算机程序指令在被处理器运行时使得所述处理器执行本说明书上述“示例性方法”部分中描述的根据本公开各种实施例的用户行为特征分析方法或者基于用户行为特征的推荐方法中的步骤。

[0074] 所述计算机程序产品可以以一种或多种程序设计语言的任意组合来编写用于执行本公开实施例操作的程序代码,所述程序设计语言包括面向对象的程序设计语言,诸如Java、C++等,还包括常规的过程式程序设计语言,诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。

[0075] 此外,本公开的实施例还可以是计算机可读存储介质,其上存储有计算机程序指令,所述计算机程序指令在被处理器运行时使得所述处理器执行本说明书上述“示例性方法”部分中描述的根据本公开各种实施例的用户行为特征分析方法或者基于用户行为特征的推荐方法中的步骤。

[0076] 所述计算机可读存储介质可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以包括但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0077] 以上结合具体实施例描述了本公开的基本原理,但是,需要指出的是,在本公开中提及的优点、优势、效果等仅是示例而非限制,不能认为这些优点、优势、效果等是本公开的各个实施例必须具备的。另外,上述公开的具体细节仅是为了示例的作用和便于理解的作

用，而非限制，上述细节并不限制本公开为必须采用上述具体的细节来实现。

[0078] 本说明书中各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其它实施例的不同之处，各个实施例之间相同或相似的部分相互参见即可。对于系统实施例而言，由于其与方法实施例基本对应，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。

[0079] 本公开中涉及的器件、装置、设备、系统的方框图仅作为例示性的例子并且不意图要求或暗示必须按照方框图示出的方式进行连接、布置、配置。如本领域技术人员将认识到的，可以按任意方式连接、布置、配置这些器件、装置、设备、系统。诸如“包括”、“包含”、“具有”等等的词语是开放性词汇，指“包括但不限于”，且可与其互换使用。这里所使用的词汇“或”和“和”指词汇“和/或”，且可与其互换使用，除非上下文明确指示不是如此。这里所使用的词汇“诸如”指词组“诸如但不限于”，且可与其互换使用。

[0080] 可能以许多方式来实现本公开的方法和装置。例如，可通过软件、硬件、固件或者软件、硬件、固件的任何组合来实现本公开的方法和装置。用于所述方法的步骤的上述顺序仅是为了进行说明，本公开的方法的步骤不限于以上具体描述的顺序，除非以其它方式特别说明。此外，在一些实施例中，还可将本公开实施为记录在记录介质中的程序，这些程序包括用于实现根据本公开的方法的机器可读指令。因而，本公开还覆盖存储用于执行根据本公开的方法的程序的记录介质。

[0081] 还需要指出的是，在本公开的装置、设备和方法中，各部件或各步骤是可以分解和/或重新组合的。这些分解和/或重新组合应视为本公开的等效方案。

[0082] 提供所公开的方面的以上描述以使本领域的任何技术人员能够做出或者使用本公开。对这些方面的各种修改对于本领域技术人员而言是非常显而易见的，并且在此定义的一般原理可以应用于其他方面而不脱离本公开的范围。因此，本公开不意图被限制到在此示出的方面，而是按照与在此公开的原理和新颖的特征一致的最宽范围。

[0083] 为了例示和描述的目的已经给出了以上描述。此外，此描述不意图将本公开的实施例限制到在此公开的形式。尽管以上已经讨论了多个示例方面和实施例，但是本领域技术人员将认识到其某些变型、修改、改变、添加和子组合。本发明的描述是为了示例和描述起见而给出的，而并不是无遗漏的或者将本发明限于所公开的形式。很多修改和变化对于本领域的普通技术人员而言是显然的。选择和描述实施例是为了更好说明本发明的原理和实际应用，并且使本领域的普通技术人员能够理解本发明从而设计适于特定用途的带有各种修改的各种实施例。

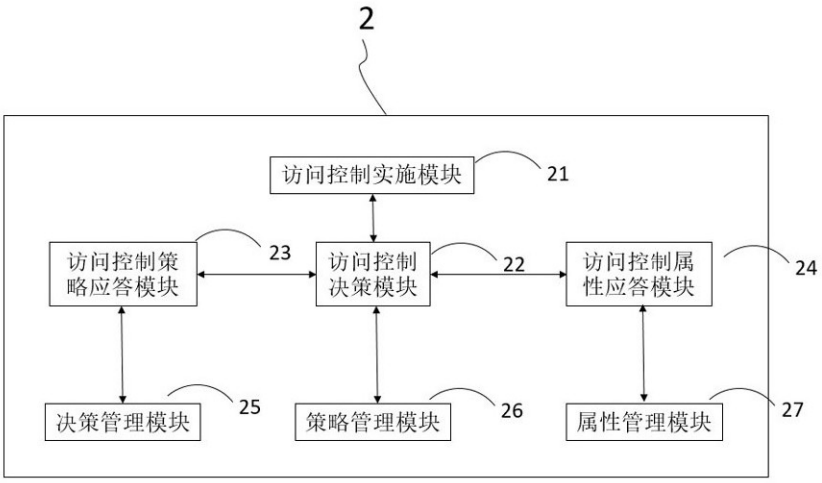

2
访问控制实施模块
21
访问控制策略应答模块
23
访问控制决策模块
22
访问控制属性应答模块
24
决策管理模块
25
策略管理模块
26
属性管理模块
27

图1

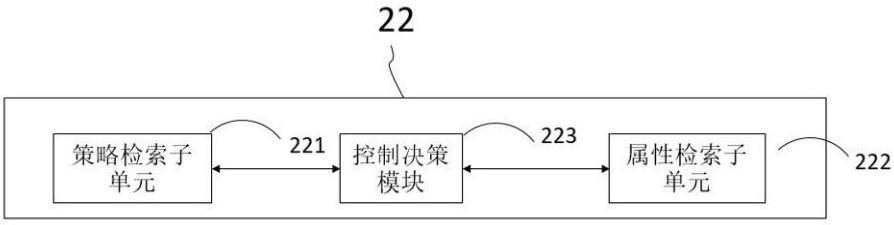

22
策略检索子单元
221
控制决策模块
223
属性检索子单元
222

图2

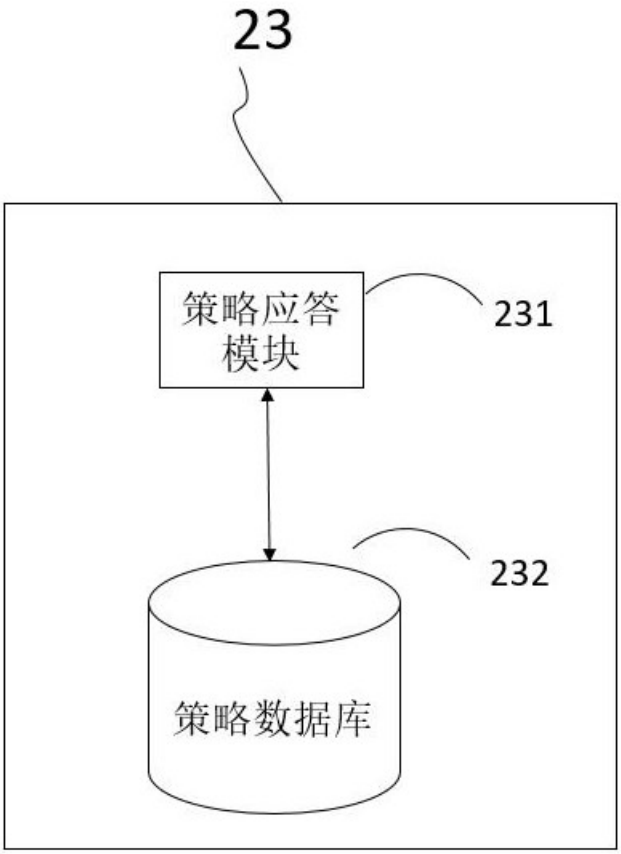


图3

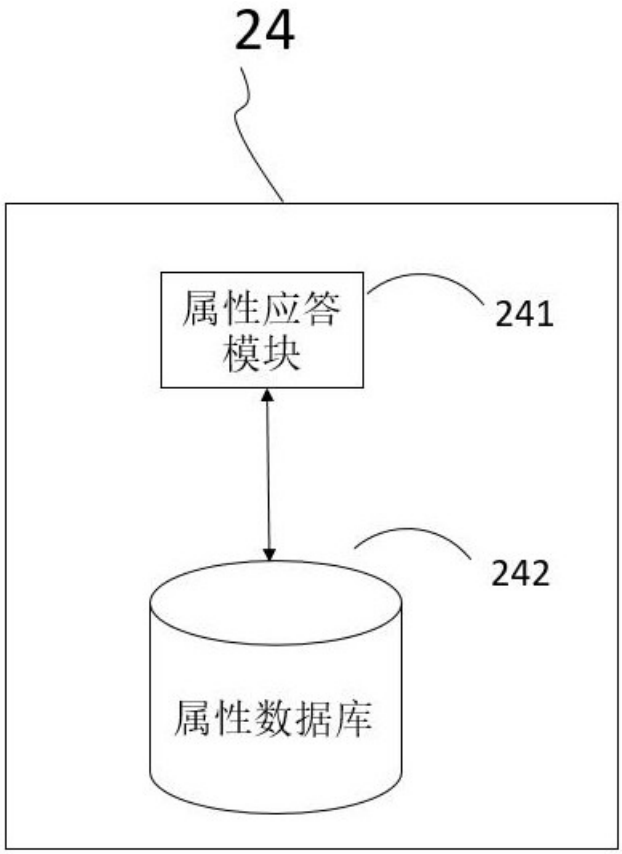

24
属性应答模块
241
242
属性数据库

图4

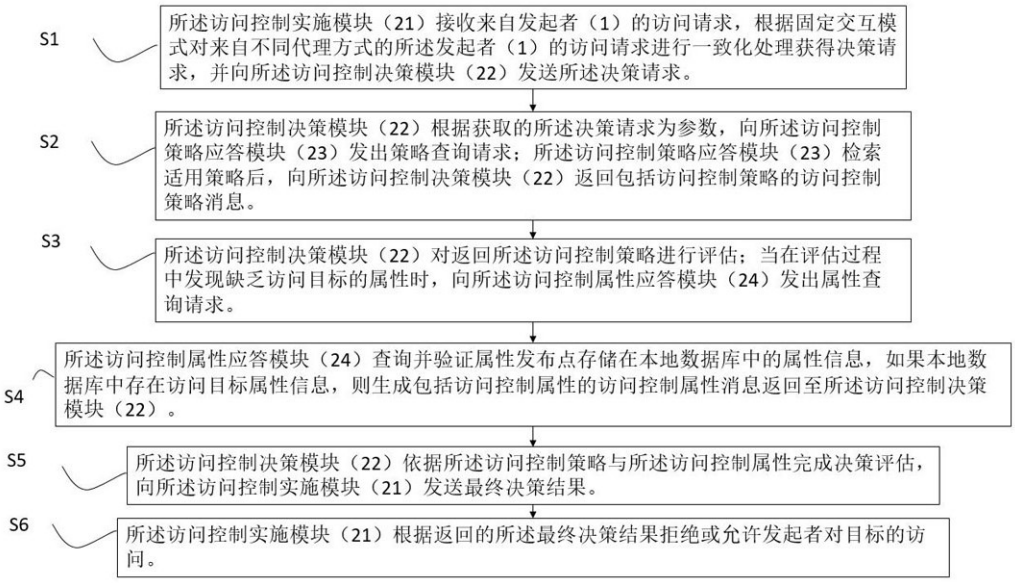

S1
所述访问控制实施模块（21）接收来自发起者（1）的访问请求，根据固定交互模式对来自不同代理方式的所述发起者（1）的访问请求进行一致化处理获得决策请求，并向所述访问控制决策模块（22）发送所述决策请求。
S2
所述访问控制决策模块（22）根据获取的所述决策请求为参数，向所述访问控制策略应答模块（23）发出策略查询请求；所述访问控制策略应答模块（23）检索适用策略后，向所述访问控制决策模块（22）返回包括访问控制策略的访问控制策略消息。
S3
所述访问控制决策模块（22）对返回所述访问控制策略进行评估；当在评估过程中发现缺乏访问目标的属性时，向所述访问控制属性应答模块（24）发出属性查询请求。
S4
所述访问控制属性应答模块（24）查询并验证属性发布点存储在本地数据库中的属性信息，如果本地数据库中存在访问目标属性信息，则生成包括访问控制属性的访问控制属性消息返回至所述访问控制决策模块（22）。
S5
所述访问控制决策模块（22）依据所述访问控制策略与所述访问控制属性完成决策评估，向所述访问控制实施模块（21）发送最终决策结果。
S6
所述访问控制实施模块（21）根据返回的所述最终决策结果拒绝或允许发起者对目标的访问。

图5