**专利名称：一种基于双线性映射和点积协议的认证方案**

**申请人 ：南京邮电大学**

**发明人：柯昌博、朱泽江**

**第一发明人身份证号：**

本发明公开了一种基于双线性映射和点积协议的认证方案，解决了智能医疗环境中不同功能实体之间的可信计算问题，以保证患者用户在发生紧急情况时得到安全有效的雾计算服务。本发明的认证方案针对雾计算环境中用户的隐私保护设计了具有两阶段的认证模型，其中第一阶段的身份认证利用椭圆曲线和双线性对技术来帮助用户有效地识别出环境中的可信雾节点，同时能够拦截外部伪装节点的攻击以降低用户隐私数据泄露的风险。第二阶段的属性认证能够在用户终端和雾节点主机不相互暴露功能属性的条件下，让用户快速找到满足其功能需求的雾节点主机，同时通过简化功能属性向量来降低终端设备在认证过程中的计算开销。本发明通过两阶段的认证过程，在保证用户隐私安全的前提下，满足了用户不同的功能需求。



1.一种基于双线性映射和点积协议的认证方案，包括以下步骤：

步骤 1）系统初始化，本发明通过第三方可信中心TC来管理和引导整个系统的运行，首先选取三个阶数为*q*的乘法循环群和用以构造双线性对。同时引入JPBC函数库，调用函数来生成系统参数，之后将系统参数发送给所有经过注册的用户智能终端和雾节点设备。

步骤 2）设备注册，用户将自己设置的身份和密码发送给可信中心TC，TC接收到后在用户信息表中添加用户的身份信息并计算其加密私钥，并将私钥和系统参数返回给用户。雾节点将自己的唯一身份(如物理MAC地址)发送给可信中心TC，TC接收到后在雾节点信息表中添加雾节点的身份信息并计算其访问控制秘钥。

步骤 3）身份认证，用户用私钥来加密系统参数中的双线性映射结果，同时计算自己的身份认证凭证，然后用户将发送给等待认证的雾节点。在接收到消息后使用控制秘钥还原出映射结果并结合当前的时间戳进行加密，然后将加密后结果和时间戳返回给用户。用户在时间戳为接收到消息后，计算和之间的差值，如果差值不在预期的传输延迟范围内则拒收该认证消息，否则利用本地存储的映射结果和接收到的结果进行比较。如果两者相等则雾节点被认为通过身份认证，否则认证失败。

步骤 4）属性认证，将用户和雾节点的功能属性通过二进制向量的形式表示。用户定义一个阈值来表示两者功能属性期待相同的数量，之后对用户和雾节点的每个向量元素通过点积协议进行计算。如果点积运算的返回值，雾节点则被认为通过功能属性认证并能接收用户发送的隐私数据。

其中所述步骤1）具体如下：

步骤11）可信中心TC选取一个安全参数*C*，通过运行生成器生成双线性参数*,,G,,*，其中*G*和均为循环群，为循环群*G*的阶数，为循环群*G*的生成元，示一种映射关系。

步骤 12）选择一个安全的加密哈希函数*Hash:*，此外再选择两个随机的数字作为主秘钥，以及群*G*中的随机元素，并计算，，其中元素是注册用户的认证参数，是群*G*中生成元在群上的映射结果。然后TC发布系统参数。

所述步骤 2）具体如下：

步骤21）用户设置自己的唯一身份和密码，同时生成一个随机数，计算密码密文。之后将注册信息发送给可信中心TC。可信中心TC接收到注册请求后，首先会检查是否存在于用户信息表中。如果不存在，则计算用户的加密私钥，并初始化用户的功能属性向量，之后将和系统参数返回给用户。若存在，则可信中心将拒绝该注册请求。

步骤 22）雾节点将自己的唯一身份(如物理MAC地址)发送给可信中心TC。可信中心TC接收到注册请求后，首先会检查是否存在于雾节点信息表中，如果不存在，则在表中记录该设备信息并初始化雾节点的功能属性向量，同时选择随机数，计算雾节点的加密私钥，访问控制密钥，其中,,，之后将访问控制密钥和返回给雾节点。若存在，则可信中心将拒绝该注册请求。

所述步骤 3）具体如下：

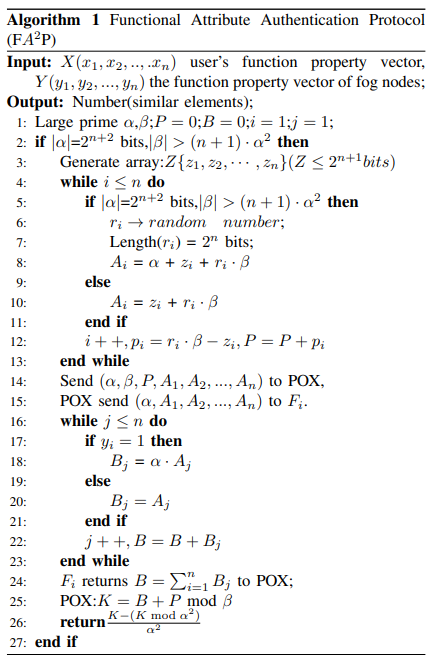
步骤 31）用户首先利用本地存储的加密私钥分别计算映射结果和身份凭证。然后用户将身份凭证发送给等待认证的雾节点，在接收到身份凭证后雾节点使用它的访问控制秘钥，计算

步骤 32）雾节点计算完成后得到结果，并结合当前的时间戳以的形式返回给用户。假设用户在时间戳为时接收到，为避免重试攻击，用户会检查这两个时间戳之间的时差。如果（表示预期的有效传输时间间隔），用户便会接收，否则拒绝。一旦被接收成功后，用户利用待认证雾节点的身份计算，然后比较是否等于，如果相等，则该雾节点通过身份认证并被认为是一个可信的节点。

所述步骤 4）具体如下：

步骤 41）用户的功能属性向量抽象为，待认证雾节点的功能属性向量抽象为，其中元素0代表不具备该功能，元素1代表具备该功能。

步骤 42）首先用户选取两个大质数，并初始化参数。如果大质数满足的长度等于位，的长度大于，则生成一个随机长度不大于位的数组Z。同时对用户的属性向量进行遍历，如果向量中元素等于1，则随机选取一个长度为位的随机数，并计算，否则计算，对每次遍历都需要计算，。最后用户将消息发送给POX控制器，POX控制器接收到后将*P*和存储在本地并将转发给雾节点。雾节点接收到后对属性向量进行遍历，如果向量中元素等于1，则计算，否则计算。遍历完成后，雾节点将所有之和*B*返回给POX，POX利用接收到的*B*和本地的*P*，计算，最后的结果就是用户和雾节点相同的属性个数。之后用户将点积结果和阈值进行比较，如果则认为该雾节点无法满足用户的功能需求，认证失败；否则认证成功。该步骤的代码如下所示：



**一种基于双线性映射和点积协议的两阶段认证方案**

**技术领域**

本发明提出一种在智能医疗中基于双线性映射和点积协议的两阶段认证方案，属于边缘计算、隐私安全和身份认证等交叉技术领域。

**背景技术**

随着2011年思科首次提出雾计算的架构，用户逐渐将数据从传统的云计算数据中心迁移到部署距离更近的雾节点设备上，以此提高数据分析与处理效率，减少网络传输压力。雾计算作为一种新型的计算范式，可以通过部署智能医疗保障系统为患者提供更高效、高质量的医疗服务。智能医疗需要在雾节点中存储和共享患者的生理数据，以便进行在线诊断。但是，如果智能医疗的雾节点缺乏有效的安全机制，用户的隐私数据可能会被恶意用户窃取。此外，雾计算还会面临一些全新的挑战，如物联网中的移动终端计算和存储资源受限以及敌手的内部攻击。为防止用户数据在网络传输过程中发生隐私泄漏问题的安全认证方案是雾计算领域中的一个重要研究课题，具有重要的理论意义与实际应用价值。

目前国内外研究者对雾计算认证协议的研究大多是在现有的安全协议基础上进行改进和优化，包括协议的灵活性、高效性、节能性和隐私保护等。其中主要的技术原理包括椭圆曲线加密、双线性映射和点积协议。

椭圆曲线密码系统和双线性映射技术可以构造基于身份认证的秘钥管理机制，通过可信中心(TC)发布全局系统参数并计算系统内雾节点的访问控制秘钥，用户和雾节点利用系统参数和访问控制秘钥计算或还原相应的结果来完成身份认证。身份认证是雾计算中保护用户数据和隐私安全的基础，在雾计算中通常包含多个功能实体，比如用户的智能移动终端、便携式传感器以及提供计算服务的虚拟化雾节点等，为确保这些功能实体的真实可信性，需要为每个实体分配身份证书用于可信验证。

通过点积协议可以设计满足用户功能需求的属性认证方案，利用可信中心(TC)对用户和雾节点的功能属性进行初始化，使得每个用户和雾节点都拥有自己固定的功能属性，然后通过点积运算可以得出用户和雾节点相似属性的数量，从而用户能够找到符合自己功能需求的雾节点。属性认证能够很好地适用于雾计算的分布式架构，实现细粒度数据共享和访问控制。

基于上述研究成果，本发明针对智能医疗中患者用户的隐私保护问题，提出一种基于双线性映射和点积协议的两阶段认证方案，旨在帮助用户得到安全可靠的雾计算服务。

**发明内容**

**技术问题：**发明所要解决的技术问题是设计一种同时满足用户隐私安全需求和功能需求的两阶段认证方案，以有效地降低雾计算中隐私数据在传输过程中的泄露风险。

**技术方案：**本发明的一种基于双线性映射和点积协议的两阶段认证方案包括以下步骤：

步骤 1）系统初始化，本发明通过第三方可信中心TC来管理和引导整个系统的运行，首先选取三个阶数为*q*的乘法循环群和用以构造双线性对。同时引入JPBC函数库，调用函数来生成系统参数，之后将系统参数发送给所有经过注册的用户智能终端和雾节点设备。

步骤 2）设备注册，用户将自己设置的身份和密码发送给可信中心TC，TC接收到后在用户信息表中添加用户的身份信息并计算其加密私钥，并将私钥和系统参数返回给用户。雾节点将自己的唯一身份(如物理MAC地址)发送给可信中心TC，TC接收到后在雾节点信息表中添加雾节点的身份信息并计算其访问控制秘钥。

步骤 3）身份认证，用户用私钥来加密系统参数中的双线性映射结果，同时计算自己的身份认证凭证，然后用户将发送给等待认证的雾节点。在接收到消息后使用控制秘钥还原出映射结果并结合当前的时间戳进行加密，然后将加密后结果和时间戳返回给用户。用户在时间戳为接收到消息后，计算和之间的差值，如果差值不在预期的传输延迟范围内则拒收该认证消息，否则利用本地存储的映射结果和接收到的结果进行比较。如果两者相等则雾节点被认为通过身份认证，否则认证失败。

步骤 4）属性认证，将用户和雾节点的功能属性通过二进制向量的形式表示。用户定义一个阈值来表示两者功能属性期待相同的数量，之后对用户和雾节点的每个向量元素通过点积协议进行计算。如果点积运算的返回值，雾节点则被认为通过功能属性认证并能接收用户发送的隐私数据。

其中所述步骤1）具体如下：

步骤11）可信中心TC选取一个安全参数*C*，通过运行生成器生成双线性参数*,,G,,*，其中*G*和均为循环群，为循环群*G*的阶数，为循环群*G*的生成元，示一种映射关系。

步骤 12）选择一个安全的加密哈希函数*Hash:*，此外再选择两个随机的数字作为主秘钥，以及群*G*中的随机元素，并计算，，其中元素是注册用户的认证参数，是群*G*中生成元在群上的映射结果。然后TC发布系统参数。

所述步骤 2）具体如下：

步骤21）用户设置自己的唯一身份和密码，同时生成一个随机数，计算密码密文。之后将注册信息发送给可信中心TC。可信中心TC接收到注册请求后，首先会检查是否存在于用户信息表中。如果不存在，则计算用户的加密私钥，并初始化用户的功能属性向量，之后将和系统参数返回给用户。若存在，则可信中心将拒绝该注册请求。

步骤 22）雾节点将自己的唯一身份(如物理MAC地址)发送给可信中心TC。可信中心TC接收到注册请求后，首先会检查是否存在于雾节点信息表中，如果不存在，则在表中记录该设备信息并初始化雾节点的功能属性向量，同时选择随机数，计算雾节点的加密私钥，访问控制密钥，其中,,，之后将访问控制密钥和返回给雾节点。若存在，则可信中心将拒绝该注册请求。

所述步骤 3）具体如下：

步骤 31）用户首先利用本地存储的加密私钥分别计算映射结果和身份凭证。然后用户将身份凭证发送给等待认证的雾节点，在接收到身份凭证后雾节点使用它的访问控制秘钥，计算

步骤 32）雾节点计算完成后得到结果，并结合当前的时间戳以的形式返回给用户。假设用户在时间戳为时接收到，为避免重试攻击，用户会检查这两个时间戳之间的时差。如果（表示预期的有效传输时间间隔），用户便会接收，否则拒绝。一旦被接收成功后，用户利用待认证雾节点的身份计算，然后比较是否等于，如果相等，则该雾节点通过身份认证并被认为是一个可信的节点。

所述步骤 4）具体如下：

步骤 41）用户的功能属性向量抽象为，待认证雾节点的功能属性向量抽象为，其中元素0代表不具备该功能，元素1代表具备该功能。

步骤 42）首先用户选取两个大质数，并初始化参数。如果大质数满足的长度等于位，的长度大于，则生成一个随机长度不大于位的数组Z。同时对用户的属性向量进行遍历，如果向量中元素等于1，则随机选取一个长度为位的随机数，并计算，否则计算，对每次遍历都需要计算，。最后用户将消息发送给POX控制器，POX控制器接收到后将*P*和存储在本地并将转发给雾节点。雾节点接收到后对属性向量进行遍历，如果向量中元素等于1，则计算，否则计算。遍历完成后，雾节点将所有之和*B*返回给POX，POX利用接收到的*B*和本地的*P*，计算，最后的结果就是用户和雾节点相同的属性个数。之后用户将点积结果和阈值进行比较，如果则认为该雾节点无法满足用户的功能需求，认证失败；否则认证成功。

**有益效果：**本发明采用的以上技术方案与现有技术相比，具有以下技术效果：

本发明在兼顾用户隐私安全的同时还能够让用户根据自身的功能需求来认证所需的雾节点，用户可以通过动态调节阈值的大小来改变认证结果。例如当用户在某一阈值下认证成功雾节点的数量较多时，可以适当增加当前阈值的大小来减少通过认证的雾节点数量，以达到降低隐私数据泄露风险的目的。当用户认证成功雾节点的数量较少并无法满足当前的计算需求时，可以减小当前阈值的大小来保证雾计算的可靠性。此外还通过哈希加密、时间戳等技术手段来保证消息在传输过程中的安全，具体来说：

1. 本发明利用椭圆曲线和双线性映射技术设计身份认证方案，使得用户在认证完雾节点后想要继续向其他雾节点发起认证，无需重复计算元组，只需重新生成时间戳就能进行认证，减少了认证时的计算开销。
2. 本发明通过时间戳和哈希函数对每条认证消息进行加密，可以有效得阻拦重试攻击。
3. 本发明将用户和雾节点的功能属性抽象成二进制向量的形式，相比传统的点积协议简化了繁琐的模幂运算，降低了用户智能终端的资源消耗。
4. 本发明允许用户根据实际需求来改变阈值的大小，提升了认证的灵活性。

**附图说明**

图1是本认证方案所运用的实际场景。

图2是基于椭圆曲线和点积协议的认证方法流程。

### 具体实施方式

下面结合附图对本发明的技术方案做进一步的详细说明：

在具体实施中，图1是本认证方案所运用的实际场景。在智能医疗领域中，用户通过各种可穿戴设备收集包括血压、心率、体温、代谢等医疗数据，然后使用蓝牙传输给智能终端进行计算分析用户的健康状况。一旦用户智能终端的计算资源被大量占用，不能及时对医疗数据进行计算，以至于用户在发生紧急病况时无法向医疗中心发出预警信息。在该情况下，用户需要将自己的隐私数据发送给附近的雾节点，利用边缘计算来均衡智能终端的计算负载，与此同时用户希望自己的隐私数据在不被泄露的同时能够满足相应的功能需求。因此用户需要通过身份认证和功能属性认证来获取安全可信且满足功能需求的雾计算服务。

图2是本专利的认证流程图，假设用户首先在智能终端中设置自己的身份和密码进行注册，可信中心TC接收到注册请求后，利用系统参数计算相应的加密私钥并将私钥和系统参数返回给用户。注册完成后，用户利用自己的私钥对系统参数中的映射结果进行加密，计算。之后生成自己的身份凭证，计算。然后用户将身份凭证发送给等待认证的雾节点，雾节点接收到后使用访问控制秘钥还原出映射结果，并利用自己的私钥对映射结果进行加密，计算用于身份认证的认证令牌返回给用户。用户接收到认证令牌后，首先通过系统参数中的哈希函数和待认证雾节点的身份计算出，然后计算来还原出雾节点所计算出来的映射结果，最后比较是否等于,如果相等,则该雾节点通过身份认证。

通过身份认证后用户初始化自己的属性向量，并设置期待的属性相似阈值，假设待认证雾节点的属性向量为。用户首先计算.接着雾节点计算.之后可以被用户计算出来：

因为,所以

所以可以去除对的取模运算：

又因为,所以

最后用户将阈值和点积结果进行比较，如果阈值小于等于点积结果则该雾节点通过属性认证，否则将认证失败。



图1 认证场景



图2 认证流程