(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112217774 A
(43)申请公布日 2021.01.12

(21)申请号 201910626751.7

(22)申请日 2019.07.11

(71)申请人 中移(苏州)软件技术有限公司
地址 215163 江苏省苏州市高新区昆仑山路58号1幢
申请人 中国移动通信集团有限公司

(72)发明人 段朦 李杰亮 孙道

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 王姗姗 张颖玲

(51)Int.Cl.
H04L 29/06(2006.01)

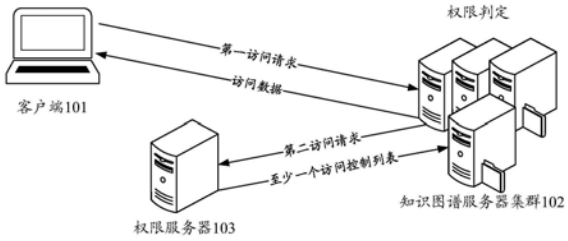
权利要求书5页 说明书19页 附图11页

(54)发明名称

一种权限控制系统及方法、服务器、存储介质

(57)摘要

本公开实施例公开了一种权限控制系统及方法、服务器、存储介质，权限控制系统包括：客户端获取用户组信息，将携带有用户组信息的第一访问请求发送给知识图谱服务器集群；知识图谱服务器集群根据响应第一访问请求获取的用户组信息生成第二访问请求，并发送给权限服务器；权限服务器根据响应第二访问请求获取的用户组信息和预设权限三元映射关系，获取与用户组信息对应的至少一个访问控制列表，并发送给知识图谱服务器集群；知识图谱服务器集群根据至少一个访问控制列表，获取访问数据，并发送访问数据给客户端，能够以知识图谱数据对象的属性为粒度实现权限控制，解决了权限控制方式单一和精度低的问题，提高了权限控制的灵活性和精度。



CN 112217774 A

1.一种权限控制系统,其特征在于,所述系统包括:客户端、权限服务器和知识图谱服务器集群,其中,

所述客户端,用于获取用户组信息,将所述用户组信息携带在第一访问请求中,并发送所述第一访问请求给所述知识图谱服务器集群,所述第一访问请求用于向所述知识图谱服务器集群请求访问数据;

所述知识图谱服务器集群,用于响应所述第一访问请求,获取所述用户组信息,根据所述用户组信息生成第二访问请求,并发送所述第二访问请求给所述权限服务器,所述第二访问请求用于向所述权限服务器请求访问权限;

所述权限服务器,用于响应所述第二访问请求,获取所述用户组信息,根据所述用户组信息和预设权限三元映射关系,获取与所述用户组信息对应的至少一个访问控制列表,并将所述至少一个访问控制列表发送给所述知识图谱服务器集群,所述至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的所述访问权限,所述预设权限三元映射关系用于表征所述用户组信息、数据源信息和所述访问控制列表之间的映射关系;

所述知识图谱服务器集群,还用于根据所述至少一个访问控制列表,获取所述访问数据,并将所述访问数据发送给所述客户端。

2.根据权利要求1所述的系统,其特征在于,所述系统还包括轻量目录访问协议LDAP服务器,

所述客户端,还用于在发送所述第一访问请求给所述知识图谱服务器集群之前,发送第三访问请求给所述LDAP服务器,所述第三访问请求中携带有用户标识,所述第三访问请求用于向所述LDAP服务器请求所述用户组信息;

所述LDAP服务器,用于响应所述第三访问请求,获取所述用户标识,根据所述用户标识,以及预设用户标识与用户组信息的对应关系,获取与所述用户标识对应的所述用户组信息;并发送所述用户组信息给所述客户端。

3.根据权利要求1所述的系统,其特征在于,所述预设权限三元映射关系包括:预设用户组信息与数据源信息的对应关系、预设数据源信息与访问控制列表的对应关系;

所述权限服务器,具体用于响应所述第二访问请求,获取所述用户组信息,根据所述用户组信息,以及预设用户组信息与数据源信息的对应关系,确定与所述用户组信息对应的数据源信息;根据所述数据源信息,以及预设数据源信息与访问控制列表的对应关系,确定与所述用户组信息对应的至少一个访问控制列表,并将所述至少一个访问控制列表发送给所述知识图谱服务器集群。

4.根据权利要求1所述的系统,其特征在于,

所述知识图谱服务器集群,具体用于从所述至少一个访问控制列表中,获取所述用户组信息的访问策略;通过所述访问策略访问预存的知识图谱数据,获取所述访问数据,并发送所述访问数据给所述客户端。

5.根据权利要求4所述的系统,其特征在于,所述知识图谱服务器集群包括中心服务器、主服务器和从服务器;

知识图谱服务器集群,还具体用于通过所述中心服务器确定执行所述访问策略的服务器,当执行所述访问策略的服务器为所述主服务器时,检测所述主服务器是否处于异常状态,当所述主服务器处于异常状态时,根据预设选举规则,从所述知识图谱服务器集群中选

取一个从服务器，并发送所述访问策略给所述从服务器；通过所述从服务器执行所述访问策略访问预设的知识图谱数据，获取所述访问数据。

6.根据权利要求1至5任一项所述的系统，其特征在于，

所述至少一个访问控制列表包括读权限、写权限、读权限和请求读权限、写权限和删除权限以及系统管理员权限，所述请求读权限用于表征只能得到请求数据的获取方式。

7.根据权利要求2所述的系统，其特征在于，所述LDAP服务器，还用于在所述根据所述用户标识，以及预设用户标识与用户组信息的对应关系，获取与所述用户标识对应的所述用户组信息之后，发送更新请求给所述权限服务器，所述更新请求携带有更新的用户组信息；

所述权限服务器，还用于根据所述更新的用户组信息，更新所述预设权限三元映射关系。

8.一种权限控制方法，其特征在于，所述权限控制方法应用于知识图谱服务器集群的中心服务器，所述方法包括：

接收客户端发送的第一访问请求，所述第一访问请求携带有用户组信息；

响应所述第一访问请求，根据所述用户组信息生成第二访问请求；

发送所述第二访问请求给权限服务器，所述第二访问请求用于向所述权限服务器请求访问权限；

接收所述权限服务器响应所述第二访问请求返回的至少一个访问控制列表，所述至少一个访问控制列表为与所述用户组信息中的至少一个用户组信息对应；

根据所述至少一个访问控制列表，获取访问数据；

发送所述访问数据给所述客户端。

9.根据权利要求8所述的方法，其特征在于，所述根据所述至少一个访问控制列表，获取访问数据，包括：

根据所述至少一个访问控制列表，确定执行所述访问策略的服务器；

基于所述执行所述访问策略的服务器，获取所述访问数据。

10.根据权利要求9所述的方法，其特征在于，所述基于所述执行所述访问策略的服务器，获取所述访问数据，包括：

当执行所述访问策略的服务器为所述知识图谱服务器集群中的主服务器时，发送所述访问策略给所述主服务器；

接收所述主服务器响应所述访问策略返回的所述访问数据。

11.根据权利要求9所述的方法，其特征在于，所述基于所述执行所述访问策略的服务器，获取所述访问数据，包括：

当执行所述访问策略的服务器为所述知识图谱服务器集群中的从服务器时，发送所述访问策略给所述从服务器；

接收所述从服务器响应所述访问策略返回的所述访问数据。

12.根据权利要求10所述的方法，其特征在于，所述当执行所述访问策略的服务器为知识图谱服务器集群中的主服务器时，发送所述访问策略给所述主服务器，包括：

当所述执行访问策略的服务器为所述知识图谱服务器集群中的所述主服务器时，检测所述主服务器是否处于异常状态；

当所述主服务器处于异常状态时，根据预设选举规则，从所述知识图谱服务器集群中选取一个从服务器，发送所述访问策略给所述从服务器；

对应地，所述接收所述主服务器响应所述访问策略返回的所述访问数据，包括：

接收所述从服务器响应所述访问策略返回的所述访问数据。

13.一种权限控制方法，其特征在于，所述权限控制方法应用于知识图谱服务器集群的主服务器，所述方法包括：

接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读写访问权限；

根据所述访问策略访问预存的知识图谱数据，获取访问数据；

将所述访问数据发送给所述中心服务器。

14.一种权限控制方法，其特征在于，所述权限控制方法应用于知识图谱服务器集群的从服务器，所述方法包括：

接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读访问权限；

根据所述访问策略访问预存的知识图谱数据，获取访问数据；

将所述访问数据发送给所述中心服务器。

15.一种权限控制方法，其特征在于，所述权限控制方法应用于权限服务器，所述方法包括：

接收中心服务器发送的第二访问请求，所述第二访问请求携带有用户组信息；

根据所述用户组信息和预设权限三元映射关系，获取与所述用户组信息对应的至少一个访问控制列表，所述至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的所述访问权限，所述预设权限三元映射关系用于表征所述用户组信息、数据源信息和所述访问控制列表之间的映射关系；

将所述至少一个访问控制列表发送给所述中心服务器。

16.根据权利要求15所述的方法，其特征在于，所述预设权限三元映射关系包括：预设用户组信息与数据源信息的对应关系、预设数据源信息与访问控制列表的对应关系；所述根据所述用户组信息和预设权限三元映射关系，获取与所述用户组信息对应的至少一个访问控制列表，包括：

根据所述用户组信息，以及预设用户组信息与数据源信息的对应关系，确定与所述用户组信息对应的数据源信息；

根据所述数据源信息，以及预设数据源信息与访问控制列表的对应关系，获取与所述用户组信息对应的至少一个访问控制列表。

17.根据权利要求15所述的方法，其特征在于，在所述将所述至少一个访问控制列表发送给所述中心服务器之后，所述方法还包括：

接收LDAP服务器发送的更新请求，所述更新请求携带有更新的用户组信息；

根据所述更新的用户组信息，更新所述预设权限三元映射关系。

18.一种知识图谱服务器集群的中心服务器，其特征在于，所述知识图谱服务器集群的中心服务器包括第一接收单元、第一获取单元、第一发送单元、第二接收单元、第二获取单元和第二发送单元，其中，

所述第一接收单元，用于接收客户端发送的第一访问请求，所述第一访问请求携带有用户组信息；

所述第一获取单元，用于响应所述第一访问请求，根据所述用户组信息生成第二访问请求；

所述第一发送单元，用于发送第二访问请求给权限服务器，所述第二访问请求用于向所述权限服务器请求访问权限；

所述第二接收单元，用于接收所述权限服务器响应所述第二访问请求返回的至少一个访问控制列表，所述至少一个访问控制列表为与所述用户组信息中的至少一个用户组信息对应；

所述第二获取单元，用于根据所述至少一个访问控制列表，获取所述访问数据；

所述第二发送单元，用于发送所述访问数据给所述客户端。

19.一种知识图谱服务器集群的主服务器，其特征在于，所述主服务器包括第三接收单元、第三获取单元、第三发送单元，其中，

所述第三接收单元，用于接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读写访问权限；

所述第三获取单元，用于根据所述访问策略访问预存的知识图谱数据，获取访问数据；

所述第三发送单元，用于将所述访问数据发送给所述中心服务器。

20.一种知识图谱服务器集群的从服务器，其特征在于，所述从服务器包括第四接收单元、第四获取单元、第四发送单元，其中，

所述第四接收单元，用于接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读访问权限；

所述第四获取单元，用于根据所述访问策略访问预存的知识图谱数据，获取访问数据；

所述第四发送单元，用于将所述访问数据发送给所述中心服务器。

21.一种权限服务器，其特征在于，所述权限服务器包括第五接收单元、第五获取单元和第五发送单元，其中，

所述第五接收单元，用于接收中心服务器发送的第二访问请求，所述第二访问请求携带有用户组信息；

所述第五获取单元，用于根据所述用户组信息和预设权限三元映射关系，获取与所述用户组信息对应的至少一个访问控制列表，所述至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的所述访问权限，所述预设权限映射关系用于表征所述用户组信息、数据源信息和所述访问控制列表之间的映射关系；

所述第五发送单元，用于将所述至少一个访问控制列表发送给所述中心服务器。

22.一种知识图谱服务器集群的中心服务器，其特征在于，所述中心服务器至少包括第一处理器、第一通信总线、第一存储器及第一通信接口，其中，所述第一通信总线用于实现所述第一处理器、所述第一通信接口和所述第一存储器之间的连接通信；所述第一通信接口用于获取用户组信息；所述第一处理器用于执行所述第一存储器中存储的可执行指令，当所述可执行指令被执行时，所述第一处理器执行时实现如权利要求8至12任一项所述的方法。

23.一种知识图谱服务器集群的主服务器，其特征在于，所述主服务器至少包括第二处

理器、第二通信总线、第二存储器及第二通信接口，其中，所述第二通信总线用于实现所述第二处理器、所述第二通信接口和所述第二存储器之间的连接通信；所述第二通信接口用于获取访问控制策略；所述第二处理器用于执行所述第二存储器中存储的可执行指令，当所述可执行指令被执行时，所述第二处理器执行时实现如权利要求13所述的方法。

24.一种知识图谱服务器集群的从服务器，其特征在于，所述从服务器至少包括第三处理器、第三通信总线、第三存储器及第三通信接口，其中，所述第三通信总线用于实现所述第三处理器、所述第三通信接口和所述第三存储器之间的连接通信；所述第三通信接口用于获取访问控制策略；所述第三处理器用于执行所述第三存储器中存储的可执行指令，当所述可执行指令被执行时，所述第三处理器执行时实现如权利要求14所述的方法。

25.一种权限服务器，其特征在于，所述权限服务器至少包括第四处理器、第四通信总线、第四存储器及第四通信接口，其中，所述第四通信总线用于实现所述第四处理器、所述第四通信接口和所述第四存储器之间的连接通信；所述第四通信接口用于获取第二访问请求；所述第四处理器用于执行所述第四存储器中存储的可执行指令，当所述可执行指令被执行时，所述第四处理器执行时实现如权利要求15至17任一项所述的方法。

26.一种计算机可读存储介质，其上存储有可执行指令，其特征在于，所述可执行指令被第一处理器执行时实现如权利要求8至12任一项所述的方法；或者所述可执行指令被第二处理器执行时实现如权利要求13所述的方法；或者所述可执行指令被第三处理器执行时实现如权利要求14所述的方法；或者所述可执行指令被第四处理器执行时实现如权利要求15至17任一项所述的方法。

一种权限控制系统及方法、服务器、存储介质

技术领域

[0001] 本公开实施例涉及互联网信息处理领域，尤其涉及一种权限控制系统及方法、服务器、存储介质。

背景技术

[0002] 知识图谱是描述现实世界中的一切事和物以及他们之间关系的知识库。由于知识图谱数据量巨大且数据源来源众多，不同的实体信息由多个数据源获取得到，用户获取某个实体时需要访问不同数据源。

[0003] 目前，知识图谱数据的权限控制方式包括本机授权的方式和通过LDAP服务器进行角色保存的方式。然而，现有的权限控制方式以整个知识图谱中数据对象为粒度进行访问控制，存在权限控制方式单一和权限控制精度低的问题。

发明内容

[0004] 为解决上述技术问题，本公开实施例期望提供一种权限控制系统及方法、服务器、存储介质，能够以知识图谱数据对象的属性为粒度实现权限控制，提高了权限控制的灵活性和精度。

[0005] 本公开实施例的技术方案是这样实现的：

[0006] 第一方面，本公开实施例提供一种权限控制系统，所述系统包括：客户端、权限服务器和知识图谱服务器集群，其中，

[0007] 所述客户端，用于获取用户组信息，将所述用户组信息携带在第一访问请求中，并发送所述第一访问请求给所述知识图谱服务器集群，所述第一访问请求用于向所述知识图谱服务器集群请求访问数据；

[0008] 所述知识图谱服务器集群，用于响应所述第一访问请求，获取所述用户组信息，根据所述用户组信息生成第二访问请求，并发送所述第二访问请求给所述权限服务器，所述第二访问请求用于向所述权限服务器请求访问权限；

[0009] 所述权限服务器，用于响应所述第二访问请求，获取所述用户组信息，根据所述用户组信息和预设权限三元映射关系，获取与所述用户组信息对应的至少一个访问控制列表，并将所述至少一个访问控制列表发送给所述知识图谱服务器集群，所述至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的所述访问权限，所述预设权限三元映射关系用于表征所述用户组信息、数据源信息和所述访问控制列表之间的映射关系；

[0010] 所述知识图谱服务器集群，还用于根据所述至少一个访问控制列表，获取所述用户的访问数据，并将所述访问数据发送给所述客户端。

[0011] 第二方面，本公开实施例提供一种权限控制方法，应用于知识图谱服务器集群的中心服务器，所述方法包括：

[0012] 接收客户端发送的第一访问请求，所述第一访问请求携带有用户组信息；

[0013] 响应所述第一访问请求，根据所述用户组信息生成第二访问请求；

[0014] 发送所述第二访问请求给权限服务器，所述第二访问请求用于向所述权限服务器请求访问权限；

[0015] 接收所述权限服务器响应所述第二访问请求返回的至少一个访问控制列表，所述至少一个访问控制列表为与所述用户组信息中的至少一个用户组信息对应；

[0016] 根据所述至少一个访问控制列表，获取所述用户的访问数据；

[0017] 发送所述访问数据给所述客户端。

[0018] 第三方面，本公开实施例提供一种权限控制方法，应用于知识图谱服务器集群的主服务器，所述方法包括：

[0019] 接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读写访问权限；

[0020] 根据所述访问策略访问预存的知识图谱数据，获取访问数据；

[0021] 将所述访问数据发送给所述中心服务器。

[0022] 第四方面，本公开实施例提供一种权限控制方法，所述权限控制方法应用于知识图谱服务器集群的从服务器，所述方法包括：

[0023] 接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读访问权限；

[0024] 根据所述访问策略访问预存的知识图谱数据，获取访问数据；

[0025] 将所述访问数据发送给所述中心服务器。

[0026] 第五方面，本公开实施例提供一种权限控制方法，应用于权限服务器，所述方法包括：

[0027] 接收中心服务器发送的第二访问请求，所述第二访问请求携带有用户组信息；

[0028] 根据所述用户组信息和预设权限三元映射关系，获取与所述用户组信息对应的至少一个访问控制列表，所述至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的所述访问权限，所述预设权限三元映射关系用于表征所述用户组信息、数据源信息和所述访问控制列表之间的映射关系；

[0029] 将所述至少一个访问控制列表发送给所述中心服务器。

[0030] 第六方面，本公开实施例提供一种知识图谱服务器集群的中心服务器，所述知识图谱服务器集群的中心服务器包括第一接收单元、第一获取单元、第一发送单元、第二接收单元、第二获取单元和第二发送单元，其中，

[0031] 所述第一接收单元，用于接收客户端发送的第一访问请求，所述第一访问请求携带有用户组信息；

[0032] 所述第一获取单元，用于响应所述第一访问请求，根据所述用户组信息生成第二访问请求；

[0033] 所述第一发送单元，用于发送第二访问请求给权限服务器，所述第二访问请求用于向所述权限服务器请求访问权限；

[0034] 所述第二接收单元，用于接收所述权限服务器响应所述第二访问请求返回的至少一个访问控制列表，所述至少一个访问控制列表为与所述用户组信息中的至少一个用户组信息对应；

[0035] 所述第二获取单元，用于根据所述至少一个访问控制列表，获取所述访问数据；

[0036] 所述第二发送单元，用于发送所述访问数据给所述客户端。

[0037] 第七方面，本公开实施例提供一种知识图谱服务器集群的主服务器，所述中心服务器包括第三接收单元、第三获取单元、第三发送单元，其中，

[0038] 所述第三接收单元，用于接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读写访问权限；

[0039] 所述第三获取单元，用于根据所述访问策略访问预存的知识图谱数据，获取访问数据；

[0040] 所述第三发送单元，用于将所述访问数据发送给所述中心服务器。

[0041] 第八方面，本公开实施例提供一种知识图谱服务器集群的从服务器，所述从服务器包括第四接收单元、第四获取单元、第四发送单元，其中，

[0042] 所述第四接收单元，用于接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读访问权限；

[0043] 所述第四获取单元，用于根据所述访问策略访问预存的知识图谱数据，获取访问数据；

[0044] 所述第四发送单元，用于将所述访问数据发送给所述中心服务器。

[0045] 第九方面，本公开实施例提供一种权限服务器，所述权限服务器包括第五接收单元、第五获取单元和第五发送单元，其中，

[0046] 所述第五接收单元，用于接收中心服务器发送的第二访问请求，所述第二访问请求携带有用户组信息；

[0047] 所述第五获取单元，用于根据所述用户组信息和预设权限三元映射关系，获取与所述用户组信息对应的至少一个访问控制列表，所述至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的所述访问权限，所述预设权限映射关系用于表征所述用户组信息、数据源信息和所述访问控制列表之间的映射关系；

[0048] 所述第五发送单元，用于将所述至少一个访问控制列表发送给所述中心服务器。

[0049] 第十方面，本公开实施例提供一种知识图谱服务器集群的中心服务器，所述中心服务器至少包括第一处理器、第一通信总线、第一存储器及第一通信接口，其中，所述第一通信总线用于实现所述第一处理器、所述第一通信接口和所述第一存储器之间的连接通信；所述第一通信接口用于获取用户组信息；所述第一处理器用于执行所述第一存储器中存储的可执行指令，当所述可执行指令被执行时，所述第一处理器执行时实现上述实施例提供的权限控制方法。

[0050] 第十一方面，本公开实施例提供一种知识图谱服务器集群的主服务器，所述主服务器至少包括第二处理器、第二通信总线、第二存储器及第二通信接口，其中，所述第二通信总线用于实现所述第二处理器、所述第二通信接口和所述第二存储器之间的连接通信；所述第二通信接口用于获取访问控制策略；所述第二处理器用于执行所述第二存储器中存储的可执行指令，当所述可执行指令被执行时，所述第二处理器执行时实现上述实施例提供的权限控制方法。

[0051] 第十二方面，本公开实施例提供一种知识图谱服务器集群的从服务器，所述从服务器至少包括第三处理器、第三通信总线、第三存储器及第三通信接口，其中，所述第三通信总线用于实现所述第三处理器、所述第三通信接口和所述第三存储器之间的连接通信；

所述第三通信接口用于获取访问控制策略;所述第三处理器用于执行所述第三存储器中存储的可执行指令,当所述可执行指令被执行时,所述第三处理器执行时实现上述实施例提供的权限控制方法。

[0052] 第十三方面,本公开实施例提供一种权限服务器,所述权限服务器至少包括第四处理器、第四通信总线、第四存储器及第四通信接口,其中,所述第四通信总线用于实现所述第四处理器、所述第四通信接口和所述第四存储器之间的连接通信;所述第四通信接口用于获取第二访问请求;所述第四处理器用于执行所述第四存储器中存储的可执行指令,当所述可执行指令被执行时,所述第四处理器执行时实现上述实施例提供的权限控制方法。

[0053] 第十四方面,本公开实施例提供一种计算机可读存储介质,其上存储有可执行指令,所述可执行指令被第一处理器、第二处理器、第三处理器或者第四处理器执行时实现上述实施例提供的权限控制方法。

[0054] 本公开实施例提供了一种权限控制系统及方法、服务器、存储介质,权限控制系统包括:客户端、权限服务器和知识图谱服务器集群,其中,客户端,用于获取用户组信息,将用户组信息携带在第一访问请求中,并发送第一访问请求给知识图谱服务器集群,第一访问请求用于向知识图谱服务器集群请求访问数据;知识图谱服务器集群,用于响应第一访问请求,获取用户组信息,根据用户组信息生成第二访问请求,并发送第二访问请求给权限服务器,第二访问请求用于向权限服务器请求访问权限;权限服务器,用于响应第二访问请求,获取用户组信息,根据用户组信息和预设权限三元映射关系,获取与用户组信息对应的至少一个访问控制列表,并将至少一个访问控制列表发送给知识图谱服务器集群,至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的访问权限,预设权限三元映射关系用于表征用户组信息、数据源信息和访问控制列表之间的映射关系;知识图谱服务器集群,还用于根据至少一个访问控制列表,获取访问数据,并将访问数据发送给客户端。也就是说,本公开实施例中权限服务器存储的是用户组信息、数据源信息和访问控制列表之间的映射关系,访问控制列表为知识图谱数据对象的属性对应的访问权限,通过用户组信息和该权限三元映射关系便可以得到用户组对应的知识图谱数据对象的属性的访问权限,如此,能够以知识图谱数据对象的属性为粒度实现对用户的权限控制,提高了权限控制的灵活性和精度。

附图说明

[0055] 图1为本公开实施例提供的一种权限控制系统结构示意图一;

[0056] 图2为本公开实施例提供的一种权限控制系统结构示意图二;

[0057] 图3为本公开实施例提供的一种权限控制系统结构示意图三;

[0058] 图4为本公开实施例提供的权限控制方法的流程示意图一;

[0059] 图5为本公开实施例提供的权限控制方法的流程示意图二;

[0060] 图6为本公开实施例提供的权限控制方法的流程示意图三;

[0061] 图7为本公开实施例提供的权限控制方法的流程示意图四;

[0062] 图8为本公开实施例提供的权限控制方法的流程示意图五;

[0063] 图9为本公开实施例提供的权限控制方法的流程示意图六;

[0064] 图10为本公开实施例提供的一种权限控制方法的交互示意图；

[0065] 图11为本公开实施例提供的知识图谱服务器集群的中心服务器的组成结构示意图一；

[0066] 图12为本公开实施例提供的知识图谱服务器集群的主服务器的组成结构示意图一；

[0067] 图13为本公开实施例提供的知识图谱服务器集群的从服务器的组成结构示意图一；

[0068] 图14为本公开实施例提供的权限服务器的组成结构示意图一；

[0069] 图15为本公开实施例提供的客户端的组成结构示意图一；

[0070] 图16为本公开实施例提供的LDAP服务器的组成结构示意图一；

[0071] 图17为本公开实施例提供的知识图谱服务器集群的中心服务器的组成结构示意图二；

[0072] 图18为本公开实施例提供的知识图谱服务器集群的主服务器的组成结构示意图二；

[0073] 图19为本公开实施例提供的知识图谱服务器集群的从服务器的组成结构示意图二；

[0074] 图20为本公开实施例提供的权限服务器的组成结构示意图二；

[0075] 图21为本公开实施例提供的客户端的组成结构示意图二；

[0076] 图22为本公开实施例提供的LDAP服务器的组成结构示意图二。

具体实施方式

[0077] 下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述。

[0078] 知识图谱数据存储在知识图谱服务器集群的图数据库中，图数据库可以为Neo4j，在图数据库Neo4j的属性图中，图是由顶点(Vertex)，边(Edge)和属性(Property)组成的，顶点和边都可以设置属性，顶点也称作节点，边也称作关系，每个节点和关系都可以由一个或多个属性。图数据库Neo4j创建的图是用顶点和边构建一个有向图，其查询语言为cypher。

[0079] 通常，图数据库Neo4j的权限控制方式有两种，一种是本机授权方式，在图数据库Neo4j所在的服务器磁盘上存储用户和用户角色信息，用户角色信息可以分为读者、发表者、创造者和管理员，通过管理员可以给其他用户分配角色，用户根据自己的角色向图数据库Neo4j发出数据请求进行访问控制。另一种是通过轻量目录访问协议(Lightweight Directory Access Protocol，LDAP)服务器的方式保存用户和角色，用户在客户端请求访问数据时首先要访问LDAP服务器获取用户角色，再通过图数据库Neo4j对过程赋予权限进行子图的访问控制，其中，该过程指用户的代码或打包成的jar包，如可以通过用户代码dbms.security.procedures.roles＝apoc.convert.*:reader表示具有读角色的用户都可以对apoc.convert.*命名空间下的过程进行读操作。

[0080] 然而，在本机授权方式中，通过本机磁盘保存的角色进行权限控制无法在多集群服务器中应用，只能通过手动复制角色信息到其他集群服务器上，并且权限控制粒度控制

为整个知识图谱服务器，不符合公共安全领域的知识图谱的要求；在LDAP服务器的方式保存角色中，权限控制以过程为粒度，无法满足知识图谱大量不同数据源之间的数据杂乱组合的要求，并且也无法满足机密性的访问控制需求。

[0081] 由此可以看出，基于角色的知识图谱权限控制方式只能对单一的数据进行权限控制，同时权限控制精度也比较低，因此，本公开实施例提出了一种权限控制系统，通过用户组信息，以及用户组信息、数据源信息和访问控制列表之间的映射关系，查找不同用户组信息的访问权限，能够以用户组对应的知识图谱数据对象的属性为粒度实现对用户的权限控制，提高了权限控制的灵活性和精度。

[0082] 本公开实施例提供一种权限控制系统，图1为本公开实施例提供的一种权限控制系统的结构示意图一，如图1所示，权限控制系统包括：客户端101、知识图谱服务器集群102和权限服务器103，客户端101与知识图谱服务器集群102进行通信；知识图谱服务器集群102分别与客户端101和权限服务器103进行通信，其中，

[0083] 客户端101，用于获取用户组信息，将用户组信息携带在第一访问请求中，并发送第一访问请求给知识图谱服务器集群102，第一访问请求用于向知识图谱服务器集群102请求访问数据；

[0084] 知识图谱服务器集群102，用于响应第一访问请求，获取用户组信息，根据用户组信息生成第二访问请求，并发送第二访问请求给权限服务器103，第二访问请求用于向权限服务器103请求访问权限；

[0085] 权限服务器103，用于响应第二访问请求，获取用户组信息，根据用户组信息和预设权限三元映射关系，获取与用户组信息对应的至少一个访问控制列表，并将至少一个访问控制列表发送给知识图谱服务器集群102，至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的访问权限，预设权限三元映射关系用于表征用户组信息、数据源信息和访问控制列表之间的映射关系；

[0086] 知识图谱服务器集群102，还用于根据至少一个访问控制列表，获取用户的访问数据，并将访问数据发送给客户端101。

[0087] 本公开实施例中，客户端101在进行访问知识图谱服务器集群102时，需要先获取用户组信息，然后将用户组信息携带在第一访问请求中，发送第一访问请求给知识图谱服务器集群102。

[0088] 需要说明的是，第一访问请求用于向知识图谱服务器集群102请求访问数据，一个用户可以对应一个或多个用户组，一个用户组信息是相同知识图谱数据对象属性的访问权限集合，每个用户组对应不同的知识图谱数据对象属性的访问权限。

[0089] 示例性地，用户组A对应居民基础信息的访问权限，用户组B对应居民身份信息的访问权限，用户a可以对应用户组A，也可以同时对应用户组A和用户组B，本公开实施例这里不作限制。

[0090] 本公开实施例中，在客户端101发送第一访问请求给知识图谱服务器集群102之后，知识图谱服务器集群102响应该第一访问请求，获取用户组信息，根据该用户组信息生成第二访问请求，并发送该第二访问请求给权限服务器103，其中，第二访问请求用于向权限服务器103请求访问权限。

[0091] 需要说明的是，知识图谱服务器集群102用于存储知识图谱数据，该知识图谱数据

包括实体、实体属性以及实体与实体属性之间的关系。

[0092] 示例性地，知识图谱服务器集群102中的知识图谱数据可以用三元组的形式进行保存，如公式(1)：

[0093] G＝(E,R,S) (1)

[0094] 其中，G为三元组形式存储的知识图谱数据，E为实体，S为属性、R为实体与属性之间的关系。

[0095] 本公开实施例中，知识图谱服务器集群102存储的知识图谱数据可以采用不同的数据源，以使得其数据库中的知识图谱数据更加丰富和全面。

[0096] 示例性地，数据源可以包括公安数据源、移动运营商数据、个人数据和公共网络数据，本公开实施例这里不作限制。

[0097] 本公开实施例中，在知识图谱服务器集群102发送第二访问请求给权限服务器103之后，权限服务器103响应第二访问请求，获取用户组信息，根据用户组信息和预设权限三元映射关系，获取与用户组信息对应的至少一个访问控制列表，并将至少一个访问控制列表发送给知识图谱服务器集群102。

[0098] 需要说明的是，权限服务器103用于存储知识图谱中所有数据的访问权限，该访问权限以权限三元映射关系存储在权限服务器103，其中，该权限三元映射关系用于表征用户组信息、数据源信息和访问控制列表之间的映射关系。

[0099] 本公开实施例中，在权限服务器103根据用户组信息和预设权限三元映射关系，获取与用户组信息对应的至少一个访问控制列表的过程中，权限服务器103根据用户组信息，以及预设用户组信息与数据源信息的对应关系，确定与用户组信息对应的数据源信息；根据数据源信息，以及预设数据源信息与访问控制列表的对应关系，确定与用户组信息对应的至少一个访问控制列表。

[0100] 需要说明的是，预设权限三元映射关系中的三元包括：用户组信息、数据源信息和访问控制列表；权限三元映射关系包括用户组信息与数据源信息的对应关系、预设数据源信息与访问控制列表的对应关系。

[0101] 可以理解的是，权限服务器103中的用户组信息都会绑定对应的数据源信息，且每个数据源都对应着访问控制列表，又访问控制列表用于表征知识图谱数据对象的属性对应的访问权限，也就是说，每一个用户组信息都对应一种知识图谱数据对象的属性的访问权限，通过一个用户可以对应一个或多个用户组，即可得到该用户对应的不同知识图谱数据对象的属性的访问权限，如此，实现了以知识图谱数据对象的属性为粒度进行访问控制，使得访问控制粒度更细，精度更高。

[0102] 本公开实施例中，至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的访问权限，该至少一个访问控制列表可以包括：读权限、写权限、读权限和请求读权限、写权限和删除权限以及系统管理员权限。

[0103] 需要说明的是，读权限用于表征用户对知识图谱数据只能执行读操作；写权限用于表征用户可以向知识图谱数据库中插入数据；写权限和删除权限用于表征用户既可以向知识图谱数据库中插入数据，还可以删除知识图谱数据库中的数据；系统管理员权限用于表征用户可以对知识图谱数据库中的知识图谱数据执行任何权限的操作，包括读权限、写权限、读权限和请求读权限以及写权限和删除权限；请求读权限用于表征用户只能得到请

求数据的获取方式，不能直接得到请求数据的具体信息。

[0104] 示例性地，请求读权限的获取方式可以包括人工审核获取和验证码获取，本公开实施例这里不作限制。

[0105] 可以理解的是，对于机密性不高的数据，如果用户具有请求读权限，可以通过验证码的方式获取访问数据；对于机密性极高的数据，用户可以根据通过人工审核，向指定的人员获取访问数据，如此，满足了不同权限的访问控制需求，能够保证机密性高数据的安全性。

[0106] 本公开实施例中，在权限服务器103将至少一个访问控制列表发送给知识图谱服务器集群102之后，知识图谱服务器集群102还用于根据至少一个访问控制列表，获取访问数据，并将访问数据发送给客户端101，实现对用户的权限控制。

[0107] 需要说明的是，当用户访问知识图谱服务器集群102中存储的知识图谱数据时，知识图谱服务器集群102需要先获取至少一个访问控制列表，如果知识图谱服务器集群102没有获取到至少一个访问控制列表，则表示该用户不能对知识图谱服务器集群102中存储的知识图谱数据进行访问操作。

[0108] 本公开实施例中，知识图谱服务器集群102在根据至少一个访问控制列表，获取访问数据的过程中，知识图谱服务器集群102从至少一个访问控制列表中，获取用户组信息的访问策略；通过访问策略访问预存的知识图谱数据，获取访问数据，并发送访问数据给客户端。

[0109] 需要说明的是，用户组信息的访问策略可以是根据一个用户的不同用户组对应的访问控制列表，综合得到用户组信息的访问策略。

[0110] 示例性地，该访问策略可以包括读权限、写权限、读权限和请求读权限、写权限和删除权限以及系统管理员权限中的一个或者两个以上的组合，本公开实施例这里不作限制。

[0111] 本公开实施例中，一个用户对应一个或多个用户组，用户组是相同权限用户的集合，也就是说，当一个用户对应多个用户组时，该用户就对应着多种访问权限。

[0112] 示例性地，假定用户组A的访问权限为读权限，用户组B的访问权限为写权限，如果一个用户同时对应用户组A和用户组B，则该用户综合得到用户组信息的访问策略就是同时具备读权限和写权限，然后基于该读权限和写权限访问预存的知识图谱数据，得到该用户的访问数据。

[0113] 本公开实施例中，知识图谱服务器集群102包括中心服务器、主服务器和从服务器，该知识图谱服务器集群102在通过访问策略访问预存的知识图谱数据，获取访问数据的过程中，知识图谱服务器集群102可以通过中心服务器确定执行访问策略的服务器，当执行访问策略的服务器为主服务器时，检测主服务器是否处于异常状态，当主服务器处于异常状态时，根据预设选举规则，从知识图谱服务器集群102中选取一个从服务器，并发送访问策略给从服务器；通过从服务器执行该访问策略访问预设的知识图谱数据，获取访问数据。

[0114] 需要说明的是，在实际用户请求访问数据的过程中，读操作的需求量远远大于写操作，用户需要不断发出读操作请求数据，知识图谱服务器集群102需要根据该用户读权限执行来获取访问数据，并将该访问数据返回给客户端101，这时，用户对读取到的访问数据进行分析和过滤得到满足需求的访问数据。

[0115] 基于此，考虑到读操作的需求量的问题，本公开实施例知识图谱服务器集群102设置为主从服务器工作模式，将知识图谱服务器集群102中的多个服务器分别设置为中心服务器、主服务器和从服务器。中心服务器用于与客户端101、权限服务器102进行信息交互和确定执行访问策略的服务器；主服务器用于执行访问策略中的读写操作来获取访问数据；从服务器用于执行访问策略中的读操作来获取访问数据。

[0116] 可以理解的是，知识图谱服务器集群102设置为主从服务器的模式，作为主服务器的扩展，从服务器为主服务器分摊工作压力，能够提高访问效率。

[0117] 本公开实施例中，由于主服务器处于异常状态时，会影响用户获取访问数据，因此，中心服务器需要确定执行访问策略的服务器，当执行访问策略的服务器为主服务器时，检测主服务器是否处于异常状态，当主服务器处于异常状态时，根据预设选举规则，从知识图谱服务器集群102中选取一个从服务器来代替该异常的主服务器。

[0118] 需要说明的是，中心服务器一旦发现主服务器异常，就会将访问策略发送给选举得到的从服务器；通过从服务器执行访问策略访问预设的知识图谱数据，获取访问数据。

[0119] 本公开实施例中，主服务器处于异常状态可以是主服务器处于异常不工作状态，还可以是主服务器处于崩溃状态或者故障状态。

[0120] 需要说明的是，知识图谱服务器集群102中各服务器之间采用RAFT协议，以保证各服务器之间的数据同步。上述预设选举规则可以是根据RAFT协议采取“投票选举”的规则自动从至少一个从服务器中选择一个从服务器作为主服务器，来提供读写功能，其中，“投票选举”的规则可以为在所有的服务器中，当超过预设比例的主服务器选择同一个从服务器作为备用时，将该从服务器作为主服务器。

[0121] 示例性地，预设比例可以根据实际需求进行设置，如可以将该预设比例设置为0.5，即当所有的服务器中有一半的主服务器选择该从服务器时，该从服务器就作为主服务器，以代替异常的主服务器进行读写操作，具体预设比例设置，本公开实施例这里不作限制。

[0122] 在其他实施例中，图2为本公开实施例提供的一种权限控制系统结构示意图二，如图2所示，该权限控制系统还包括LDAP服务器104，LDAP服务器104与客户端101进行通信，其中，

[0123] 客户端101，还用于在发送第一访问请求给知识图谱服务器集群102之前，发送第三访问请求给LDAP服务器104，第三访问请求中携带有用户标识，第三访问请求用于向LDAP服务器104请求用户组信息；

[0124] LDAP服务器104，用于响应第三访问请求，获取用户标识，根据用户标识，以及预设用户标识与用户组信息的对应关系，获取与用户标识对应的用户组信息；并发送用户组信息给所述客户端101。

[0125] 本公开实施例中，当用户向知识图谱服务集群102中的知识图谱数据请求访问数据时，需要先向LDAP服务器104发起第三访问请求，该第三访问请求用于向LDAP服务器104请求用户组信息。

[0126] 需要说明的是，LDAP服务器104是基于LDAP搭建的服务器，用于存储所有的用户和用户组信息，可以是将用户信息和用户组信息存储为静态数据，并提供静态数据的快速查询方式，其中静态数据是指在运行过程中保持稳定的数据。

[0127] 本公开实施例中，在接收到客户端发送的第三访问请求之后，LDAP服务器104可以响应第三访问请求，获取用户标识，并根据用户标识，以及预设用户标识与用户组信息的对应关系，获取与用户标识对应的用户组信息；并发送用户组信息给所述客户端101。

[0128] 需要说明的是，LDAP服务器104只作为保存用户信息和用户组信息的服务器，不作为权限控制的服务器。

[0129] 在其他实施例中，图3为本公开实施例提供的一种权限控制系统结构示意图三，如图3所示，LDAP服务器104还与权限服务器103进行通信，权限控制系统中的LDAP服务器104，还用于在根据用户标识，以及预设用户标识与用户组信息的对应关系，获取与用户标识对应的用户组信息之后，发送更新请求给权限服务器103，该更新请求携带有更新的用户组信息；

[0130] 权限服务器103，还用于根据更新的用户组信息，更新预设权限三元映射关系。

[0131] 本公开实施例中，为了适应不断变化的需求，客户端101会在预设时间段内周期性地向LDAP服务器104请求最新的用户组信息，一旦LDAP服务器104更新了用户组信息，就会立即发送更新请求给权限服务器103，用于更新预设权限三元映射关系中用户组信息、数据源信息和访问控制列表之间的映射关系，如此，可以及时更新权限服务器103，提高了权限控制的精度。

[0132] 需要说明的是，上述预设时间段可以根据用户实际需求进行设置，如可以设置为5秒钟或者10秒钟，本公开实施例这里不作限制。

[0133] 通过上述本公开实施例，权限服务器存储的是用户组信息、数据源信息和访问控制列表之间的映射关系，访问控制列表为知识图谱数据对象的属性对应的访问权限，通过用户组信息和该权限三元映射关系便可以得到用户组对应的知识图谱数据对象的属性的访问权限，如此，能够以知识图谱数据对象的属性为粒度实现对用户的权限控制，提高了权限控制的灵活性和精度。

[0134] 基于上述公开实施例的同一发明构思，本公开实施例提供了权限控制方法，应用于知识图谱服务器集群的中心服务器，图4为本公开实施例提供的权限控制方法的流程示意图一，如图4所示，知识图谱服务器集群的中心服务器实现权限控制方法至少包括以下步骤：

[0135] S201、接收客户端发送的第一访问请求，第一访问请求携带有用户组信息。

[0136] 本公开实施例中，知识图谱服务器集群用于存储知识图谱数据，中心服务器在进行权限控制的过程中，中心服务器需要接收客户端发送的携带有用户组信息的第一访问请求。

[0137] 需要说明的是，一个用户可以对应一个或多个用户组，且用户组是相同权限用户的集合，也就是说，当一个用户对应多个用户组时，该用户就对应着多种知识图谱数据对象属性的访问权限。

[0138] 示例性地，用户组A对应居民基础信息的访问权限，用户组B对应居民身份信息的访问权限，如果用户a仅属于用户组A，那么该用户a具备访问居民基础信息的权限，不具备访问居民身份信息的权限；如果用户a属于用户组A和用户组B，那么用户a同时具备访问居民基础信息的权限和访问居民身份信息的权限，本公开实施例这里不作限制。

[0139] S202、响应第一访问请求，根据用户组信息生成第二访问请求，第二访问请求用于

向权限服务器请求访问权限。

[0140] 本公开实施例中，中心服务器在接收客户端发送的第一访问请求之后，响应第一访问请求，生成第二访问请求，该第二访问请求用于向权限服务器请求访问权限。

[0141] 需要说明的是，中心服务器中不存储知识图谱数据的访问权限，该知识图谱数据的访问权限存储在权限服务器。

[0142] S203、发送第二访问请求给权限服务器。

[0143] 本公开实施例中，权限服务器用于存储知识图谱中所有数据中的访问权限，在用户访问知识图谱服务器集群中的知识图谱数据时，中心服务器需要发送第二请求给权限服务器，以得到权限服务器返回的用户组信息对应的至少一个访问控制列表。

[0144] S204、接收权限服务器响应第二访问请求返回的至少一个访问控制列表，至少一个访问控制列表为与用户组信息中的至少一个用户组信息对应。

[0145] 本公开实施例中，中心服务器在发送第二访问请求给权限服务器之后，需要接收权限服务器响应第二访问请求返回的至少一个访问控制列表。

[0146] 需要说明的是，一个用户可以对应至少一个用户组信息，本公开实施例的用户组信息可以理解为至少一个用户组信息，进而得到对应的至少一个访问控制列表。

[0147] S205、根据至少一个访问控制列表，获取访问数据。

[0148] 本公开实施例中，中心服务器在接收到用户组信息对应的至少一个访问控制列表之后，根据至少一个访问控制列表，获取访问权限。

[0149] 考虑到知识图谱服务器集群中的主服务器处于异常状态时，会影响用户获取访问数据，因此，中心服务器需要确定执行访问策略的服务器，在根据至少一个访问控制列表，获取访问数据的过程中，中心服务器先根据至少一个访问控制列表，确定执行访问策略的服务器；再基于执行访问策略的服务器，获取访问数据。

[0150] 具体地，中心服务器在基于执行访问策略的服务器，获取访问数据过程中，当执行访问策略的服务器为知识图谱服务器集群中的主服务器时，发送访问策略给主服务器，接收主服务器响应访问策略返回的访问数据；当执行访问策略的服务器为知识图谱服务器集群中的从服务器时，发送访问策略给从服务器，接收从服务器响应访问策略返回的访问数据。

[0151] 进一步，中心服务器当执行访问策略的服务器为知识图谱服务器集群中的主服务器时，发送访问策略给主服务器的过程中，会检测主服务器的状态，具体地，当执行访问策略的服务器为知识图谱服务器集群中的主服务器时，检测主服务器是否处于异常状态；当主服务器处于异常状态时，根据预设选举规则，从知识图谱服务器集群中选取一个从服务器，发送访问策略给从服务器，接收该从服务器响应访问策略返回的访问数据。

[0152] 如此，本公开实施考虑到知识图谱服务器集群中的主服务器处于异常状态时，会影响用户获取访问数据，通过预设选举规则以防止主服务器异常导致不能返回访问数据给客户端，这样的防错机制提高了用户的体验感。

[0153] S206、发送访问数据给客户端。

[0154] 通过本公开实施例，中心服务器通过向权限服务器请求用户组信息对应的至少一个访问控制列表，能够基于用户组信息，使得用户得到以知识图谱数据对象的属性信息为粒度的权限控制，提高了权限控制的灵活性和精度。

[0155] 基于上述公开实施例的同一发明构思，本公开实施例提供了权限控制方法，应用于知识图谱服务器集群的主服务器，图5为本公开实施例提供的权限控制方法的流程示意图二，如图5所示，主服务器实现权限控制方法至少包括以下步骤：

[0156] S301、接收知识图谱服务器集群的中心服务器发送的访问策略，访问策略用于表征读写访问权限。

[0157] 本公开实施例中，访问策略用于表征读写访问权限，如在主服务器执行访问策略时，能够基于访问策略执行读写操作。

[0158] S302、根据访问策略访问预存的知识图谱数据，获取访问数据。

[0159] 本公开实施例中，主服务器接收到访问策略之后，根据该访问策略执行读写权限操作，具体地，依据访问策略中的读写权限，访问预存的知识图谱数据，获取访问数据。

[0160] S303、将访问数据发送给中心服务器。

[0161] 通过本公开实施例，在确定主服务器执行访问策略之后，主服务器能够执行对应的读写权限操作，便于精确的获取用户的访问数据。

[0162] 基于上述公开实施例的同一发明构思，本公开实施例提供了权限控制方法，应用于知识图谱服务器集群的从服务器，图6为本公开实施例提供的权限控制方法的流程示意图三，如图6所示，从服务器实现权限控制方法至少包括以下步骤：

[0163] S401、接收知识图谱服务器集群的中心服务器发送的访问策略，访问策略用于表征读访问权限。

[0164] 本公开实施例中，访问策略用于表征读访问权限，在从服务执行访问策略时，能够基于访问策略执行读操作。

[0165] S402、根据访问策略访问预存的知识图谱数据，获取访问数据。

[0166] 本公开实施例中，从服务器接收到访问策略之后，根据该访问策略执行读权限操作，具体地，依据访问策略中的读权限，访问预存的知识图谱数据，获取访问数据。

[0167] S403、将访问数据发送给中心服务器。

[0168] 通过本公开实施例，在确定从服务器执行访问策略之后，从服务器能够执行对应的读权限操作，便于精确的获取用户的访问数据，并且能够基于用户的读请求来控制对应的从服务器获取读数据，这种主从模式，能够缓解主服务器的工作压力，提高了工作效率。

[0169] 基于上述公开实施例的同一发明构思，本公开实施例提供了权限控制方法，应用于权限服务器，图7为本公开实施例提供的权限控制方法的流程示意图四，如图7所示，权限服务器实现权限控制至少包括以下步骤：

[0170] S501、接收中心服务器发送的第二访问请求，第二访问请求携带有用户组信息。

[0171] 本公开实施例中，在知识图谱服务器集群执行用户的第一访问请求的过程中，需要向权限服务器发送第二访问请求，用于获取用户组信息对应的至少一个访问控制列表，对应地，权限服务器接收该知识图谱服务器集群发送的第二访问请求。

[0172] S502、根据用户组信息和预设权限三元映射关系，获取与用户组信息对应的至少一个访问控制列表，至少一个访问控制列表用于表征知识图谱数据对象的属性信息对应的访问权限，预设三元映射关系用于表征用户组信息、数据源信息和访问控制列表之间的映射关系。

[0173] 本公开实施例中，权限服务器在获取用户组信息之后，根据用户组信息和预设权

限三元映射关系，获取与用户组信息对应的至少一个访问控制列表。

[0174] 需要说明的是，预设权限三元映射关系中的三元包括：用户组信息、数据源信息和访问控制列表；权限三元映射关系包括用户组信息与数据源信息的对应关系、预设数据源信息与访问控制列表的对应关系。

[0175] 权限服务器在根据用户组信息和预设权限三元映射关系，获取与用户组信息对应的至少一个访问控制列表的过程中，根据用户组信息，以及预设用户组信息与数据源信息的对应关系，确定与用户组信息对应的数据源信息；根据数据源信息，以及预设数据源信息与访问控制列表的对应关系，确定与用户组信息对应的至少一个访问控制列表。

[0176] 可以理解的是，权限服务器中的用户组信息都会绑定对应的数据源信息，且每个数据源都对应着访问控制列表，该访问控制列表用于表征知识图谱数据对象的属性信息对应的访问权限，也就是说，每一个用户组信息都对应一种知识图谱数据对象的属性的访问权限，通过一个用户对应的多个用户组，即可得到该用户对应的不同访问权限，如此，实现了以知识图谱数据对象的属性为粒度进行访问控制，使得访问控制粒度更细，精度更高。

[0177] S503、将至少一个访问控制列表发送给中心服务器。

[0178] 本公开实施例中，权限服务器在获取至少一个访问控制列表之后，将至少一个访问控制列表发送给知识图谱服务器集群。

[0179] 权限服务器在将至少一个访问控制列表发送给中心服务器之后，还可以接收LDAP服务器发送的更新请求，更新请求携带有更新的用户组信息；根据更新的用户组信息，更新预设权限三元映射关系。

[0180] 本公开实施例中，为了适应不断变化的用户组信息，需要周期性的更新LDAP服务器中存储的用户组信息，以实现及时更新权限服务器，提高了权限控制的精度。

[0181] 通过本公开实施例，权限服务器中存储的是用户组信息、数据源信息和访问控制列表之间的映射关系，通过用户组信息和该映射关系，就可以得到用户组信息对应的访问权限，如此，能够基于知识图谱数据对象的属性存储对应的访问权限，便于知识图谱服务器集群能够以知识图谱数据对象的属性为粒度进行权限控制。

[0182] 基于上述公开实施例的同一发明构思，本公开实施例提供了权限控制方法，应用于客户端，图8为本公开实施例提供的权限控制方法的流程示意图五，如图8所示，客户端实现权限控制方法至少包括以下步骤：

[0183] S601、接收LDAP服务器发送的用户组信息。

[0184] 本公开实施例中，客户端在发送第一访问请求给中心服务器请求访问数据之前，需要发送第三访问请求给LDAP服务器以获取该用户的用户组信息，具体地，发送第三访问请求给LDAP服务器，第三访问请求中携带有用户标识；获取LDAP服务器响应第三访问请求返回的用户组信息。

[0185] 需要说明的是，客户端可以在预设时间段内周期性地发送第三访问请求给LDAP服务器，该预设时间段可以依据用户实际需求进行设置，如可以设置为3秒钟，以实现得到该用户最新的用户组信息。

[0186] 本公开实施例中，LDAP服务器用于存储用户和用户组信息，客户端通过发送携带有用户标识的第三访问请求，便可以获取该用户标识对应的用户组信息。

[0187] 由于一个用户可以对应一个以上的用户组，当用户对应多个用户组时，客户端获

取多个用户组信息。

[0188] S602、将用户组信息携带在第一访问请求中，发送第一访问请求给中心服务器。

[0189] 本公开实施例中，当用户需要获取知识图谱数据时，通过客户端发送第一访问请求给中心服务器，用于向该中心服务器请求访问数据，该访问数据可以理解为用户想要获取的知识图谱数据。

[0190] S603、获取中心服务器响应第一访问请求返回的访问数据。

[0191] 本公开实施例中，客户端在发送第一访问请求给中心服务器之后，中心服务器根据用户组信息生成第二访问请求，发送第二访问请求给权限服务器，权限服务器响应该第二访问请求返回至少一个访问控制列表给中心服务器，中心服务器根据至少一个访问控制列表，获取访问数据，并将访问数据发送给客户端。

[0192] 通过本公开实施例中，客户端通过第一访问请求中携带的用户组信息，向中心服务器请求访问数据，能够获取中心服务器以属性为粒度进行权限控制返回的访问数据，实现了以属性为粒度的权限控制。

[0193] 基于上述公开实施例的同一发明构思，本公开实施例提供了权限控制方法，应用于LDAP服务器，图9为本公开实施例提供的权限控制方法的流程示意图六，如图9所示，LDAP服务器实现权限控制方法至少包括以下步骤：

[0194] S701、接收客户端发送的第三访问请求，第三访问请求携带有用户标识。

[0195] 本公开实施例中，LDAP服务器用于存储用户信息和用户组信息，LDAP服务器在客户端发送第一访问请求给中心服务器之前，接收客户端发送的用于请求用户组信息的第三访问请求。

[0196] S702、根据用户标识，以及预设用户标识与用户组信息的对应关系，获取与用户标识对应的用户组信息。

[0197] 本公开实施例中，LDAP服务器在接收客户端发送的第三访问请求之后，还根据用户标识，以及预设用户标识与用户组信息的对应关系，获取与用户标识对应的用户组信息。

[0198] 需要说明的是，由于一个用户可以对应一个以上的用户组，当用户对应多个用户组时，客户端获取多个用户组信息。

[0199] 示例性地，当用户对应用户身份组和用户名称组时，这时获取则是用户身份组信息和用户名称组信息这两个用户组信息。

[0200] S703、发送用户组信息给客户端。

[0201] 本公开实施例中，LDAP服务器在获取用户组信息之后，发送用户组信息给客户端。

[0202] 需要说明的是，LDAP服务器在发送用户组信息给客户端之后，还可以发送更新请求给权限服务器，该更新请求携带有更新的用户组信息，用于更新权限服务器中存储的用户组信息。

[0203] 通过本公开实施例中的权限控制方法，LDAP服务器存储用户组信息，一方面，可以基于用户标识获取对应的用户组信息，另一方面，可以周期性的更新用户组信息，并发送该用户组信息给权限服务器，使得权限服务器也周期性的更新存储的映射关系，便于中心服务器更精确的获取用户组信息对应的访问权限。

[0204] 基于上述公开实施例的同一发明构思，本公开实施例提出了一种权限控制方法，应用于客户端、权限服务器、LDAP服务器和知识图谱服务器集群的中心服务器，图10为本公

开实施例提供的一种权限控制方法的交互示意图，如图10所示，实现权限控制方法至少包括以下步骤：

[0205] S801、客户端发送第三访问请求给LDAP服务器，第三访问请求携带有用户标识；

[0206] S802、LDAP服务器根据用户标识，以及预设用户标识与用户组信息的对应关系，获取与用户标识对应的用户组信息；

[0207] S803、LDAP服务器发送用户组信息给客户端；

[0208] S804、客户端将用户组信息携带在第一访问请求中，发送第一访问请求给中心服务器；

[0209] S805、中心服务器响应第一访问请求，根据用户组信息，生成第二访问请求；

[0210] S806、中心服务器发送第二访问请求给权限服务器，第二访问请求中携带有用户组信息；

[0211] S807、权限服务器响应第二访问请求，根据用户组信息和预设权限三元映射关系，获取与用户组信息对应的至少一个访问控制列表；

[0212] S808、权限服务器发送至少一个访问控制列表给中心服务器；

[0213] S809、中心服务器根据至少一个访问控制列表，获取访问数据；

[0214] S810、中心服务器将访问数据发送给客户端。

[0215] 本公开实施例中权限服务器存储的是用户组信息、数据源信息和访问控制列表之间的映射关系，访问控制列表为知识图谱数据对象的属性对应的访问权限，通过用户组信息和该权限三元映射关系便可以得到用户组对应的知识图谱数据对象的属性的访问权限，如此，能够以知识图谱数据对象的属性为粒度实现对用户的权限控制，提高了权限控制的灵活性和精度，同时，本公开实施例中访问权限的获取考虑到了用户组信息的不同数据源信息，并基于该数据源信息获取用户组信息的访问权限，能够提高访问数据的安全性。

[0216] 基于上述公开实施例的同一发明构思，本公开实施例提供一种知识图谱服务器集群的中心服务器，图11为本公开实施例提供的知识图谱服务器集群的中心服务器的组成结构示意图一，如图11所示，中心服务器1000包括第一接收单元1001、第一获取单元1002、第一发送单元1003、第二接收单元1004、第二获取单元1005、和第二发送单元1006，其中，

[0217] 所述第一接收单元1001，用于接收客户端发送的第一访问请求，所述第一访问请求携带有用户组信息；

[0218] 所述第一获取单元1002，用于响应所述第一访问请求，根据所述用户组信息生成第二访问请求；

[0219] 所述第一发送单元1003，用于发送第二访问请求给权限服务器，所述第二访问请求用于向所述权限服务器请求访问权限；

[0220] 所述第二接收单元1004，用于接收所述权限服务器响应所述第二访问请求返回的至少一个访问控制列表，所述至少一个访问控制列表为与所述用户组信息中的至少一个用户组信息对应；

[0221] 所述第二获取单元1005，用于根据所述至少一个访问控制列表，获取所述用户的访问数据；

[0222] 所述第二发送单元1006，用于发送所述访问数据给所述客户端。

[0223] 在其他实施例中，所述第二获取单元1005，具体用于根据所述至少一个访问控制

列表，确定执行所述访问策略的服务器；基于所述执行所述访问策略的服务器，获取所述访问数据。

[0224] 在其他实施例中，所述第二获取单元1005，还具体用于当执行所述访问策略的服务器为所述知识图谱服务器集群中的主服务器时，发送所述访问策略给所述主服务器；当执行所述访问策略的服务器为所述知识图谱服务器集群中的从服务器时，发送所述访问策略给所述从服务器。

[0225] 在其他实施例中，所述第二获取单元1005，还具体用于当所述执行访问策略的服务器为所述知识图谱服务器集群中的所述主服务器时，检测所述主服务器是否处于异常状态；当所述主服务器处于异常状态时，根据预设选举规则，从所述知识图谱服务器集群中选取一个从服务器，发送所述访问策略给所述从服务器；接收所述从服务器响应所述访问策略返回的所述访问数据。

[0226] 基于上述公开实施例的同一发明构思，本公开实施例提供一种知识图谱服务器集群的主服务器，图12为本公开实施例提供的知识图谱服务器集群的主服务器的组成结构示意图一，如图12所示，所述主服务器2000包括第三接收单元2001、第三获取单元2002、第三发送单元2003，其中，

[0227] 所述第三接收单元2001，用于接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读写访问权限；

[0228] 所述第三获取单元2002，用于根据所述访问策略访问预存的知识图谱数据，获取第一访问数据；

[0229] 所述第三发送单元2003，用于将所述第一访问数据发送给中心服务器。

[0230] 基于上述公开实施例的同一发明构思，本公开实施例提供一种知识图谱服务器集群的从服务器3000，图13为本公开实施例提供的知识图谱服务器集群的从服务器的组成结构示意图一，如图13所示，所述从服务器3000包括第四接收单元3001、第四获取单元3002、第四发送单元3003，其中，

[0231] 所述第四接收单元3001，用于接收所述知识图谱服务器集群的中心服务器发送的访问策略，所述访问策略用于表征读访问权限；

[0232] 所述第四获取单元3002，用于根据所述访问策略访问预存的知识图谱数据，获取访问数据；

[0233] 所述第四发送单元3003，用于将所述访问数据发送给所述中心服务器。

[0234] 基于上述公开实施例的同一发明构思，本公开实施例提供一种权限服务器4000，图14为本公开实施例提供的权限服务器的组成结构示意图一，如图14所示，权限服务器4000包括第五接收单元4001、第五获取单元4002和第五发送单元4003，其中

[0235] 所述第五接收单元4001，用于接收中心服务器发送的第二访问请求，所述第二访问请求携带有用户组信息；

[0236] 所述第五获取单元4002，用于根据所述用户组信息和预设权限三元映射关系，获取与所述用户组信息对应的至少一个访问控制列表，所述至少一个访问控制列表用于表征所述知识图谱数据对象的属性信息对应的所述访问权限，所述预设权限三元映射关系用于表征所述用户组信息、数据源信息和所述访问控制列表之间的映射关系；

[0237] 所述第五发送单元4003，用于将所述至少一个访问控制列表发送给所述中心服务

器。

[0238] 在其他实施例中,所述第五获取单元4002,具体用于根据所述用户组信息,以及预设用户组信息与数据源信息的对应关系,确定与所述用户组信息对应的数据源信息;根据所述数据源信息,以及预设数据源信息与访问控制列表的对应关系,获取与所述用户组信息对应的至少一个访问控制列表。

[0239] 在其他实施例中,所述权限服务器4000,还用于接收LDAP服务器发送的更新请求,所述更新请求携带有更新的用户组信息;根据所述更新的用户组信息,更新所述预设权限三元映射关系。

[0240] 基于上述公开实施例的同一发明构思,本公开实施例提供一种客户端,图15为本公开实施例提供的客户端的组成结构示意图一,如图15所示,客户端5000包括第六接收单元5001、第六发送单元5002和第六获取单元5003,其中

[0241] 所述第六接收单元5001,用于接收LDAP服务器发送的用户组信息。

[0242] 所述第六发送单元5002,用于将用户组信息携带在第一访问请求中,发送第一访问请求给中心服务器。

[0243] 所述第六获取单元5003,用于获取中心服务器响应第一访问请求返回的访问数据。

[0244] 在其他实施例中,所述客户端5000,还用于发送第三访问请求给LDAP服务器,第三访问请求中携带有用户标识;获取LDAP服务器响应第三访问请求返回的用户组信息。

[0245] 基于上述公开实施例的同一发明构思,本公开实施例提供一种权限控制方法,图16为本公开实施例提供的LDAP服务器的组成结构示意图一,如图16所示,LDAP服务器6000包括第七获取单元6001、第七获取单元6002和第七发送单元6003,其中,

[0246] 所述第七获取单元6001,用于接收客户端发送的第三访问请求,第三访问请求有用户标识。

[0247] 所述第七获取单元6002,用于根据用户标识,以及预设用户标识与用户组信息的对应关系,获取与用户标识对应的用户组信息。

[0248] 所述第七发送单元6003,用于发送用户组信息给客户端。

[0249] 在其他实施例中,所述LDAP服务器6000,还用于发送更新请求给权限服务器,该更新请求携带有更新的用户组信息。

[0250] 通过本公开实施例,本公开实施例权限服务器存储的是用户组信息、数据源信息和访问控制列表之间的映射关系,访问控制列表为知识图谱数据对象的属性对应的访问权限,通过用户组信息和该映射关系便可以得到用户组对应的知识图谱数据对象的属性的访问权限,如此,能够以知识图谱数据对象的属性为粒度实现对权限控制,提高了权限控制的灵活性和精度。

[0251] 基于上述公开实施例的同一发明构思,本公开实施例提供一种知识图谱服务器集群的中心服务器,图17为本公开实施例提供的知识图谱服务器集群的中心服务器的组成结构示意图二,如图17所示,知识图谱服务器集群的中心服务器至少包括第一处理器01、第一通信总线02、第一存储器03及第一通信接口04,其中,第一通信总线02用于实现第一处理器01、第一通信接口04和第一存储器03之间的连接通信;第一通信接口04用于与客户端和权限服务器进行数据传输;第一处理器01用于执行第一存储器03中存储的可执行性指令,以

实现上述公开实施例提供的权限控制方法中的步骤。

[0252] 基于上述公开实施例的同一发明构思，本公开实施例提供一种知识图谱服务器集群的主服务器，图18为本公开实施例提供的知识图谱服务器集群的主服务器的组成结构示意图二，如图18所示，所述主服务器至少包括第二处理器05、第二通信总线06、第二存储器07及第二通信接口08，其中，所述第二通信总线06用于实现所述第二处理器05、所述第二通信接口08和所述第二存储器07之间的连接通信；所述第二通信接口08用于获取访问控制策略；所述第二处理器05用于执行所述第二存储器07中存储的可执行指令，当所述可执行指令被执行时，所述第二处理器05执行时实现上述公开实施例提供的权限控制方法中的步骤。

[0253] 基于上述公开实施例的同一发明构思，本公开实施例提供一种知识图谱服务器集群的从服务器，图19为本公开实施例提供的知识图谱服务器集群的从服务器的组成结构示意图二，如图19所示，所述从服务器至少包括第三处理器09、第三通信总线10、第三存储器11及第三通信接口12，其中，所述第三通信总线10用于实现所述第三处理器09、所述第三通信接口12和所述第三存储器11之间的连接通信；所述第三通信接口12用于获取访问控制策略；所述第三处理器09用于执行所述第三存储器11中存储的可执行指令，当所述可执行指令被执行时，所述第三处理器09执行时实现上述公开实施例提供的权限控制方法中的步骤。

[0254] 基于上述公开实施例的同一发明构思，本公开实施例提供一种权限服务器，图20为本公开实施例提供的权限服务器的组成结构示意图二，如图20所示，权限服务器至少包括第四处理器13、第四通信总线14、第四存储器15及第四通信接口16，其中，第四通信总线14用于实现第四处理器13、第四通信接口16和第四存储器15之间的连接通信；第四通信接口14用于与LDAP服务器和知识图谱服务器集群进行数据传输；第四处理器13用于执行第四储器15中存储的可执行指令，以实现上述公开实施例提供的权限控制方法中的步骤。

[0255] 基于上述公开实施例的同一发明构思，本公开实施例提供一种客户端，图21为本公开实施例提供的客户端的组成结构示意图二，如图21所示，客户端至少包括第五处理器17、第五通信总线18、第五存储器19及第五通信接口20，其中，第五通信总线18用于实现第五处理器20、第五通信接口20和第五存储器17之间的连接通信；第五通信接口20用于与LDAP服务器和知识图谱服务器集群进行数据传输；第五处理器20用于执行第五存储器17中存储的可执行指令，以实现上述公开实施例提供的权限控制方法中的步骤。

[0256] 基于上述公开实施例的同一发明构思，本公开实施例提供一种LDAP服务器，图22为本公开实施例提供的LDAP服务器的组成结构示意图二，如图22示，LDAP服务器至少包括第六处理器21、第六通信总线22、第六存储器23及第六通信接口24，其中，第六通信总线22用于实现第六处理器21、第六通信接口22和第六存储器23之间的连接通信；第六通信接口24用于与客户端和权限服务器进行数据传输；第六处理器21用于执行第六存储器23中存储的可执行指令，以实现上述公开实施例提供的权限控制方法中的步骤。

[0257] 另外，在本实施例中的各组成部分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模块的形式实现。

[0258] 所述集成的单元如果以软件功能模块的形式实现并非作为独立的产品进行销售

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，本实施例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)或processor(处理器)执行本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：磁性随机存取存储器(FRAM，ferromagnetic random access memory)、只读存储器(ROM，Read Only Memory)、可编程只读存储器(PROM，Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM，Erasable Programmable Read-Only Memory)、电可擦除可编程只读存储器(EEPROM，Electrically Erasable Programmable Read-Only Memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM，Compact Disc Read-Only Memory)等各种可以存储程序代码的介质，本公开实施例不作限制。

[0259] 基于前述实施例，本公开实施例提供了一种计算机可读存储介质，其上存储有可执行指令，上述可执行指令被上述第一处理器、第二处理器、第三处理器、第四处理器、第五处理器或者第六处理器执行时实现上述公开实施例提供的权限控制方法中的步骤。

[0260] 本领域内的技术人员应明白，本公开实施例的实施例可提供为方法、系统、或计算机程序产品。因此，本公开实施例可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且，本公开实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器和光学存储器等)上实施的计算机程序产品的形式。

[0261] 本公开实施例是参照根据本公开实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0262] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0263] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。以上所述，仅为本公开实施例的较佳实施例而已，并非用于限定本公开实施例的保护范围。

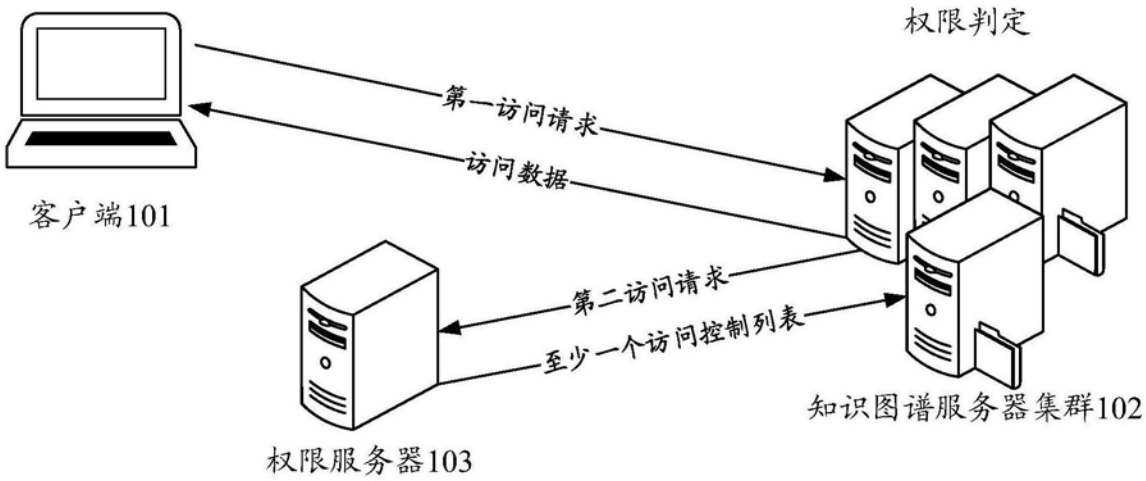

权限判定
第一访问请求
访问数据
客户端101
第二访问请求
至少一个访问控制列表
知识图谱服务器集群102
权限服务器103

图1

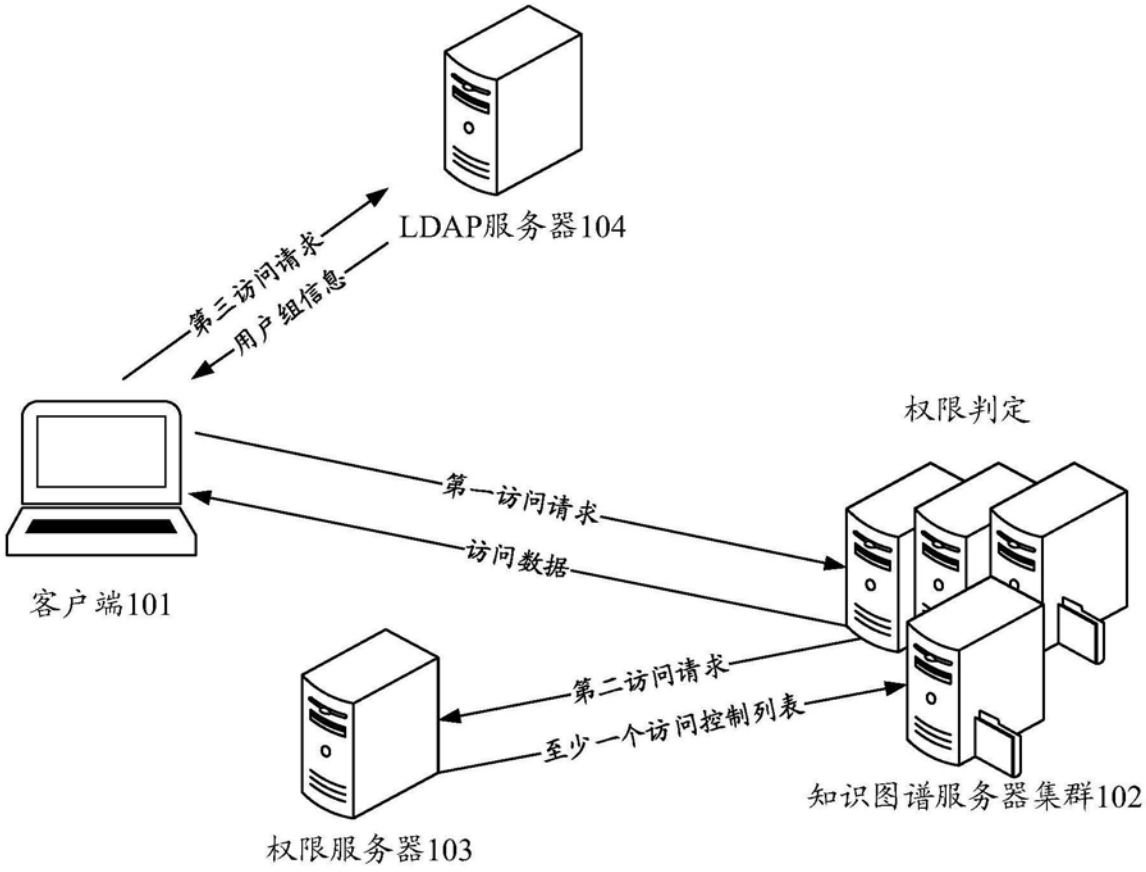

LDAP服务器104
第三访问请求
用户组信息
权限判定
第一访问请求
访问数据
客户端101
第二访问请求
至少一个访问控制列表
知识图谱服务器集群102
权限服务器103

图2

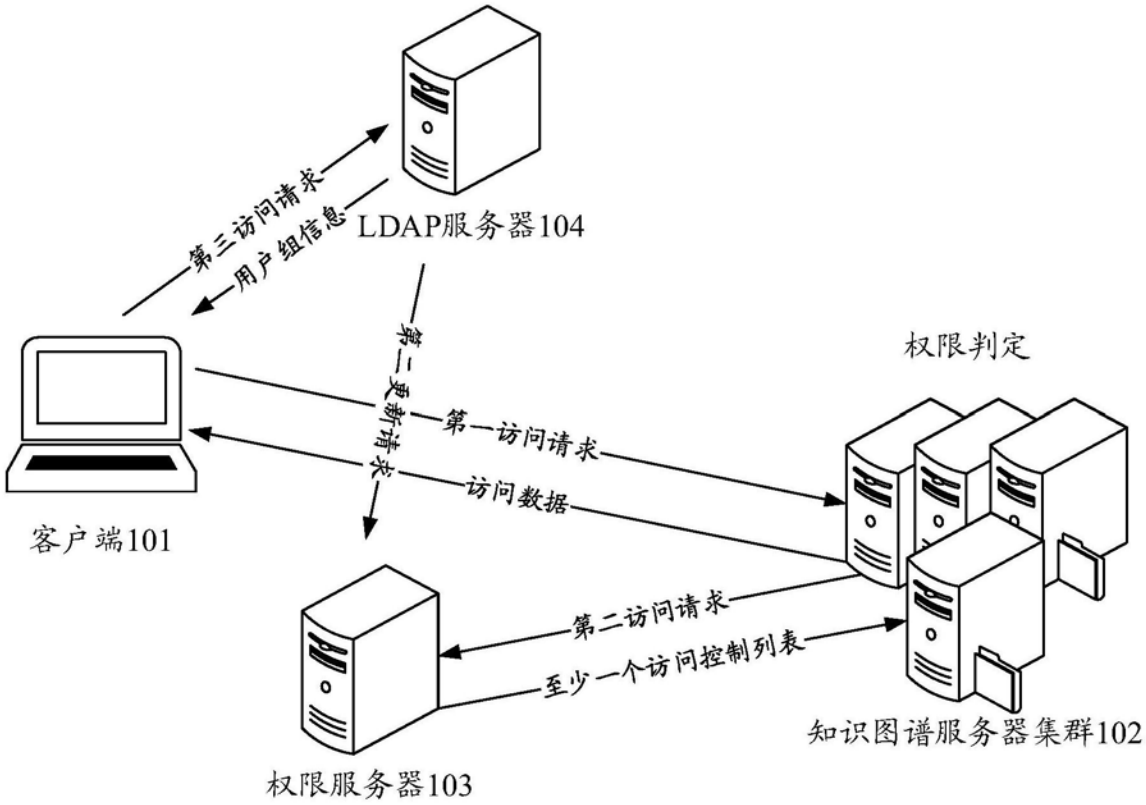

第三访问请求
用户组信息
LDAP服务器104
第一更新请求
权限判定
第一访问请求
访问数据
客户端101
第二访问请求
至少一个访问控制列表
知识图谱服务器集群102
权限服务器103

图3

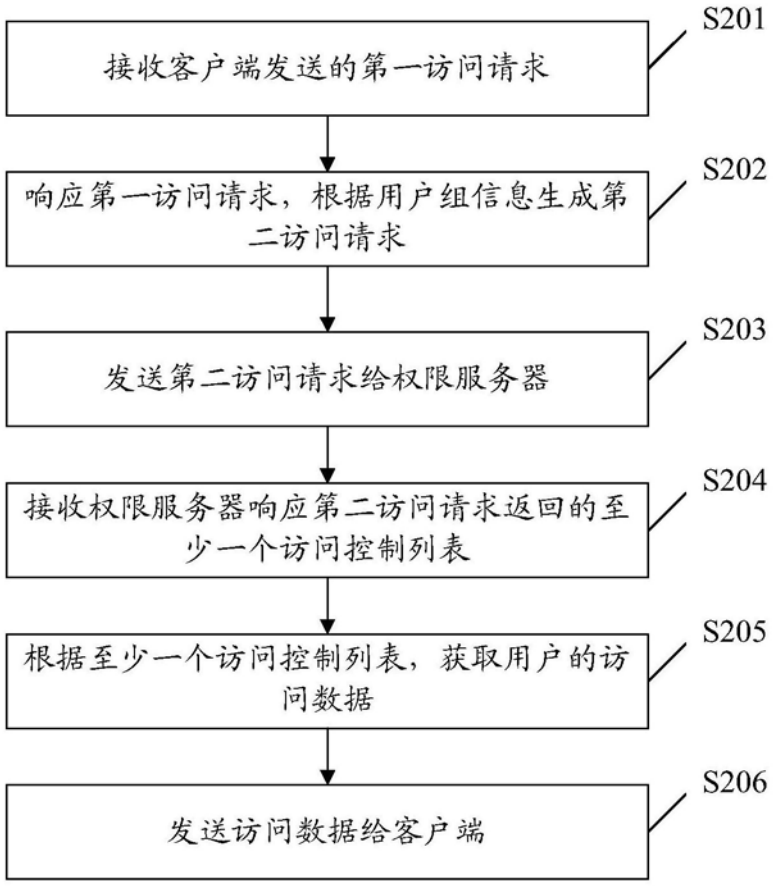

S201
接收客户端发送的第一访问请求
S202
响应第一访问请求，根据用户组信息生成第二访问请求
S203
发送第二访问请求给权限服务器
S204
接收权限服务器响应第二访问请求返回的至少一个访问控制列表
S205
根据至少一个访问控制列表，获取用户的访问数据
S206
发送访问数据给客户端

图4

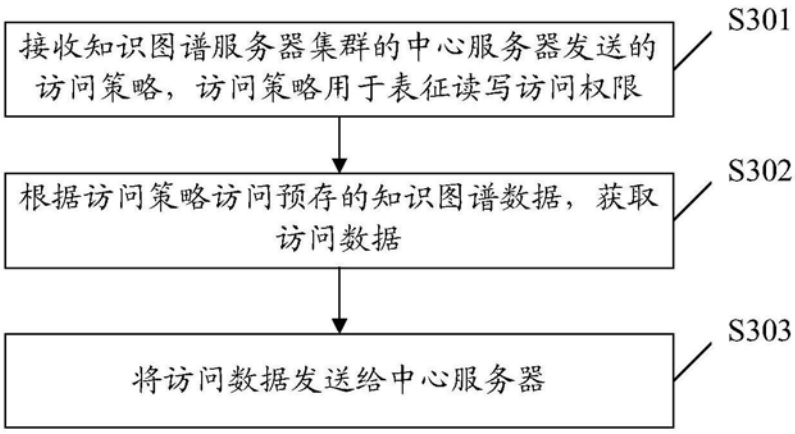

S301
接收知识图谱服务器集群的中心服务器发送的访问策略，访问策略用于表征读写访问权限
S302
根据访问策略访问预存的知识图谱数据，获取访问数据
S303
将访问数据发送给中心服务器

图5

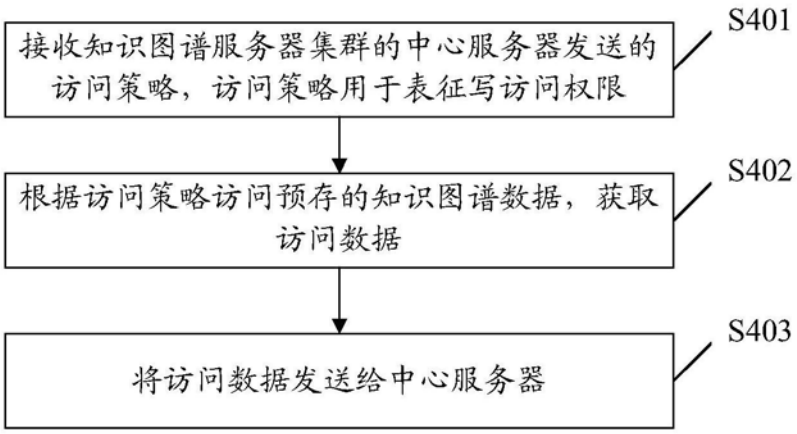

S401
接收知识图谱服务器集群的中心服务器发送的访问策略，访问策略用于表征写访问权限
S402
根据访问策略访问预存的知识图谱数据，获取访问数据
S403
将访问数据发送给中心服务器

图6

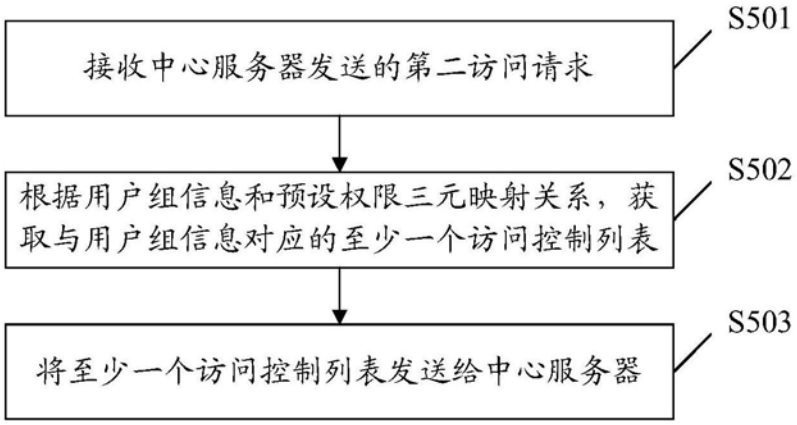

S501
接收中心服务器发送的第二访问请求
S502
根据用户组信息和预设权限三元映射关系，获取与用户组信息对应的至少一个访问控制列表
S503
将至少一个访问控制列表发送给中心服务器

图7

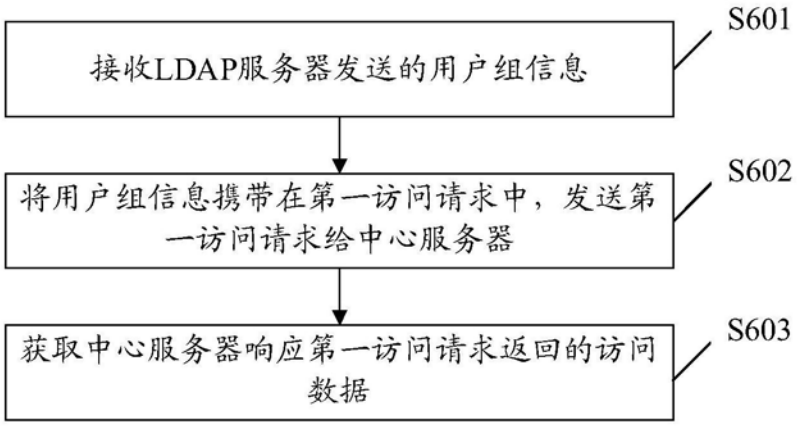

S601
接收LDAP服务器发送的用户组信息
S602
将用户组信息携带在第一访问请求中，发送第一访问请求给中心服务器
S603
获取中心服务器响应第一访问请求返回的访问数据

图8

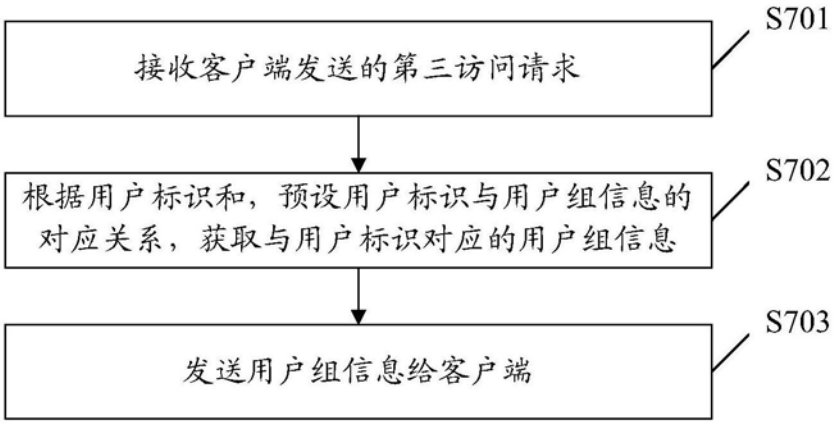

S701
接收客户端发送的第三访问请求
S702
根据用户标识和，预设用户标识与用户组信息的对应关系，获取与用户标识对应的用户组信息
S703
发送用户组信息给客户端

图9

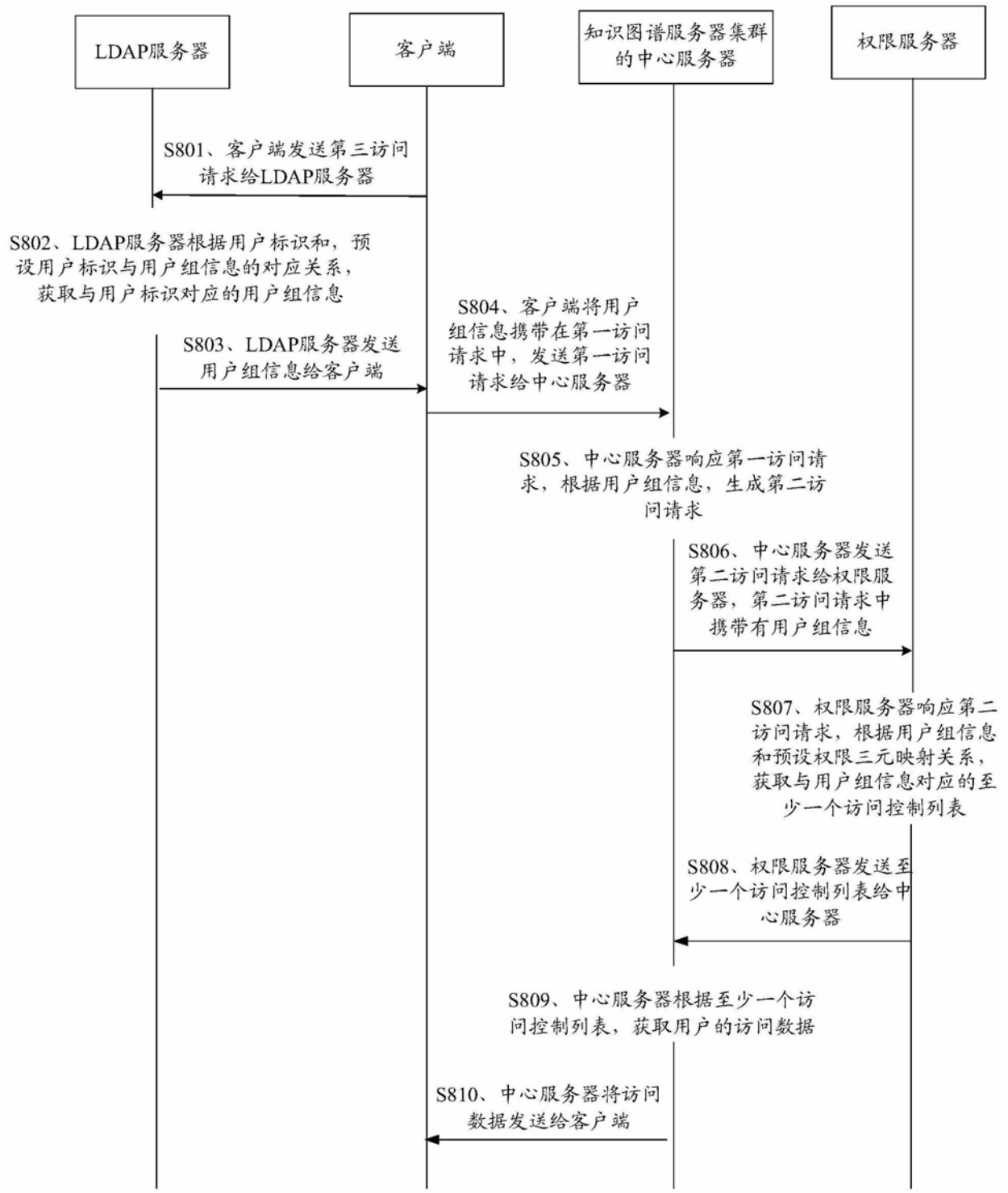

LDAP服务器
客户端
知识图谱服务器集群的中心服务器
权限服务器
S801、客户端发送第三访问请求给LDAP服务器
S802、LDAP服务器根据用户标识和，预设用户标识与用户组信息的对应关系，获取与用户标识对应的用户组信息
S803、LDAP服务器发送用户组信息给客户端
S804、客户端将用户组信息携带在第一访问请求中，发送第一访问请求给中心服务器
S805、中心服务器响应第一访问请求，根据用户组信息，生成第二访问请求
S806、中心服务器发送第二访问请求给权限服务器，第二访问请求中携带有用户组信息
S807、权限服务器响应第二访问请求，根据用户组信息和预设权限三元映射关系，获取与用户组信息对应的至少一个访问控制列表
S808、权限服务器发送至少一个访问控制列表给中心服务器
S809、中心服务器根据至少一个访问控制列表，获取用户的访问数据
S810、中心服务器将访问数据发送给客户端

图10

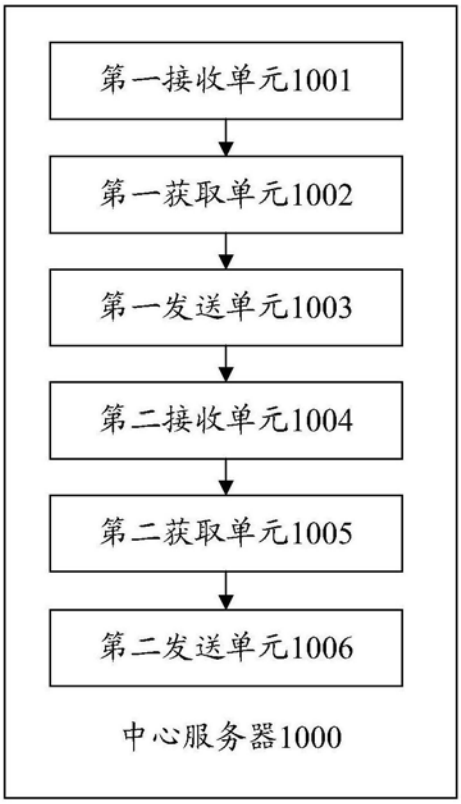

第一接收单元1001
第一获取单元1002
第一发送单元1003
第二接收单元1004
第二获取单元1005
第二发送单元1006
中心服务器1000

图11

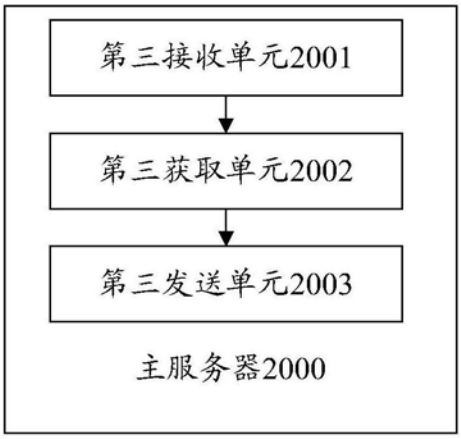

第三接收单元2001
第三获取单元2002
第三发送单元2003
主服务器2000

图12

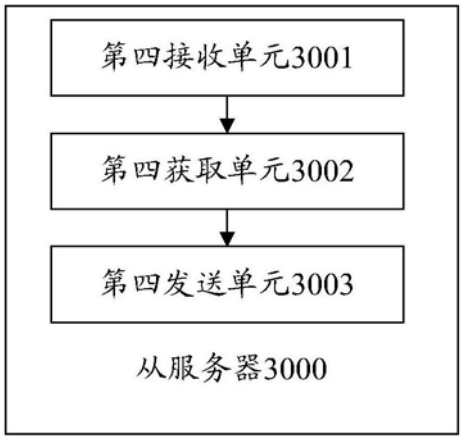

第四接收单元3001
第四获取单元3002
第四发送单元3003
从服务器3000

图13

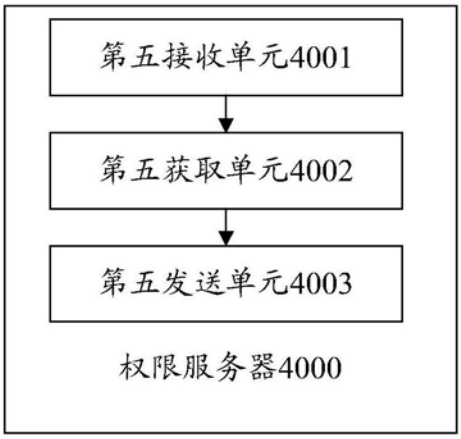

第五接收单元4001
第五获取单元4002
第五发送单元4003
权限服务器4000

图14

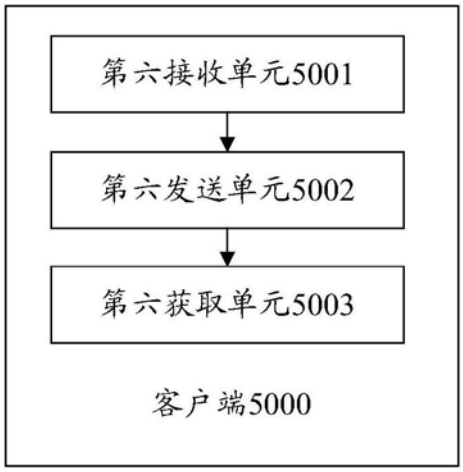

第六接收单元5001
第六发送单元5002
第六获取单元5003
客户端5000

图15

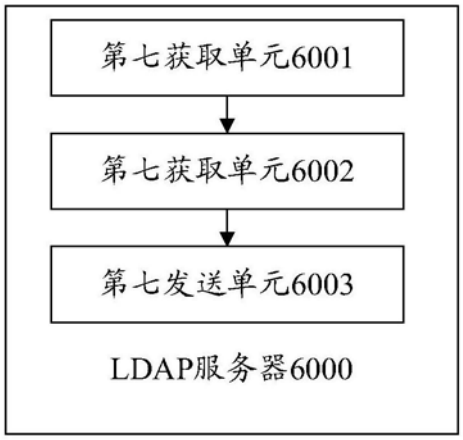

第七获取单元6001
第七获取单元6002
第七发送单元6003
LDAP服务器6000

图16

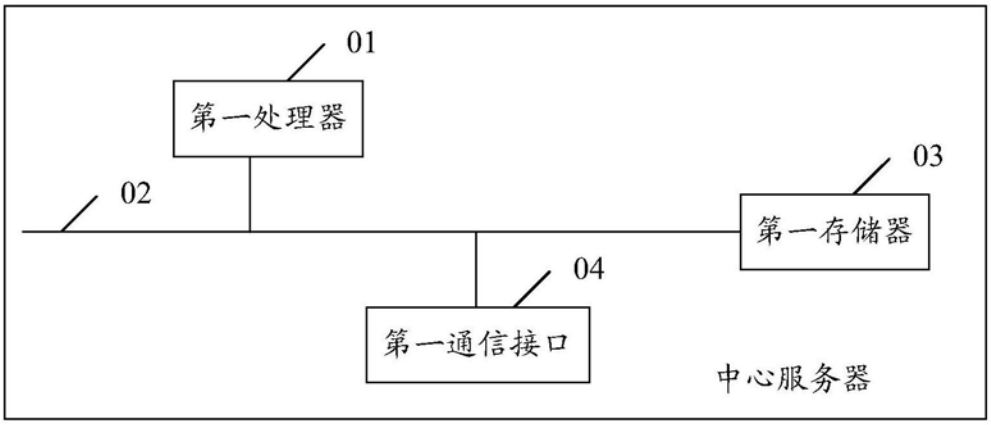

01
第一处理器
02
03
第一存储器
04
第一通信接口
中心服务器

图17

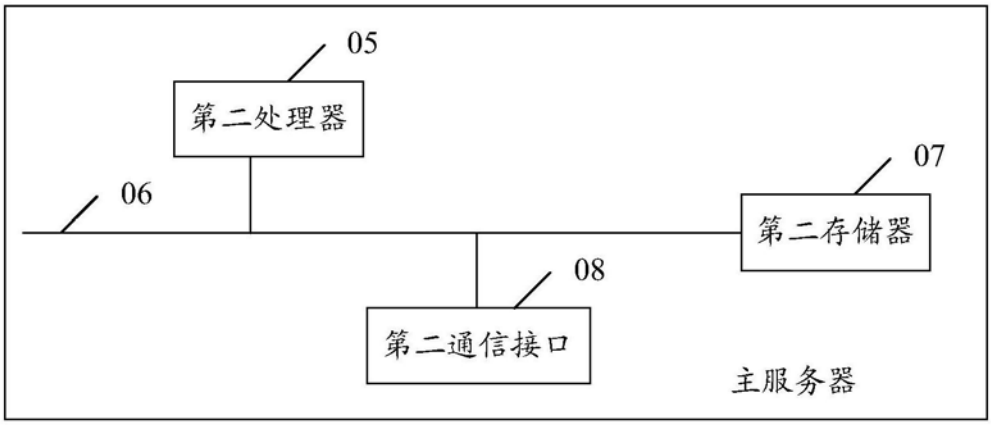

05
第二处理器
06
07
第二存储器
08
第二通信接口
主服务器

图18

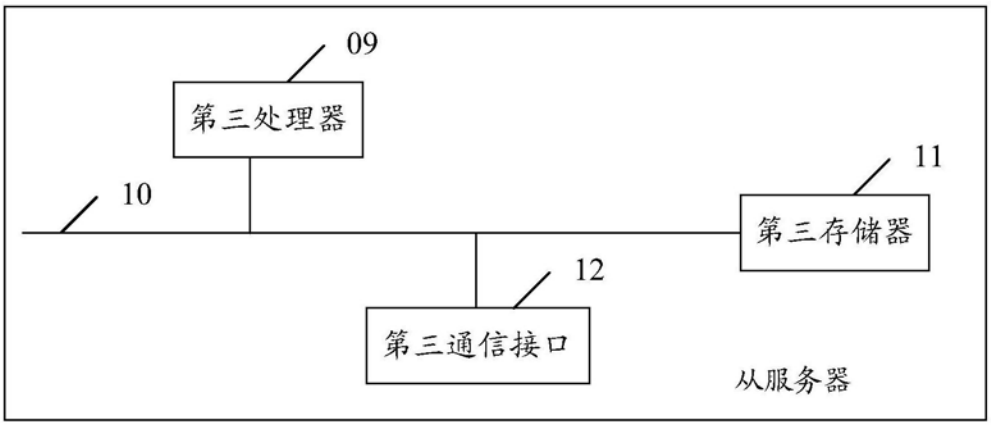

09
第三处理器
10
11
第三存储器
12
第三通信接口
从服务器

图19

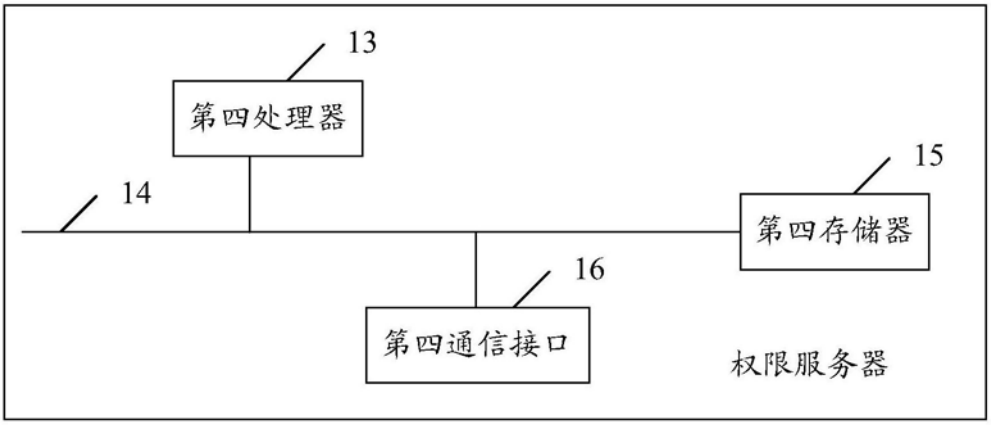

13
第四处理器
14
15
第四存储器
16
第四通信接口
权限服务器

图20

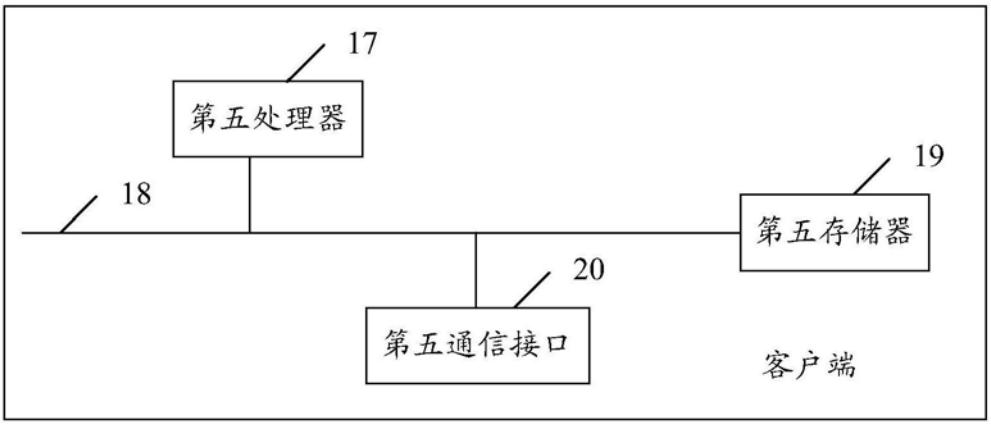

17
第五处理器
18
19
第五存储器
20
第五通信接口
客户端

图21

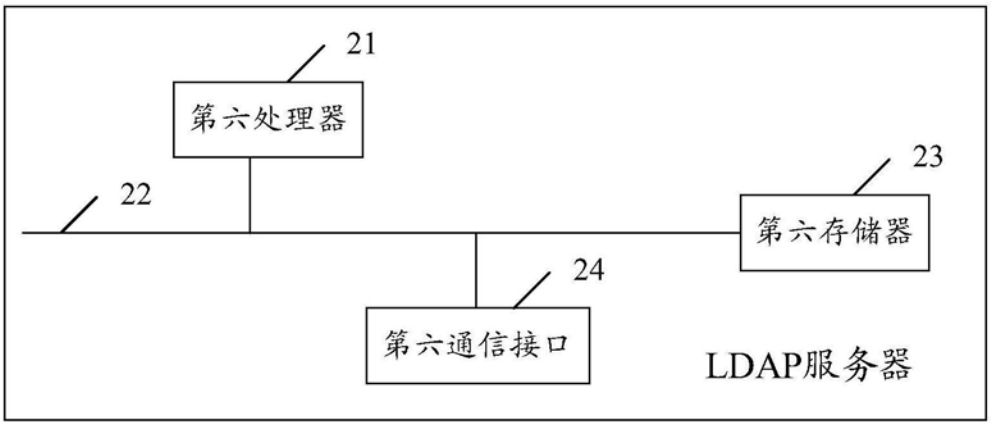


图22