(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 114422266 A
(43)申请公布日 2022.04.29

(21)申请号 202210196762.8

(22)申请日 2022.02.28

(71)申请人 深圳市中悦科技有限公司
地址 518040 广东省深圳市龙岗区吉华街道甘坑社区甘李二路11号中海信创新产业城19栋1307、1308

(72)发明人 周文明 王志鹏

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/30(2006.01)
H04L 67/60(2022.01)

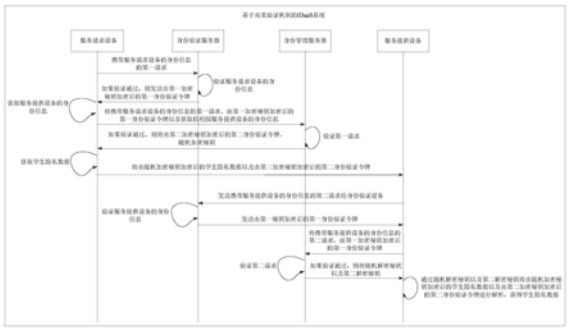
权利要求书4页 说明书11页 附图3页

(54)发明名称

一种基于双重验证机制的IDaaS系统

(57)摘要

本申请公开一种基于双重验证机制的IDaaS系统，包括：服务请求设备、身份验证服务器、身份管理服务器及服务提供设备；服务请求设备将携带自身身份信息的第一请求发送给身份验证服务器后，身份信息经身份验证服务器验证后，如果接收的第一身份验证令牌通过身份管理服务器验证，则接收身份管理服务器发送的随机加密秘钥。服务提供设备接收由随机加密秘钥加密的学生隐私数据后，发送携带自身设备身份信息的第二请求给身份验证服务器后，接收第一身份验证令牌及第二请求，第二请求经身份管理服务器验证后，接收到随机解密秘钥，对上述加密数据解析以恢复出学生隐私数据。采用本申请，可抵制身份认证攻击，提高IDaaS系统的安全性。



CN 114422266 A

1.一种基于双重验证机制的IDaaS系统,其特征在于,包括:

服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备;所述服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备之间通过网络连接;其中,

所述服务请求设备用于:将携带所述服务请求设备的身份信息的第一请求发送给所述身份验证服务器;

所述身份验证服务器用于:验证所述服务请求设备的身份信息,如果验证通过,则发送由第一加密秘钥加密后的第一身份验证令牌给所述服务请求设备;所述第一身份验证令牌用于:所述身份管理服务器将所述服务请求设备验证为合法与所述身份管理服务器进行通信的已授权设备;

所述服务请求设备还用于:将所述第一请求、所述由第一加密秘钥加密后的第一身份验证令牌以及获取的所述服务提供设备的身份信息发送给所述身份管理服务器;

所述身份管理服务器用于:验证所述第一请求,如果验证通过,则将由第二加密秘钥加密后的第二身份验证令牌、随机加密秘钥发送给所述服务请求设备;

所述服务请求设备还用于:将由所述随机加密秘钥加密后的学生隐私数据以及所述由第二加密秘钥加密后的第二身份验证令牌给所述服务提供设备;所述第二身份验证令牌用于:所述服务请求服务设备与所述服务提供设备进行通信;所述服务提供设备用于:响应于接收到所述学生隐私数据以及所述第二身份验证令牌,发送携带所述服务提供设备的身份信息的第二请求给所述身份验证服务器;

所述身份验证服务器还用于:验证所述服务提供设备的身份信息,如果验证通过,则将由所述第一加密秘钥加密后的所述第一身份验证令牌发送给所述服务提供设备;

所述服务提供设备还用于:将所述携带所述服务提供设备的身份信息的所述第二请求、所述由第一加密秘钥加密后的所述第一身份验证令牌发送给所述身份管理服务器;

所述身份管理服务器还用于:验证所述第二请求,如果验证通过,则将随机解密秘钥以及第二解密秘钥发送给所述服务提供设备;

所述服务提供设备用于:通过所述随机解密秘钥以及所述第二解密秘钥将所述由所述随机加密秘钥加密后的学生隐私数据以及所述由第二加密秘钥加密后的第二身份验证令牌进行解析,以获得所述学生隐私数据;其中,所述第二加密秘钥和所述第二解密秘钥为一对秘钥,所述随机加密秘钥和所述随机解密秘钥为一对秘钥。

2.如权利要求1所述基于双重验证机制的IDaaS系统,其特征在于,

所述第一请求用于:所述服务请求设备请求所述身份验证服务器和所述身份管理服务器提供验证令牌以实现所述服务请求设备与所述服务提供设备进行通信;

所述身份验证服务器具体用于:验证所述服务请求设备的身份信息,如果验证通过,则将由第一加密秘钥加密后的第一身份验证令牌以及获取的第一时间戳发送给所述服务请求设备;其中,所述第一加密秘钥为所述身份验证服务器与所述身份管理服务器之间的加密秘钥;所述第一时间戳为所述服务请求设备与所述身份验证服务器之间的时间戳;所述第一时间戳用于指示出所述身份验证服务器生成所述第一加密秘钥、所述第一身份验证令牌以及通过所述第一加密秘钥加密所述第一身份验证令牌的时间点;

所述服务请求设备具体还用于:将所述携带所述服务请求设备的身份信息的第一请求、所述由第一加密秘钥加密后的第一身份验证令牌、所述服务提供设备的身份信息以及

所述服务请求设备生成的第二时间戳发送给所述身份管理服务器;所述第二时间戳用于指示出所述由第一加密秘钥加密后的第一身份验证令牌、所述服务提供设备的身份信息的获取时间点;

所述身份管理服务器具体用于:验证所述第一请求是否为合法的已授权的设备所发送,如果验证通过,则将由第二加密秘钥加密后的第二身份验证令牌、随机加密秘钥、第三时间戳以及所述服务提供设备的身份信息发送给所述服务请求设备;其中,所述第二加密秘钥为所述服务请求设备与所述身份管理服务器之间的加密秘钥;所述随机加密秘钥为所述服务请求设备与所述服务提供设备之间的加密秘钥;所述第三时间戳用于指示出所述身份管理服务器生成所述第二加密秘钥以及所述第二身份验证令牌的时间点;

所述身份验证服务器具体用于:验证所述服务提供设备的身份信息,如果验证通过,则发送由所述第一加密秘钥加密后的所述第一身份验证令牌、获取的第四时间戳以及所述服务提供设备的用户身份信息给所述服务提供设备;所述第四时间戳用于指示出所述身份验证服务器生成所述第一加密秘钥、所述第一身份验证令牌以及通过所述第一加密秘钥加密所述第一身份验证令牌的时间点;

所述服务提供设备还用于:将所述携带所述服务提供设备的身份信息的第二请求、所述由第一加密秘钥加密后的所述第一身份验证令牌、所述服务请求设备的身份信息以及获取的第五时间戳发送给所述身份管理服务器;所述第五时间戳用于指示出第一加密秘钥加密后的所述第一身份验证令牌、所述服务请求设备的身份信息的获取时间点;

所述身份管理服务器具体还用于:验证所述第二请求,如果验证通过,则将所述随机解密秘钥、所述第二解密秘钥及第六时间戳发送给所述服务提供设备;所述第六时间戳用于指示出随机解密秘钥以及所述第二解密秘钥的生成时间点;

所述服务提供设备具体用于:通过所述随机解密秘钥以及所述第二解密秘钥将所述由所述随机加密秘钥加密后的学生隐私数据以及所述由第二加密秘钥加密后的第二身份验证令牌进行解析,获得所述学生隐私数据。

3.如权利要求2所述基于双重验证机制的IDaaS系统,其特征在于,

所述服务请求设备,具体用于:

将携带所述服务请求设备的身份信息ID的第一请求$Request_1$发送给所述身份验证服务器;或者,

所述身份验证服务器,具体用于:

验证所述服务请求设备的身份信息ID_A,如果验证通过,则将由第一加密秘钥$E_{k(AS-IDS)}$加密后的第一身份验证令牌$E_{k(AS-IDS)}(Token_1)$、获取的第一时间戳T_1以及所述服务请求设备的身份信息ID_A发送给所述服务请求设备。

4.如权利要求3所述基于双重验证机制的IDaaS系统,其特征在于,

所述服务请求设备具体还用于:

将所述携带所述服务请求设备的身份信息ID_A的第一请求$Request_1$、所述由第一加密秘钥$E_{k(AS-IDS)}$加密后的第一身份验证令牌$E_{k(AS-IDS)}(Token_1)$、所述服务提供设备的身份信息ID_B以及所述服务请求设备生成的第二时间戳T_2发送给所述身份管理服务器;或者,

所述身份管理服务器具体用于:

验证所述第一请求$Request_1$是否为合法的已授权的设备所发送,如果验证通过,则将由

第二加密秘钥$E_{K\text{-}SAML(IDS\text{-}B)}$加密后的第二身份验证令牌$E_{K\text{-}SAML(IDS\text{-}B)}(Token_2)$、随机加密秘钥$E_{RK(A\text{-}B)}$、第三时间戳$T_3$、所述服务请求设备的身份信息$ID_A$以及所述服务提供设备的身份信息$ID_B$发送给所述服务请求设备。

5.如权利要求4所述基于双重验证机制的IDaaS系统,其特征在于,

所述服务请求设备具体还用于:

将由随机加密秘钥$RK_{(A\text{-}B)}$加密后的学生隐私数据Msg以及所述由第二加密秘钥$E_{K\text{-}SAML(IDS\text{-}B)}$加密后的第二身份验证令牌$E_{K\text{-}SAML(IDS\text{-}B)}(Token_2)$给所述服务提供设备;其中,所述第二加密秘钥$E_{K\text{-}SAML(IDS\text{-}B)}$基于SAML协议所生成;

所述服务提供设备具体用于:

响应于接收到所述学生隐私数据Msg以及所述由第二加密秘钥$E_{K\text{-}SAML(IDS\text{-}B)}$加密后的第二身份验证令牌$E_{K\text{-}SAML(IDS\text{-}B)}(Token_2)$,发送携带所述服务提供设备的身份信息$ID_B$的第二请求$Request_2$给所述身份验证服务器;

所述身份验证服务器,具体还用于:

验证所述服务提供设备的身份信息ID_B,如果验证通过,则将由所述第一加密秘钥$E_{k(AS\text{-}IDS)}$加密后的所述第一身份验证令牌$E_{k(AS\text{-}IDS)}(Token_1)$、获取的第四时间戳$T_4$以及所述服务提供设备的用户身份信息$ID_B$发送给所述服务提供设备;

所述服务提供设备具体还用于:

将所述携带所述服务提供设备的身份信息ID_B的第二请求$Request_2$、所述由第一加密秘钥$E_{k(AS\text{-}IDS)}$加密后的所述第一身份验证令牌$E_{k(AS\text{-}IDS)}(Token_1)$、所述服务请求设备的身份信息$ID_A$以及获取的第五时间戳$T_5$发送给所述身份管理服务器;

所述身份管理服务器具体还用于:

验证所述第二请求$Request_2$,如果验证通过,则将随机解密秘钥RK(A-B)以及所述第二解密秘钥K-SAML(IDS-B)发送给所述服务提供设备;所述第二解密秘钥K-SAML(IDS-B)基于SAML协议所生成;

所述服务提供设备具体还用于:

通过所述随机解密秘钥RK(A-B)以及所述第二解密秘钥K-SAML(IDS-B)将所述由所述随机加密秘钥$E_{RK(A\text{-}B)}$加密后的学生隐私数据$E_{RK(A\text{-}B)}(Msg)$以及所述由第二加密秘钥$E_{K\text{-}SAML(IDS\text{-}B)}$加密后的第二身份验证令牌$E_{K\text{-}SAML(IDS\text{-}B)}(Token_2)$进行解析,获得所述学生隐私数据Msg。

6.如权利要求5所述基于双重验证机制的IDaaS系统,其特征在于,

所述服务请求设备、所述身份验证服务器以及所述身份管理服务器被部署在雾计算环境中,所述服务提供设备被部署在云计算环境中;

或者,

所述服务请求设备、所述身份验证服务器部署在所述雾计算环境中,所述身份管理服务器以及所述服务提供设备被部署在所述云计算环境中。

7.如权利要求5所述基于双重验证机制的IDaaS系统,其特征在于,

所述身份管理服务器具体还用于:

在将由第二加密秘钥$E_{K\text{-}SAML(IDS\text{-}B)}$加密后的第二身份验证令牌$E_{K\text{-}SAML(IDS\text{-}B)}(Token_2)$、随机加密秘钥$E_{RK(A\text{-}B)}$、第三时间戳$T_3$、所述服务请求设备的身份信息$ID_A$以及所述服务提供设

备的身份信息ID_B发送给所述服务请求设备之前，

通过椭圆曲线密码算法生成所述随机加密秘钥E_{RK}(A-B)。

8.如权利要求5所述基于双重验证机制的IDaaS系统，其特征在于，

所述身份管理服务器具体还用于：

在将随机解密秘钥RK(A-B)以及所述第二解密秘钥K-SAML(IDS-B)发送给所述服务提供设备之前，

通过椭圆曲线密码算法生成所述随机解密秘钥RK(A-B)。

9.如权利要求1所述基于双重验证机制的IDaaS系统，其特征在于，

所述身份验证服务器具体用于：

验证所述服务请求设备的身份信息在所述身份验证服务器的本地数据库或所述身份验证服务器的内存中是否存在，如果存在，则确定出所述服务请求设备的身份信息获得验证通过；

或者，

所述身份验证服务器具体用于：

验证所述服务提供设备的身份信息在所述身份验证服务器的本地数据库或所述身份验证服务器的内存中是否存在，如果存在，则确定出所述服务提供设备的身份信息获得验证通过。

10.如权利要求1所述基于双重验证机制的IDaaS系统，其特征在于，

所述身份管理服务器具体用于：

对由第一加密秘钥加密后的第一身份验证令牌解密，根据获得的所述第一身份验证令牌，以验证出所述服务请求设备为合法与所述身份管理服务器进行通信的已授权设备、所述第一请求真实为所述服务请求设备所发送；

或者，

所述身份管理服务器具体用于：

对由第一加密秘钥加密后的所述第一身份验证令牌解密，根据获得的所述第一身份验证令牌，以验证出所述服务提供设备为合法与所述身份管理服务器进行通信的已授权设备、所述第二请求真实为所述服务提供设备所发送。

一种基于双重验证机制的IDaaS系统

技术领域

[0001] 本申请涉及信息安全技术领域，尤其涉及一种基于双重验证机制的IDaaS 系统。

背景技术

[0002] 智慧校园成为当前校园信息化发展的新趋势。然而，在智慧校园管理系统的建设探索中面临诸多信息安全问题，具体如在智慧校园管理系统建设过程中，经常遭遇到伪造攻击、身份盗窃攻击和身份认证攻击等问题。

发明内容

[0003] 基于以上存在的问题以及现有技术的缺陷，本申请提供一种基于双重验证机制的IDaaS系统，采用本申请，通过采用身份验证服务器以及身份管理服务器对通信设备的身份信息进行双重验证，以抵制身份认证攻击或者身份盗窃攻击等，可提高IDaaS系统中的数据安全性。

[0004] 第一方面，本申请提供了一种基于双重验证机制的IDaaS系统，该系统包括：

[0005] 服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备；所述服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备之间通过网络连接；其中，

[0006] 所述服务请求设备用于：将携带所述服务请求设备的身份信息的第一请求发送给所述身份验证服务器；

[0007] 所述身份验证服务器用于：验证所述服务请求设备的身份信息，如果验证通过，则发送由第一加密秘钥加密后的第一身份验证令牌给所述服务请求设备；所述第一身份验证令牌用于：所述身份管理服务器将所述服务请求设备验证为合法与所述身份管理服务器进行通信的已授权设备；

[0008] 所述服务请求设备还用于：将所述第一请求、所述由第一加密秘钥加密后的第一身份验证令牌以及获取的所述服务提供设备的身份信息发送给所述身份管理服务器；

[0009] 所述身份管理服务器用于：验证所述第一请求，如果验证通过，则将由第二加密秘钥加密后的第二身份验证令牌、随机加密秘钥发送给所述服务请求设备；

[0010] 所述服务请求设备还用于：将由所述随机加密秘钥加密后的学生隐私数据以及所述由第二加密秘钥加密后的第二身份验证令牌给所述服务提供设备；所述第二身份验证令牌用于：所述服务请求服务设备与所述服务提供设备进行通信；所述服务提供设备用于：响应于接收到所述学生隐私数据以及所述第二身份验证令牌，发送携带所述服务提供设备的身份信息的第二请求给所述身份验证服务器；

[0011] 所述身份验证服务器还用于：验证所述服务提供设备的身份信息，如果验证通过，则将由所述第一加密秘钥加密后的所述第一身份验证令牌发送给所述服务提供设备；

[0012] 所述服务提供设备还用于：将所述携带所述服务提供设备的身份信息的所述第二请求、所述由第一加密秘钥加密后的所述第一身份验证令牌发送给所述身份管理服务器；

[0013] 所述身份管理服务器还用于：验证所述第二请求，如果验证通过，则将随机解密秘

钥以及第二解密秘钥发送给所述服务提供设备；

[0014] 所述服务提供设备用于：通过所述随机解密秘钥以及所述第二解密秘钥将所述由所述随机加密秘钥加密后的学生隐私数据以及所述由第二加密秘钥加密后的第二身份验证令牌进行解析，以获得所述学生隐私数据；其中，所述第二加密秘钥和所述第二解密秘钥为一对秘钥，所述随机加密秘钥和所述随机解密秘钥为一对秘钥。

[0015] 结合第一方面，在一些可选的实施例中，

[0016] 所述第一请求用于：所述服务请求设备请求所述身份验证服务器和所述身份管理服务器提供验证令牌以实现所述服务请求设备与所述服务提供设备进行通信；

[0017] 所述身份验证服务器具体用于：验证所述服务请求设备的身份信息，如果验证通过，则将由第一加密秘钥加密后的第一身份验证令牌以及获取的第一时间戳发送给所述服务请求设备；其中，所述第一加密秘钥为所述身份验证服务器与所述身份管理服务器之间的加密秘钥；所述第一时间戳为所述服务请求设备与所述身份验证服务器之间的时间戳；所述第一时间戳用于指示出所述身份验证服务器生成所述第一加密秘钥、所述第一身份验证令牌以及通过所述第一加密秘钥加密所述第一身份验证令牌的时间点；

[0018] 所述服务请求设备具体还用于：将所述携带所述服务请求设备的身份信息的第一请求、所述由第一加密秘钥加密后的第一身份验证令牌、所述服务提供设备的身份信息以及所述服务请求设备生成的第二时间戳发送给所述身份管理服务器；所述第二时间戳用于指示出所述由第一加密秘钥加密后的第一身份验证令牌、所述服务提供设备的身份信息的获取时间点；

[0019] 所述身份管理服务器具体用于：验证所述第一请求是否为合法的已授权的设备所发送，如果验证通过，则将由第二加密秘钥加密后的第二身份验证令牌、随机加密秘钥、第三时间戳以及所述服务提供设备的身份信息发送给所述服务请求设备；其中，所述第二加密秘钥为所述服务请求设备与所述身份管理服务器之间的加密秘钥；所述随机加密秘钥为所述服务请求设备与所述服务提供设备之间的加密秘钥；所述第三时间戳用于指示出所述身份管理服务器生成所述第二加密秘钥以及所述第二身份验证令牌的时间点；

[0020] 所述身份验证服务器具体用于：验证所述服务提供设备的身份信息，如果验证通过，则发送由所述第一加密秘钥加密后的所述第一身份验证令牌、获取的第四时间戳以及所述服务提供设备的用户身份信息给所述服务提供设备；所述第四时间戳用于指示出所述身份验证服务器生成所述第一加密秘钥、所述第一身份验证令牌以及通过所述第一加密秘钥加密所述第一身份验证令牌的时间点；

[0021] 所述服务提供设备还用于：将所述携带所述服务提供设备的身份信息的第二请求、所述由第一加密秘钥加密后的所述第一身份验证令牌、所述服务请求设备的身份信息以及获取的第五时间戳发送给所述身份管理服务器；所述第五时间戳用于指示出第一加密秘钥加密后的所述第一身份验证令牌、所述服务请求设备的身份信息的获取时间点；

[0022] 所述身份管理服务器具体还用于：验证所述第二请求，如果验证通过，则将所述随机解密秘钥、所述第二解密秘钥及第六时间戳发送给所述服务提供设备；所述第六时间戳用于指示出随机解密秘钥以及所述第二解密秘钥的生成时间点；

[0023] 所述服务提供设备具体用于：通过所述随机解密秘钥以及所述第二解密秘钥将所述由所述随机加密秘钥加密后的学生隐私数据以及所述由第二加密秘钥加密后的第二身

份验证令牌进行解析，获得所述学生隐私数据。

[0024] 结合第一方面，在一些可选的实施例中，

[0025] 所述服务请求设备，具体用于：

[0026] 将携带所述服务请求设备的身份信息ID的第一请求$Request_1$发送给所述身份验证服务器；或者，

[0027] 所述身份验证服务器，具体用于：

[0028] 验证所述服务请求设备的身份信息ID_A，如果验证通过，则将由第一加密秘钥$E_{k(AS-IDS)}$加密后的第一身份验证令牌$E_{k(AS-IDS)}(Token_1)$、获取的第一时间戳T_1以及所述服务请求设备的身份信息ID_A发送给所述服务请求设备。

[0029] 结合第一方面，在一些可选的实施例中，

[0030] 所述服务请求设备具体还用于：

[0031] 将所述携带所述服务请求设备的身份信息ID_A的第一请求$Request_1$、所述由第一加密秘钥$E_{k(AS-IDS)}$加密后的第一身份验证令牌$E_{k(AS-IDS)}(Token_1)$、所述服务提供设备的身份信息ID_B以及所述服务请求设备生成的第二时间戳T_2发送给所述身份管理服务器；或者，

[0032] 所述身份管理服务器具体用于：

[0033] 验证所述第一请求$Request_1$是否为合法的已授权的设备所发送，如果验证通过，则将由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌 $E_{K-SAML(IDS-B)}(Token_2)$、随机加密秘钥$E_{RK(A-B)}$、第三时间戳$T_3$、所述服务请求设备的身份信息$ID_A$以及所述服务提供设备的身份信息$ID_B$发送给所述服务请求设备。

[0034] 结合第一方面，在一些可选的实施例中，

[0035] 所述服务请求设备具体还用于：

[0036] 将由随机加密秘钥$RK_{(A-B)}$加密后的学生隐私数据Msg以及所述由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌$E_{K-SAML(IDS-B)}(Token_2)$给所述服务提供设备；其中，所述第二加密秘钥$E_{K-SAML(IDS-B)}$基于SAML协议所生成；

[0037] 所述服务提供设备具体用于：

[0038] 响应于接收到所述学生隐私数据Msg以及所述由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌$E_{K-SAML(IDS-B)}(Token_2)$，发送携带所述服务提供设备的身份信息$ID_B$的第二请求$Request_2$给所述身份验证服务器；

[0039] 所述身份验证服务器，具体还用于：

[0040] 验证所述服务提供设备的身份信息ID_B，如果验证通过，则将由所述第一加密秘钥$E_{k(AS-IDS)}$加密后的所述第一身份验证令牌$E_{k(AS-IDS)}(Token_1)$、获取的第四时间戳T_4以及所述服务提供设备的用户身份信息ID_B发送给所述服务提供设备；

[0041] 所述服务提供设备具体还用于：

[0042] 将所述携带所述服务提供设备的身份信息ID_B的第二请求$Request_2$、所述由第一加密秘钥$E_{k(AS-IDS)}$加密后的所述第一身份验证令牌$E_{k(AS-IDS)}(Token_1)$、所述服务请求设备的身份信息ID_A以及获取的第五时间戳T_5发送给所述身份管理服务器；

[0043] 所述身份管理服务器具体还用于：

[0044] 验证所述第二请求$Request_2$，如果验证通过，则将随机解密秘钥RK(A-B) 以及所述第二解密秘钥K-SAML(IDS-B)发送给所述服务提供设备；所述第二解密秘钥K-SAML(IDS-

B)基于SAML协议所生成；

[0045] 所述服务提供设备具体还用于：

[0046] 通过所述随机解密秘钥RK(A-B)以及所述第二解密秘钥 K-SAML(IDS-B)将所述由所述随机加密秘钥$E_{RK(A-B)}$加密后的学生隐私数据 $E_{RK(A-B)}$(Msg)以及所述由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌 $E_{K-SAML(IDS-B)}$($Token_2$)进行解析，获得所述学生隐私数据Msg。

[0047] 结合第一方面，在一些可选的实施例中，

[0048] 所述服务请求设备、所述身份验证服务器以及所述身份管理服务器被部署在雾计算环境中，所述服务提供设备被部署在云计算环境中；

[0049] 或者，

[0050] 所述服务请求设备、所述身份验证服务器部署在所述雾计算环境中，所述身份管理服务器以及所述服务提供设备被部署在所述云计算环境中。

[0051] 结合第一方面，在一些可选的实施例中，

[0052] 所述身份管理服务器具体还用于：

[0053] 在将由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌 $E_{K-SAML(IDS-B)}$($Token_2$)、随机加密秘钥$E_{RK(A-B)}$、第三时间戳T_3、所述服务请求设备的身份信息ID_A以及所述服务提供设备的身份信息ID_B发送给所述服务请求设备之前，

[0054] 通过椭圆曲线密码算法生成所述随机加密秘钥$E_{RK(A-B)}$。

[0055] 结合第一方面，在一些可选的实施例中，

[0056] 所述身份管理服务器具体还用于：

[0057] 在将随机解密秘钥RK(A-B)以及所述第二解密秘钥K-SAML(IDS-B)发送给所述服务提供设备之前，

[0058] 通过椭圆曲线密码算法生成所述随机解密秘钥RK(A-B)。

[0059] 结合第一方面，在一些可选的实施例中，

[0060] 所述身份验证服务器具体用于：

[0061] 验证所述服务请求设备的身份信息在所述身份验证服务器的本地数据库或所述身份验证服务器的内存中是否存在，如果存在，则确定出所述服务请求设备的身份信息获得验证通过；

[0062] 或者，

[0063] 所述身份验证服务器具体用于：

[0064] 验证所述服务提供设备的身份信息在所述身份验证服务器的本地数据库或所述身份验证服务器的内存中是否存在，如果存在，则确定出所述服务提供设备的身份信息获得验证通过。

[0065] 结合第一方面，在一些可选的实施例中，

[0066] 所述身份管理服务器具体用于：

[0067] 对由第一加密秘钥加密后的第一身份验证令牌解密，根据获得的所述第一身份验证令牌，以验证出所述服务请求设备为合法与所述身份管理服务器进行通信的已授权设备、所述第一请求真实为所述服务请求设备所发送；

[0068] 或者，

[0069] 所述身份管理服务器具体用于：

[0070] 对由第一加密秘钥加密后的所述第一身份验证令牌解密，根据获得的所述第一身份验证令牌，以验证出所述服务提供设备为合法与所述身份管理服务器进行通信的已授权设备、所述第二请求真实为所述服务提供设备所发送。

[0071] 本申请提供了一种基于双重验证机制的IDaaS系统，系统包括：服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备；服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备之间通过网络连接；其中，服务请求设备将携带服务请求设备的身份信息的第一请求发送给身份验证服务器后，获得由第一加密秘钥加密后的第一身份验证令牌以及服务提供设备的身份信息，并基于上述第一身份验证令牌，以通过身份管理服务器的验证，如果通过验证，则将接收到身份管理服务器发送的随机加密秘钥以及由第二加密秘钥加密后的第二身份验证令牌，并将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌发送给服务提供设备。响应于上述接收到的由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌，服务提供设备发送携带服务提供设备的身份信息的第二请求给身份验证设备，如果身份信息被验证通过，服务提供设备将接收到身份验证服务器发送的由所述第一加密秘钥加密后的所述第一身份验证令牌以及上述第二请求，以通过身份管理服务器对第二请求的真实性验证，如果验证通过，服务提供设备将接收身份管理服务器发送的随机解密秘钥以及第二解密秘钥，以实现对由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌进行解析，恢复出学生隐私数据。采用本申请，通过采用身份验证服务器以及身份管理服务器对通信设备的身份信息进行双重验证，以抵制身份认证攻击或者身份盗窃攻击等，可提高IDaaS系统中的信息安全性。

附图说明

[0072] 为了更清楚地说明本申请实施例技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0073] 图1是本申请提供的一种基于双重验证机制的IDaaS系统的结构示意图；

[0074] 图2是本申请提供的另一种基于双重验证机制的IDaaS系统的结构示意图；

[0075] 图3是本申请提供的又一种基于双重验证机制的IDaaS系统的结构示意图；

[0076] 图4是本申请提供的又一种基于双重验证机制的IDaaS系统的结构示意图。

具体实施方式

[0077] 下面将结合本申请中的附图，对本申请中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0078] 为提高IDaaS系统中数据的安全性，抵制伪造攻击、身份盗窃攻击和身份认证攻击，本申请提供了一种基于双重验证机制的IDaaS系统。具体的，参见图1，是本申请提供的一种基于双重验证机制的IDaaS系统的结构流程图，如图 1所示，该系统，可包括但不限于：

[0079] 服务请求设备、身份验证服务器(Authentication Server,AD)、身份管理服务器(Identity Management Server,IDS)及服务提供设备;服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备之间通过通信网络连接;

[0080] 可选的,上述服务请求设备、身份验证服务器以及身份管理服务器被部署在雾计算环境中,上述服务提供设备被部署在云计算环境中;或者,

[0081] 可选的,上述服务请求设备、身份验证服务器部署在雾计算环境中,身份管理服务器以及服务提供设备被部署在云计算环境中。

[0082] 应当说明的,服务请求设备可包括但不限于:可用于学生隐私数据采集的课堂专用摄像头、可用于学生隐私数据采集的AI智能盒子、可用于学生隐私数据采集的摄像机、或者其他可用于学生隐私数据采集的设备。

[0083] 服务提供设备可包括但不限于:可用于对学生隐私数据进行处理的服务器。

[0084] 应当说明的,上述通信网络可包括但不限于下述方式:

[0085] 方式1:有线方式(如:网线或光纤)的通信网络;

[0086] 方式2:无线方式(如:WIFI6或5G)的通信网络;

[0087] 方式3:上述有线方式和无线方式相结合的通信网络。

[0088] 服务请求设备可用于:将携带服务请求设备的身份信息的第一请求发送给身份验证服务器;其中,

[0089] 服务请求设备的身份信息,可包括但不限于:服务请求设备所在的地理位置和/或设备唯一标识码;

[0090] 其中,设备唯一标识码,可包括但不限于:服务请求设备的设备唯一标识 (Unique Device Identifier,UDID)、IMEI码(International Mobile Equipment Identity)、厂商标识符(IDFV)、通用唯一识别码、MAC地址、IP地址或其他唯一标识。

[0091] 身份验证服务器可用于:验证服务请求设备的身份信息,如果该身份信息验证通过,则发送由第一加密秘钥加密后的第一身份验证令牌给服务请求设备;其中,第一身份验证令牌可用于:身份管理服务器将服务请求设备验证为合法与身份管理服务器进行通信的已授权设备;

[0092] 其中,第一加密秘钥可包括但不限于:非对称加密算法中的公钥,或者对称加密算法中的密钥。

[0093] 应当说明的,身份验证服务器,用于验证服务请求设备的身份信息的具体过程如下:

[0094] 身份验证服务器具体可用于:验证身份验证服务器的身份验证服务器的本地数据库或身份验证服务器的内存中是否存在上述身份信息,如果存在,则确定出服务请求设备的身份信息获得验证通过。

[0095] 应当说明的,服务请求设备还可用于:将携带服务请求设备的身份信息的第一请求、由第一加密秘钥加密后的第一身份验证令牌以及获取的服务提供设备的身份信息发送给身份管理服务器;其中,第一请求,可用于:服务请求设备请求身份验证服务器和身份管理服务器提供验证令牌以实现服务请求设备与服务提供设备进行学生隐私数据等信息通信;

[0096] 身份管理服务器可用于:验证第一请求,如果验证通过,则将由第二加密秘钥加密

后的第二身份验证令牌、随机加密秘钥发送给服务请求设备；

[0097] 具体的，身份管理服务器具体可用于：解密出由第二加密秘钥加密后的第二身份验证令牌，以验证第一请求是否为合法的已授权的设备所发送，如果验证通过，则将由第二加密秘钥加密后的第二身份验证令牌、随机加密秘钥发送给所述服务请求设备。第二身份验证令牌用于：服务请求服务设备与服务提供设备进行通信；

[0098] 服务请求设备还可用于：将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌给服务提供设备；其中，学生隐私数据，可包括但不限于：学生的人脸图像、学生的考试成绩、学生的课堂成绩、学生的考勤成绩、学生的成长档案、或者学生的家庭背景等。

[0099] 服务提供设备可用于：响应于接收到学生隐私数据以及第二身份验证令牌，发送携带服务提供设备的身份信息的第二请求给身份验证服务器；

[0100] 身份验证服务器还用于：验证服务提供设备的身份信息在身份验证服务器的本地数据库或身份验证服务器的内存中是否存在，如果存在，则确定出所述服务提供设备的身份信息获得验证通过，如果验证通过，则发送由第一加密秘钥加密后的第一身份验证令牌发送给服务提供设备；

[0101] 服务提供设备还可用于：将携带服务提供设备的身份信息的第二请求、由第一加密秘钥加密后的第一身份验证令牌发送给身份管理服务器；

[0102] 身份管理服务器还用于：通过第一解密秘钥来解密出由第一加密秘钥加密后的第一身份验证令牌，以验证第二请求是否为合法的已授权的设备所发送，以验证第二请求，如果验证通过，则将随机解密秘钥以及第二解密秘钥发送给服务提供设备；其中，第二请求，可用于：服务请求设备请求身份验证服务器和所述身份管理服务器提供验证令牌以实现服务提供设备与服务请求设备之间进行学生隐私数据通信；

[0103] 其中，第一解密秘钥和上述第一加密秘钥为一对秘钥，其中，第一解密秘钥可包括但不限于：非对称加密算法中的私钥，或者对称加密算法中的秘钥。

[0104] 服务提供设备用于：通过随机解密秘钥以及第二解密秘钥将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌进行解析，以获得上述学生隐私数据；其中，第二加密秘钥和第二解密秘钥为一对秘钥，随机加密秘钥和随机解密秘钥为一对秘钥。应当说明的，服务提供设备的身份信息，可包括但不限于：服务提供设备所在的地理位置和/或设备唯一标识码；

[0105] 其中，设备唯一标识码，可包括但不限于：服务提供设备的设备唯一标识(Unique Device Identifier,UDID)、IMEI码(International Mobile Equipment Identity)、厂商标识符(IDFV)、通用唯一识别码、MAC地址、IP地址或其他唯一标识。

[0106] 本申请中，服务请求设备将携带服务请求设备的身份信息的第一请求发送给身份验证服务器后，获得由第一加密秘钥加密后的第一身份验证令牌以及服务提供设备的身份信息，并基于上述第一身份验证令牌，以通过身份管理服务器的验证，如果通过验证，则将接收到身份管理服务器发送的随机加密秘钥以及由第二加密秘钥加密后的第二身份验证令牌，并将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌发送给服务提供设备；应当说明的，身份管理服务器可基于共享属性对由第一加密秘钥加密的第一身份验证令牌进行解密。

[0107] 响应于上述接收到的由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌，服务提供设备发送携带服务提供设备的身份信息的第二请求给身份验证设备，如果身份信息被验证通过，服务提供设备将接收到身份验证服务器发送的由所述第一加密秘钥加密后的第一身份验证令牌以及上述第二请求，以通过身份管理服务器对第二请求的真实性验证，如果验证通过，服务提供设备将接收身份管理服务器发送的随机解密秘钥以及第二解密秘钥，以实现对由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌进行解析，恢复出学生隐私数据。

[0108] 为提高IDaaS系统中数据的安全性，抵制伪造攻击、身份盗窃攻击和身份认证攻击，本申请提供了另一种基于双重验证机制的IDaaS系统。具体的，

[0109] 参见图2，是本申请提供的一种基于双重验证机制的IDaaS系统的结构示意图，如图2所示，该系统可包括但不限于：

[0110] 服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备；其中，服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备之间通过通信网络连接，具体描述可参见图1实施例，此处不再赘述。

[0111] 服务请求设备可用于：将携带服务请求设备的身份信息的第一请求发送给身份验证服务器；其中，第一请求可用于：服务请求设备请求身份验证服务器和身份管理服务器提供验证令牌以实现服务请求设备与服务提供设备进行通信；

[0112] 应当说明的，服务请求设备具体可用于：

[0113] 将携带服务请求设备的身份信息ID(Identity)的第一请求$Request_1$发送给身份验证服务器；

[0114] 身份验证服务器可用于：验证服务请求设备的身份信息，如果身份信息验证通过，则发送由第一加密秘钥加密后的第一身份验证令牌、获取的第一时间戳以及服务请求设备的身份信息给服务请求设备；其中，第一加密秘钥为身份验证服务器与身份管理服务器之间的加密秘钥；第一时间戳为服务请求设备与份验证服务器之间的时间戳。其中，第一时间戳，可为身份验证服务器基于数字签名技术所生成，或者由其他时间戳服务中心设备所生成。第一时间戳用于指示出身份验证服务器生成第一加密秘钥、第一身份验证令牌以及通过第一加密秘钥加密第一身份验证令牌的时间点。

[0115] 举例来说，身份验证服务器具体可用于：

[0116] 验证服务请求设备的身份信息ID_A，如果身份信息ID_A存在于服务请求设备中，即身份信息ID_A获得验证通过，则发送由第一加密秘钥$E_{k(AS-IDS)}$加密后的第一身份验证令牌$E_{k(AS-IDS)}(Token_1)$、获取的第一时间戳T_1以及服务请求设备的身份信息ID_A给服务请求设备。

[0117] 服务请求设备还可用于：将携带服务请求设备的身份信息的第一请求、由第一加密秘钥加密后的第一身份验证令牌、服务提供设备的身份信息以及获取的第二时间戳发送给身份管理服务器；此处的第一身份令牌，可用于服务请求设备与身份管理服务器进行通信。其中，第二时间戳，可为服务请求设备基于数字签名技术所生成，或者由其他时间戳服务中心设备所生成。第二时间戳用于指示出由第一加密秘钥加密后的第一身份验证令牌、服务提供设备的身份信息的获取时间点。

[0118] 举例来说，服务请求设备具体还可用于：

[0119] 将携带服务请求设备的身份信息ID_A的第一请求$Request_1$、由第一加密秘钥

$E_{k(AS-IDS)}$加密后的第一身份验证令牌$E_{k(AS-IDS)}(Token_1)$、服务提供设备的身份信息ID_B以及获取的第二时间戳T_2发送给身份管理服务器；

[0120] 身份管理服务器可用于：验证第一请求是否为合法的已授权的设备所发送，如果验证通过，则将由第二加密秘钥加密后的第二身份验证令牌、随机加密秘钥、第三时间戳、服务请求设备的身份信息以及服务提供设备的身份信息发送给服务请求设备；其中，第二加密秘钥为服务请求设备与身份管理服务器之间的加密秘钥；随机加密秘钥为服务请求设备与服务提供设备之间的加密秘钥；第二身份令牌，用于服务请求设备与服务提供设备进行通信。其中，第三时间戳，可为身份管理服务器基于数字签名技术所生成，或者由其他时间戳服务中心设备所生成。第三时间戳用于指示出身份管理服务器生成第二加密秘钥以及第二身份验证令牌的时间点。

[0121] 举例来说，身份管理服务器具体可用于：验证第一请求$Request_1$是否为合法的已授权的设备所发送，如果第一请求$Request_1$被验证通过，则将由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌$E_{K-SAML(IDS-B)}(Token_2)$、随机加密秘钥 $E_{RK(A-B)}$、第三时间戳T_3、服务请求设备的身份信息ID_A以及服务提供设备的身份信息ID_B发送给服务请求设备。

[0122] 身份管理服务器还可用于：

[0123] 在将由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌 $E_{K-SAML(IDS-B)}(Token_2)$、随机加密秘钥$E_{RK(A-B)}$、第三时间戳$T_3$、服务请求设备的身份信息$ID_A$以及服务提供设备的身份信息$ID_B$发送给服务请求设备之前，

[0124] 通过椭圆曲线密码算法(Elliptic curve cryptography，ECC)生成随机加密秘钥$E_{RK(A-B)}$。

[0125] 应当说明的，身份管理服务器还可用于：将由第二加密秘钥加密后的第二身份验证令牌、随机加密秘钥、第三时间戳、服务请求设备的身份信息以及服务提供设备的身份信息发送给服务请求设备之前，

[0126] 还将通过椭圆曲线密码算法生成随机加密秘钥。

[0127] 服务请求设备还可用于：将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌发送给服务提供设备。

[0128] 举例来说，服务请求设备具体还可用于：

[0129] 将由随机加密秘钥$RK_{(A-B)}$加密后的学生隐私数据Msg以及由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌$E_{K-SAML(IDS-B)}(Token_2)$发送给服务提供设备；其中，第二加密秘钥$E_{K-SAML(IDS-B)}$基于SAML协议所生成。

[0130] 服务提供设备具体可用于：响应于接收到学生隐私数据以及第二身份验证令牌，发送携带服务提供设备的身份信息的第二请求给身份验证服务器。

[0131] 举例来说，服务提供设备具体用于：响应于接收到由随机秘钥加密的学生隐私数据Msg以及由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌$E_{K-SAML(IDS-B)}(Token_2)$，发送携带服务提供设备的身份信息的第二请求$Request_2$给身份验证服务器。

[0132] 身份验证服务器具体可用于：验证服务提供设备的身份信息，如果身份验证服务器的数据库存在上述服务提供设备的身份信息，则验证通过，如果验证通过，则发送由第一加密秘钥加密后的第一身份验证令牌、身份验证服务器生成的第四时间戳以及服务提供设备的用户身份信息给所述服务提供设备；其中，第四时间戳，可为身份验证服务器基于数字

签名技术所生成，或者由其他时间戳服务中心设备所生成。第四时间戳用于指示出身份验证服务器生成第一加密秘钥、第一身份验证令牌以及通过第一加密秘钥加密第一身份验证令牌的时间点。

[0133] 举例来说，身份验证服务器，具体可用于：验证服务提供设备的身份信息ID_B，如果验证通过，则发送由第一加密秘钥$E_{k(AS-IDS)}$加密后的第一身份验证令牌 $E_{k(AS-IDS)}(Token_1)$、身份验证服务器生成的第四时间戳T_4以及服务提供设备的用户身份信息ID_B给服务提供设备。

[0134] 服务提供设备具体还可用于：将携带服务提供设备的身份信息的第二请求、由第一加密秘钥加密后的第一身份验证令牌、服务请求设备的身份信息以及服务提供设备生成的第五时间戳发送给身份管理服务器；其中，第五时间戳，可为服务提供设备基于数字签名技术所生成，或者由其他时间戳服务中心设备所生成。第五时间戳用于指示出第一加密秘钥加密后的第一身份验证令牌、服务请求设备的身份信息的获取时间点。

[0135] 举例来说，服务提供设备还用于：将携带服务提供设备的身份信息ID_B的第二请求$Request_2$、由第一加密秘钥$E_{k(AS-IDS)}$加密后的第一身份验证令牌 $E_{k(AS-IDS)}(Token_1)$、服务请求设备的身份信息ID_A以及服务提供设备生成的第五时间戳T_5发送给身份管理服务器。

[0136] 身份管理服务器具体还可用于：解密出由第一加密秘钥加密后的第一身份验证令牌，并根据第一身份验证令牌确认出服务提供设备为合法的已授权的设备所发送，则验证通过，且将随机解密秘钥、第二解密秘钥、第六时间戳、服务请求设备的身份信息以及服务提供设备的身份信息发送给服务提供设备。其中，第六时间戳，可为身份管理服务器基于数字签名技术所生成，或者由其他时间戳服务中心设备所生成。第六时间戳用于指示出随机解密秘钥以及第二解密秘钥的生成时间点。

[0137] 举例来说，身份管理服务器具体还用于：验证第二请求$Request_2$，如果验证通过，则将随机解密秘钥RK(A-B)、所述第二解密秘钥K-SAML(IDS-B)、第六时间戳T_6、服务请求设备的身份信息ID_A以及服务提供设备的身份信息ID_B发送给服务提供设备；第二解密秘钥K-SAML(IDS-B)基于SAML协议所生成。

[0138] 身份管理服务器具体还用于：

[0139] 在将随机解密秘钥RK(A-B)以及第二解密秘钥K-SAML(IDS-B)发送给服务提供设备之前，

[0140] 通过椭圆曲线密码算法(ECC)生成随机解密秘钥RK(A-B)。

[0141] 服务提供设备可用于：通过随机解密秘钥以及第二解密秘钥将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌进行解析，获得学生隐私数据。

[0142] 举例来说，服务提供设备具体用于：通过随机解密秘钥RK(A-B)以及第二解密秘钥K-SAML(IDS-B)将由随机加密秘钥$E_{RK(A-B)}$加密后的学生隐私数据 $E_{RK(A-B)}(Msg)$以及由第二加密秘钥$E_{K-SAML(IDS-B)}$加密后的第二身份验证令牌 $E_{K-SAML(IDS-B)}(Token_2)$进行解析，恢复出学生隐私数据Msg。

[0143] 应当说明的，图2实施例中未详细进行解释的定义或说明，可参考图1实施例。

[0144] 参见图3，是本申请提供的又一种基于双重验证机制的IDaaS系统的结构示意图，该系统，可包括但不限于：服务请求设备、身份验证服务器、身份管理服务器及服务提供设

备;其中,服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备之间通过通信网络连接;

[0145] 应当说明的,服务请求设备、身份验证服务器以及身份管理服务器被部署在雾计算环境中,上述服务提供设备被部署在云计算环境中。

[0146] 应当说明的,服务请求设备、身份验证服务器、身份管理服务器及服务提供设备的具体功能的实现,可参考图1-2实施例,此处不再赘述。

[0147] 参见图4,是本申请提供的又一种基于双重验证机制的IDaaS系统的结构示意图,该系统,可包括但不限于:服务请求设备、身份验证服务器、身份管理服务器及服务提供设备;其中,服务请求设备、身份验证服务器、身份管理服务器以及服务提供设备之间通过通信网络连接;

[0148] 应当说明的,上述服务请求设备、身份验证服务器以及身份管理服务器被部署在雾计算环境中,上述服务提供设备被部署在云计算环境中。

[0149] 应当说明的,服务请求设备、身份验证服务器、身份管理服务器及服务提供设备的具体功能的实现,可参考图1-2实施例,此处不再赘述。

[0150] 本领域普通技术人员可以意识到,结合本申请中所公开的实施例描述的各示例的内容,能够以电子硬件、计算机软件或者二者的结合来实现,为了清楚地说明硬件和软件的可互换性,在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。

[0151] 所属领域的技术人员可以清楚地了解到,为了描述的方便和简洁,上述描述的设备、系统的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0152] 在本申请所提供的几个实施例中,应该理解到,所揭露的设备或系统,可以通过其它的方式实现。系统或设备的这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方式来实现所描述的设备的功能,但是这种实现不应认为超出本申请的范围。

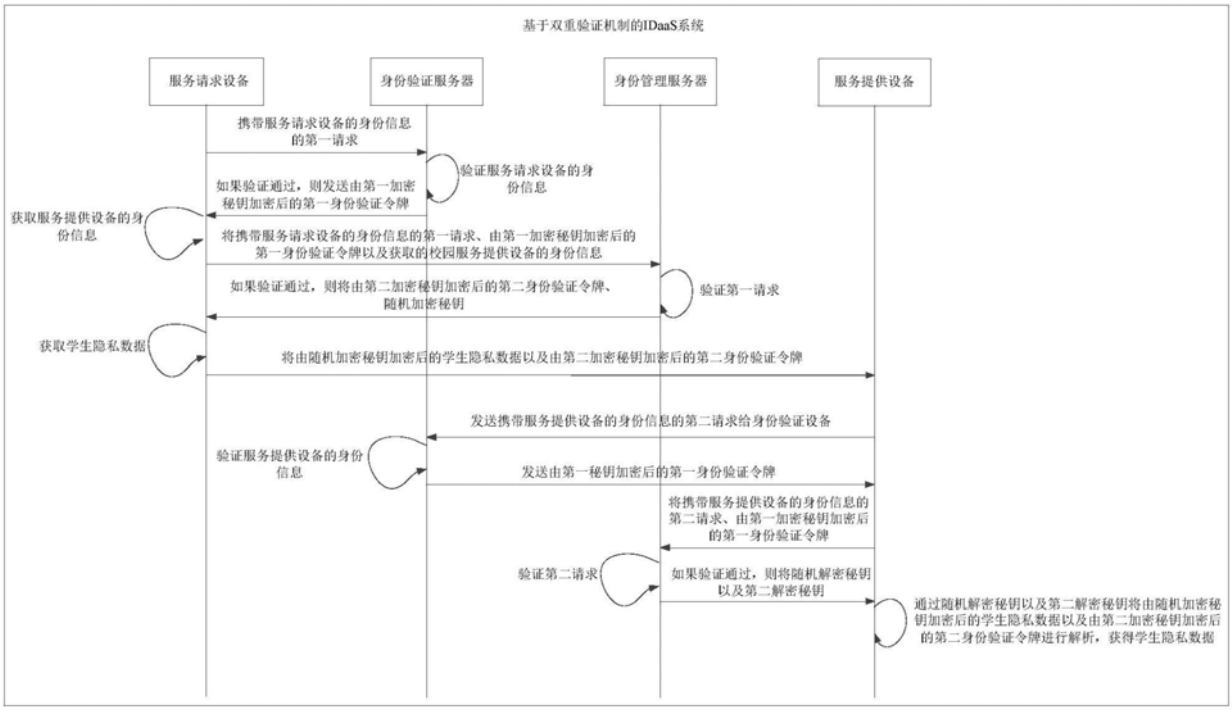

基于双重验证机制的IDaaS系统
服务请求设备
身份验证服务器
身份管理服务器
服务提供设备
携带服务请求设备的身份信息的第一请求
验证服务请求设备的身份信息
如果验证通过，则发送由第一加密秘钥加密后的第一身份验证令牌
获取服务提供设备的身份信息
将携带服务请求设备的身份信息的第一请求、由第一加密秘钥加密后的第一身份验证令牌以及获取的校园服务提供设备的身份信息
如果验证通过，则将由第二加密秘钥加密后的第二身份验证令牌、随机加密秘钥
验证第一请求
获取学生隐私数据
将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌
发送携带服务提供设备的身份信息的第二请求给身份验证设备
验证服务提供设备的身份信息
发送由第一秘钥加密后的第一身份验证令牌
将携带服务提供设备的身份信息的第二请求、由第一加密秘钥加密后的第一身份验证令牌
验证第二请求
如果验证通过，则将随机解密秘钥以及第二解密秘钥
通过随机解密秘钥以及第二解密秘钥将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌进行解析，获得学生隐私数据

图1

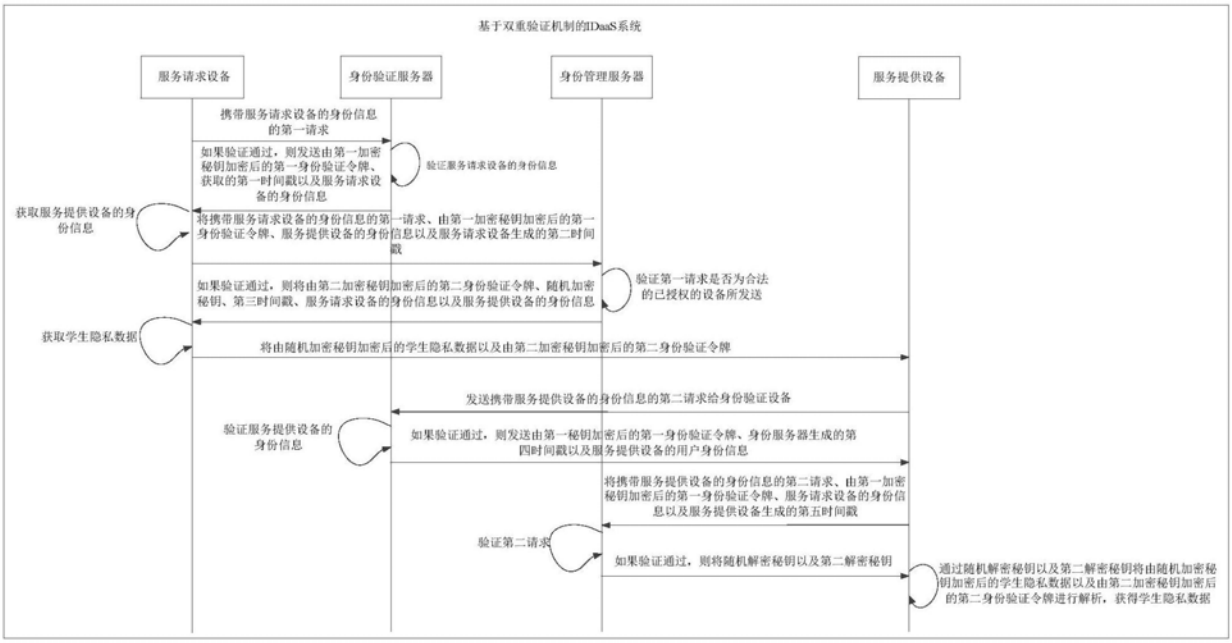

基于双重验证机制的IDaaS系统
服务请求设备
身份验证服务器
身份管理服务器
服务提供设备
携带服务请求设备的身份信息的第一请求
如果验证通过，则发送由第一加密秘钥加密后的第一身份验证令牌、获取的第一时间戳以及服务请求设备的身份信息
验证服务请求设备的身份信息
获取服务提供设备的身份信息
将携带服务请求设备的身份信息的第一请求、由第一加密秘钥加密后的第一身份验证令牌、服务提供设备的身份信息以及服务请求设备生成的第二时间戳
如果验证通过，则将由第二加密秘钥加密后的第二身份验证令牌、随机加密秘钥、第三时间戳、服务请求设备的身份信息以及服务提供设备的身份信息
验证第一请求是否为合法的已授权的设备所发送
获取学生隐私数据
将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌
发送携带服务提供设备的身份信息的第二请求给身份验证设备
验证服务提供设备的身份信息
如果验证通过，则发送由第一秘钥加密后的第一身份验证令牌、身份服务器生成的第四时间戳以及服务提供设备的用户身份信息
将携带服务提供设备的身份信息的第二请求、由第一加密秘钥加密后的第一身份验证令牌、服务请求设备的身份信息以及服务提供设备生成的第五时间戳
验证第二请求
如果验证通过，则将随机解密秘钥以及第二解密秘钥
通过随机解密秘钥以及第二解密秘钥将由随机加密秘钥加密后的学生隐私数据以及由第二加密秘钥加密后的第二身份验证令牌进行解析，获得学生隐私数据

图2

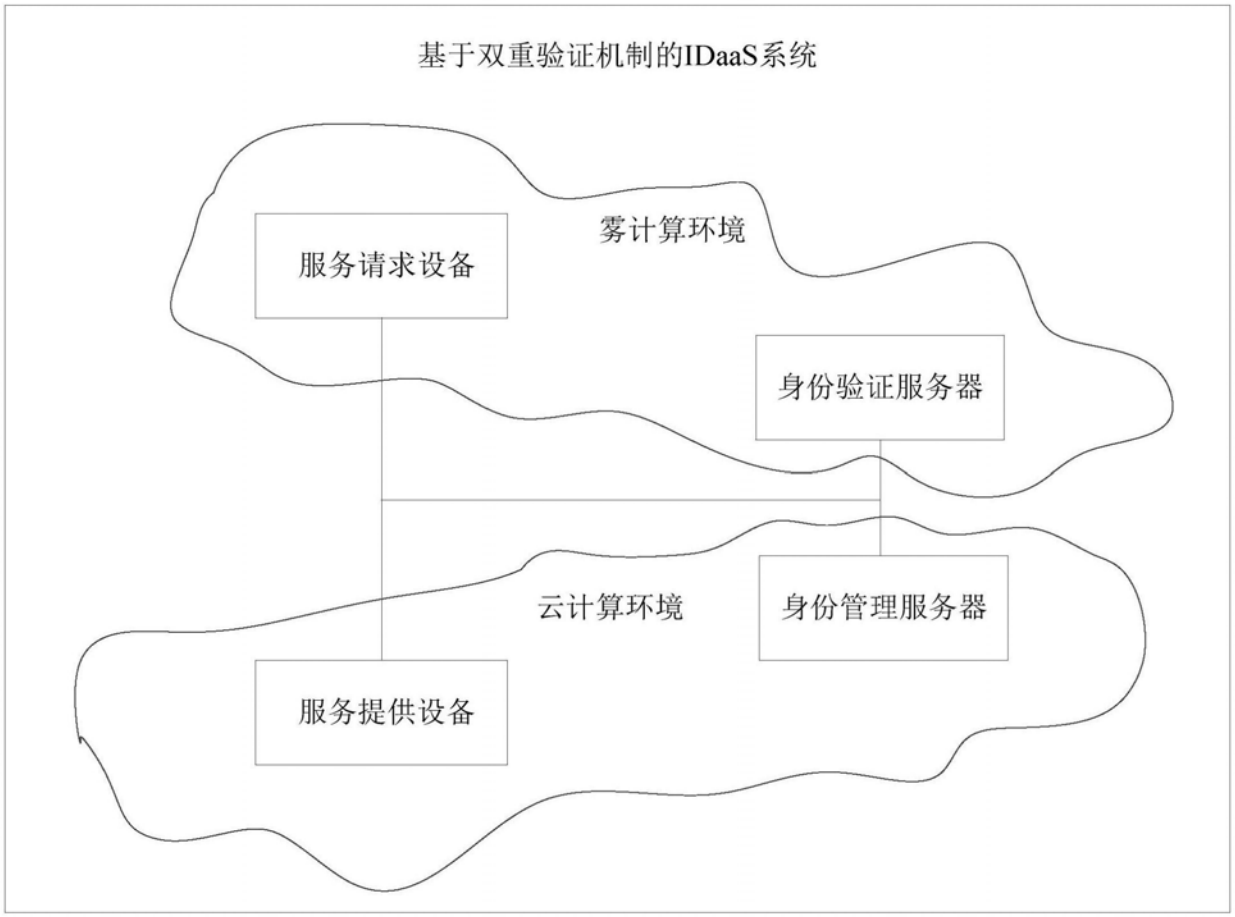

基于双重验证机制的IDaaS系统
雾计算环境
服务请求设备
身份验证服务器
云计算环境
身份管理服务器
服务提供设备

图3

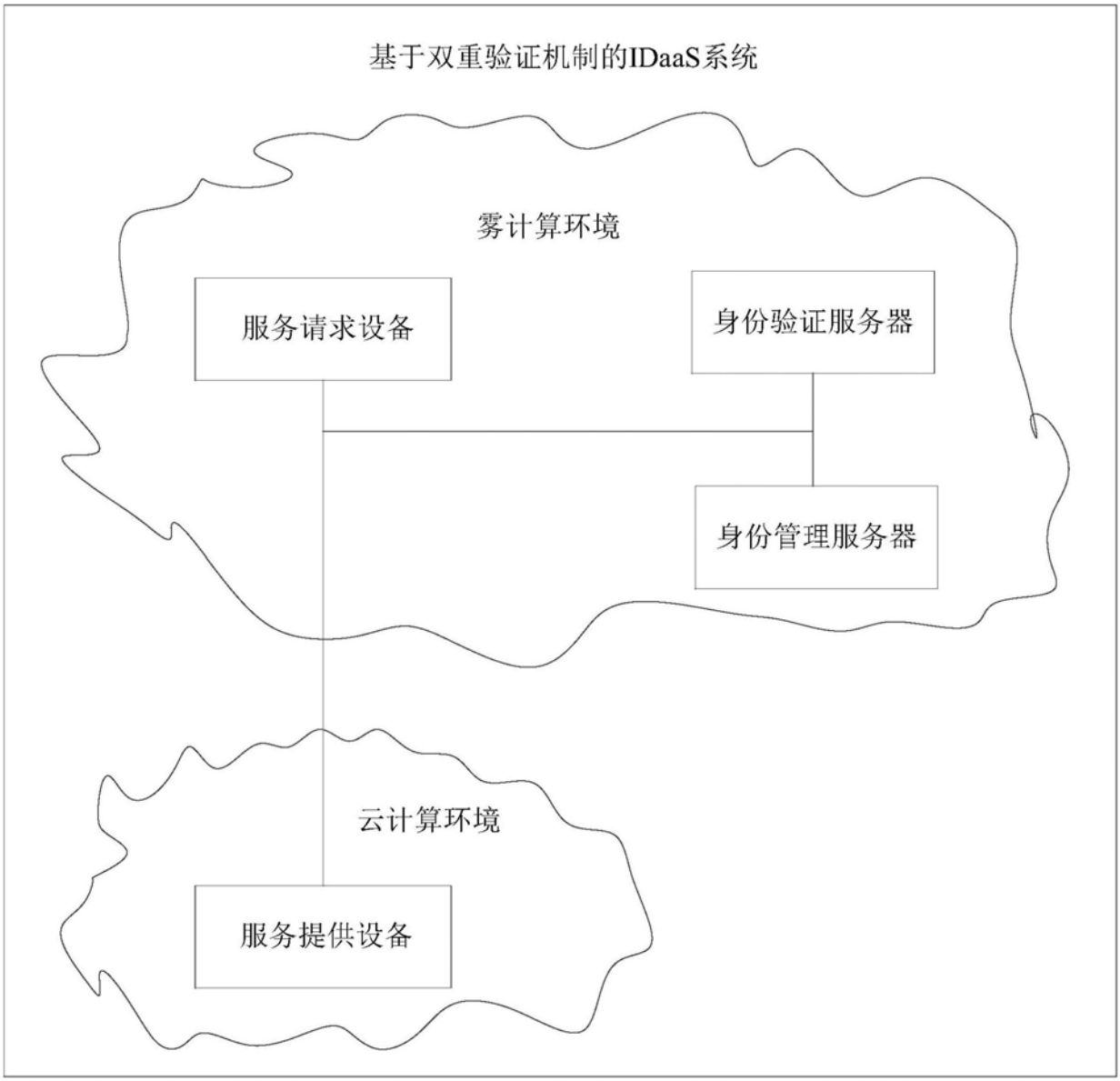

基于双重验证机制的IDaaS系统
雾计算环境
服务请求设备
身份验证服务器
身份管理服务器
云计算环境
服务提供设备

图4