(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103166757 B
(45)授权公告日 2016.01.20

(21)申请号 201110426218.X

(22)申请日 2011.12.19

(73)专利权人 卓望数码技术(深圳)有限公司
地址 518057 广东省深圳市南山区高新技术产业园南区深港产学研基地大楼西座六楼南翼

(72)发明人 唐轶贤 郝振宇 张啸雄 王巍 关学功

(74)专利代理机构 深圳市顺天达专利商标代理有限公司 44217
代理人 李琴

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 101064595 A,2007.10.31, 全文.
CN 101778381 A,2010.07.14, 全文.
CN 1019117710 A,2010.12.15, 全文.
CN 1832398 A,2006.09.13, 全文.
US 2006/0198517 A1,2006.09.07, 全文.

审查员 王田园

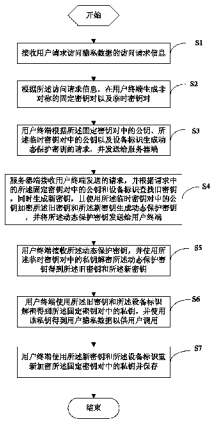
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种动态保护用户隐私数据的方法及系统

(57)摘要

本发明公开了一种动态保护用户隐私数据的方法及系统，本发明在用户终端生成非对称的固定密钥对以及临时密钥对，通过固定密钥对中的私钥加密用户隐私数据，而该私钥又通过服务器端生成的动态保护密钥进行加密，根据用户终端的请求，每次生成的动态保护密钥都不一样，所生成的动态保护密钥通过临时密钥对中的公钥进行加密传输，保证了数据传输通道的安全性，同时提高了用户终端上的用户隐私数据的安全性。



CN 103166757 B

1. 一种动态保护用户隐私数据的方法，其特征在于，包括步骤：

接收用户请求访问隐私数据的访问请求信息；

根据所述访问请求信息，在用户终端生成非对称的固定密钥对以及非对称的临时密钥对；

用户终端根据所述固定密钥对中的公钥、所述临时密钥对中的公钥以及设备标识生成动态保护密钥的请求，并发送给服务器端；

服务器端接收用户终端发送的请求，并根据请求中的所述固定密钥对中的公钥和设备标识查找旧密钥，同时生成新密钥，且使用所述临时密钥对中的公钥加密所述旧密钥和所述新密钥生成动态保护密钥，并将所述动态保护密钥发送给用户终端；

用户终端接收所述动态保护密钥，并使用所述临时密钥对中的私钥解密所述动态保护密钥得到所述旧密钥和所述新密钥；

用户终端使用所述旧密钥和设备标识解密得到所述固定密钥对中的私钥，并使用该私钥得到用户隐私数据以供用户调用；

用户终端使用所述新密钥和所述设备标识重新加密所述固定密钥对中的私钥并保存。

2. 根据权利要求 1 所述的方法，其特征在于，所述临时密钥对的长度小于所述固定密钥对的长度。

3. 根据权利要求 2 所述的方法，其特征在于，所述固定密钥对为 2048 位的非对称的密钥对，所述临时密钥对为 512 位的非对称的密钥对。

4. 根据权利要求 1 所述的方法，其特征在于，每次根据所述访问请求信息生成的所述临时密钥对均不相同。

5. 根据权利要求 1-4 中任一项所述的方法，其特征在于，所述新密钥与所述固定密钥对中的公钥以及所述设备标识均相关联。

6. 一种动态保护用户隐私数据的系统，包括用户终端和服务器端，其特征在于，

所述用户终端包括安全组件，该安全组件包括：

访问请求信息接收模块，用于接收用户请求访问隐私数据的访问请求信息；

密钥对生成模块，用于根据所述访问请求信息生成非对称的固定密钥对以及非对称的临时密钥对；

动态保护密钥请求生成模块，用于根据所述固定密钥对中的公钥、所述临时密钥对中的公钥以及设备标识生成动态保护密钥请求；

请求发送模块，用于将所述动态保护密钥的请求发送给所述服务器端；

所述服务器端包括：

请求接收模块，用于接收所述动态保护密钥请求；

动态保护密钥生成模块，用于根据所述动态保护密钥请求中的所述固定密钥对中的公钥和设备标识查找旧密钥，同时生成新密钥，且使用所述临时密钥对中的公钥加密所述旧密钥和所述新密钥生成动态保护密钥；

发送模块，用于将所述动态保护密钥发送给所述用户终端；

所述安全组件还包括：

动态保护密钥接收模块，用于接收所述服务器端发送的所述动态保护密钥；

解密模块，用于使用所述临时密钥对中的私钥解密所述动态保护密钥得到所述旧密钥

和所述新密钥；使用所述旧密钥和设备标识解密得到所述固定密钥对中的私钥，并使用该私钥得到用户隐私数据以供用户调用；

加密模块，用于使用所述新密钥和所述设备标识重新加密所述固定密钥对中的私钥并保存。

7. 根据权利要求 6 所述的系统，其特征在于，所述临时密钥对的长度小于所述固定密钥对的长度。

8. 根据权利要求 7 所述的系统，其特征在于，所述固定密钥对为 2048 位的非对称的密钥对，所述临时密钥对为 512 位的非对称的密钥对。

9. 根据权利要求 6 所述的系统，其特征在于，所述密钥对生成模块每次根据所述访问请求信息生成的所述临时密钥对均不相同。

10. 根据权利要求 6-9 中任一项所述的系统，其特征在于，所述动态保护密钥生成模块生成的所述新密钥与所述固定密钥对中的公钥以及所述设备标识均相关联。

一种动态保护用户隐私数据的方法及系统

技术领域

[0001] 本发明涉及数字密钥领域，尤其涉及一种动态保护用户隐私数据的方法及系统。

背景技术

[0002] 现有的技术中对用户隐私数据的保护主要包括以下两种：

[0003] 其一，用户隐私数据保存在服务器端，在需要使用时对用户进行鉴权，鉴权通过后从服务器端读取。该保护方法中，用户隐私数据保存在服务器端，安全性上达到了要求，但是目前用户移动终端设备网络带宽较低、访问不稳当、通道不安全，在用户鉴权通过后，对用户隐私数据的访问存在速度慢、访问不稳定的情况，另外一方面，通道的不安全因素导致用户隐私数据的安全性降低；

[0004] 其二，用户隐私数据保存在用户终端上，使用加密的方法保存，在需要使用时对用户进行鉴权，鉴权通过后从服务器端获得密钥，然后对加密的用户隐私数据解密后使用。该保护方法中，该用户隐私数据加密保存在用户终端上时，访问速度慢、访问不稳定的情况得到了解决，但是通道的不安全导致用户的加密密钥会泄露，降低了用户隐私数据保护的安全性。

发明内容

[0005] 本发明要解决的技术问题在于针对现有技术中用户隐私数据加密保存在用户终端上时，会因为数据传输通道的不安全引发用户密钥泄露，使用户隐私数据安全性降低的缺陷，提供一种动态保护用户隐私数据的方法及系统。

[0006] 本发明解决其技术问题所采用的技术方案是：

[0007] 提供一种动态保护用户隐私数据的方法，包括步骤：

[0008] 接收用户请求访问隐私数据的访问请求信息；

[0009] 根据所述访问请求信息，在用户终端生成非对称的固定密钥对以及临时密钥对；

[0010] 用户终端根据所述固定密钥对中的公钥、所述临时密钥对中的公钥以及设备标识生成动态保护密钥的请求，并发送给服务器端；

[0011] 服务器端接收用户终端发送的请求，并根据请求中的所述固定密钥对中的公钥和设备标识查找旧密钥，同时生成新密钥，且使用所述临时密钥对中的公钥加密所述旧密钥和所述新密钥生成动态保护密钥，并将所述动态保护密钥发送给用户终端；

[0012] 用户终端接收所述动态保护密钥，并使用所述临时密钥对中的私钥解密所述动态保护密钥得到所述旧密钥和所述新密钥；

[0013] 用户终端使用所述旧密钥解密得到所述固定密钥对中的私钥，并使用该私钥得到用户隐私数据以供用户调用；

[0014] 用户终端使用所述新密钥和所述设备标识重新加密所述固定密钥对中的私钥并保存。

[0015] 本发明所述的方法中，所述临时密钥对的长度小于所述固定密钥对的长度。

[0016] 本发明所述的方法中，所述固定密钥对为2048位的非对称的密钥对，所述临时密钥对为512位的非对称的密钥对。

[0017] 本发明所述的方法中，每次根据所述访问请求信息生成的所述临时密钥对均不相同。

[0018] 本发明所述的方法中，所述新密钥与所述固定密钥对中的公钥和所述设备标识相关联。

[0019] 本发明解决其技术问题所采用的另一技术方案是：

[0020] 提供一种动态保护用户隐私数据的系统，包括用户终端和服务器端，

[0021] 所述用户终端包括安全组件，该安全组件包括：

[0022] 访问请求信息接收模块，用于接收用户请求访问隐私数据的访问请求信息；

[0023] 密钥对生成模块，用于根据所述访问请求信息生成非对称的固定密钥对以及临时密钥对；

[0024] 动态保护密钥请求生成模块，用于根据所述固定密钥对中的公钥、所述临时密钥对中的公钥以及设备标识生成动态保护密钥请求；

[0025] 请求发送模块，用于将所述动态保护密钥的请求发送给所述服务器端；

[0026] 所述服务器端包括：

[0027] 请求接收模块，用于接收所述动态保护密钥请求；

[0028] 动态保护密钥生成模块，用于根据所述动态保护密钥请求中的所述固定密钥对中的公钥和设备标识查找旧密钥，同时生成新密钥，且使用所述临时密钥对中的公钥加密所述旧密钥和所述新密钥生成动态保护密钥；

[0029] 发送模块，用于将所述动态保护密钥发送给所述用户终端；

[0030] 所述安全组件还包括：

[0031] 动态保护密钥接收模块，用于接收所述服务器端发送的所述动态保护密钥；

[0032] 解密模块，用于使用所述临时密钥对中的私钥解密所述动态保护密钥得到所述旧密钥和所述新密钥；使用所述旧密钥和设备标识解密得到所述固定密钥对中的私钥，并使用该私钥得到用户隐私数据以供用户调用；

[0033] 加密模块，用于使用所述新密钥和所述设备标识重新加密所述固定密钥对中的私钥并保存。

[0034] 本发明所述的系统中，所述临时密钥对的长度小于所述固定密钥对的长度。

[0035] 本发明所述的系统中，所述固定密钥对为2048位的非对称的密钥对，所述临时密钥对为512位的非对称的密钥对。

[0036] 本发明所述的系统中，所述密钥对生成模块每次根据所述访问请求信息生成的所述临时密钥对均不相同。

[0037] 本发明所述的系统中，所述动态保护密钥生成模块生成的所述新密钥与所述固定密钥对中的公钥和所述设备标识相关联。

[0038] 本发明产生的有益效果是：本发明在用户终端生成非对称的固定密钥对以及临时密钥对，通过固定密钥对中的私钥加密用户隐私数据，而该私钥又通过服务器端生成的动态保护密钥进行加密，根据用户终端的请求，每次生成的动态保护密钥都不一样，所生成的动态保护密钥通过临时密钥对中的公钥进行加密传输，保证了数据传输通道的安全性，同

时提高了用户终端上的用户隐私数据的安全性。

附图说明

[0039] 下面将结合附图及实施例对本发明作进一步说明，附图中：

[0040] 图 1 是本发明实施例动态保护用户隐私数据的方法流程图；

[0041] 图 2 是本发明实施例动态保护用户隐私数据系统的结构示意图。

具体实施方式

[0042] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

[0043] 如图 1 所示，本发明实施例动态保护用户隐私数据的方法主要包括步骤：

[0044] S1、用户终端接收用户请求访问隐私数据的访问请求信息；本发明实施例中用户的隐私数据保存在用户终端，由于是隐私数据故对其进行了加密，以保证其安全性。用户可以通过发送请求信息进行访问。

[0045] S2、根据访问请求信息，在用户终端生成非对称的固定密钥对以及临时密钥对；在本发明实施例中生成基于 PKI 的非对称的密钥对，采用固定密钥对中的私钥对用户隐私数据进行加密。固定密钥对第一次生成后就不再生成，且不会改变，其公钥会保存在服务器端，而临时密钥对则每次根据用户的访问请求都会生成，且每一次生成的密钥对均不一样。

[0046] S3、用户终端根据固定密钥对中的公钥、临时密钥对中的公钥以及设备标识生成动态保护密钥的请求，并发送给服务器端。固定密钥对中的公钥和设备标识对应唯一的用户。设备标识包括但不限于 IMEI、MAC 等。

[0047] S4、服务器端接收用户终端发送的请求，并根据请求中的固定密钥对中的公钥和设备标识查找旧密钥，同时生成新密钥，且使用临时密钥对中的公钥加密旧密钥和新密钥生成动态保护密钥，并将动态保护密钥发送给用户终端。利用临时密钥对中的公钥加密动态保护密钥，而每次生成的临时密钥对又不相同，增加了破解的难度，从而提高了动态保护密钥在传输过程中的安全性。

[0048] 在本发明的一个实施例中，所生成的新密钥与固定密钥对中的公钥和设备标识相关联。服务器端根据固定密钥对中的公钥和设备标识可以快速查找到对应的密钥。

[0049] S5、用户终端接收动态保护密钥，并使用临时密钥对中的私钥解密动态保护密钥得到旧密钥和新密钥；

[0050] S6、用户终端使用旧密钥和设备标识解密得到固定密钥对中的私钥，并使用该私钥得到解密后的用户隐私数据以供用户调用；

[0051] S7、用户终端使用新密钥和设备标识重新加密固定密钥对中的私钥并保存。由于使用了设备标识进行加密，所以当设备变更时就无法解密，更有效地保证了固定密钥对中的私钥的安全性。

[0052] 在用户第一次请求动态保护密钥时，服务器端并不存在旧密钥，服务器端可以直接保存固定密钥对中的公钥和设备标识之间的关系，同时生成新密钥，并返回给用户终端，并利用该新密钥加密固定密钥对中的私钥。在用户终端使用固定密钥对中的私钥加密用户

隐私数据，相当于在用户终端先进行初始化。初始化后，在用户请求访问隐私数据时则进行如图 1 中的步骤。

[0053] 在本发明实施例中，临时密钥对的长度小于固定密钥对的长度，在本发明实施例中每次生成的临时密钥对均不相同，在兼顾安全和效率的情况下，临时密钥对的长度并不是越长越好。在本发明的一个优选实施例中，固定密钥对为 2048 位的非对称的密钥对，临时密钥对为 512 位的非对称的密钥对。长度较短的轻量临时密钥对生成时间相对较短，利用其公钥加密动态保护密钥的时间也较短，但又能保证动态保护密钥传输的安全性。

[0054] 如图 2 所示，本发明实施例动态保护用户隐私数据的系统主要包括用户终端 10 和服务器端 20，

[0055] 用户终端包括安全组件，该安全组件主要用于保护用户的隐私数据，安全组件包括访问请求信息接收模块 11、密钥对生成模块 12、动态保护密钥请求生成模块 13、请求发送模块 14、动态保护密钥接收模块 15、解密模块 16 和加密模块 17，其中，

[0056] 访问请求信息接收模块 11，用于接收用户请求访问隐私数据的访问请求信息；

[0057] 密钥对生成模块 12，用于根据访问请求信息生成非对称的固定密钥对以及临时密钥对；在本发明的实施例中密钥对生成模块 12 每次根据访问请求信息生成的临时密钥对均不相同。

[0058] 动态保护密钥请求生成模块 13，用于根据固定密钥对中的公钥、临时密钥对中的公钥以及设备标识生成动态保护密钥请求；由于每次生成的临时密钥对均不相同，则利用其公钥加密生成的动态保护密钥的安全性也较高，提高了动态保护密钥在传输通道中的安全性。

[0059] 请求发送模块 14，用于将动态保护密钥的请求发送给服务器端 20；

[0060] 服务器端 20 包括请求接收模块 21、动态保护密钥生成模块 22 和发送模块 23。请求接收模块 21，用于接收请求发送模块 14 发送的动态保护密钥请求；动态保护密钥生成模块 22，用于根据动态保护密钥请求中的固定密钥对中的公钥和设备标识查找旧密钥，同时生成新密钥，且使用临时密钥对中的公钥加密旧密钥和新密钥生成动态保护密钥；服务器端 20 还可以包括一存储模块用于保存固定密钥对中的公钥和设备标识，以及动态保护密钥生成模块 22 所生成的密钥。发送模块 23，用于将动态保护密钥生成模块 22 生成的动态保护密钥发送给用户终端 10。

[0061] 安全组件中的动态保护密钥接收模块 15，用于接收服务器端 20 的发送模块 23 发送的动态保护密钥；解密模块 16，用于使用临时密钥对中的私钥解密动态保护密钥得到旧密钥和新密钥；使用旧密钥解密和设备标识进行解密得到固定密钥对中的私钥，并使用该私钥解密得到用户隐私数据以供用户调用；加密模块 17，用于使用新密钥和设备标识重新加密固定密钥对中的私钥并保存。

[0062] 在本发明实施例中临时密钥对的长度小于固定密钥对的长度，本发明的一个优选实施例中固定密钥对为 2048 位的非对称的密钥对，临时密钥对为 512 位的非对称的密钥对，长度较短的轻量临时密钥对生成时间相对较短，利用其公钥加密动态保护密钥的时间也较短，但又能保证动态保护密钥传输的安全性。

[0063] 在本发明的实施例中，动态保护密钥生成模块 22 生成的新密钥与固定密钥对中的公钥和设备标识相关联，固定密钥对中的公钥和设备标识对应唯一的用户，服务器端 20

根据固定密钥对中的公钥和设备标识可以快速查找到上一次生成的密钥。

[0064] 应当理解的是，对本领域普通技术人员来说，可以根据上述说明加以改进或变换，而所有这些改进和变换都应属于本发明所附权利要求的保护范围。

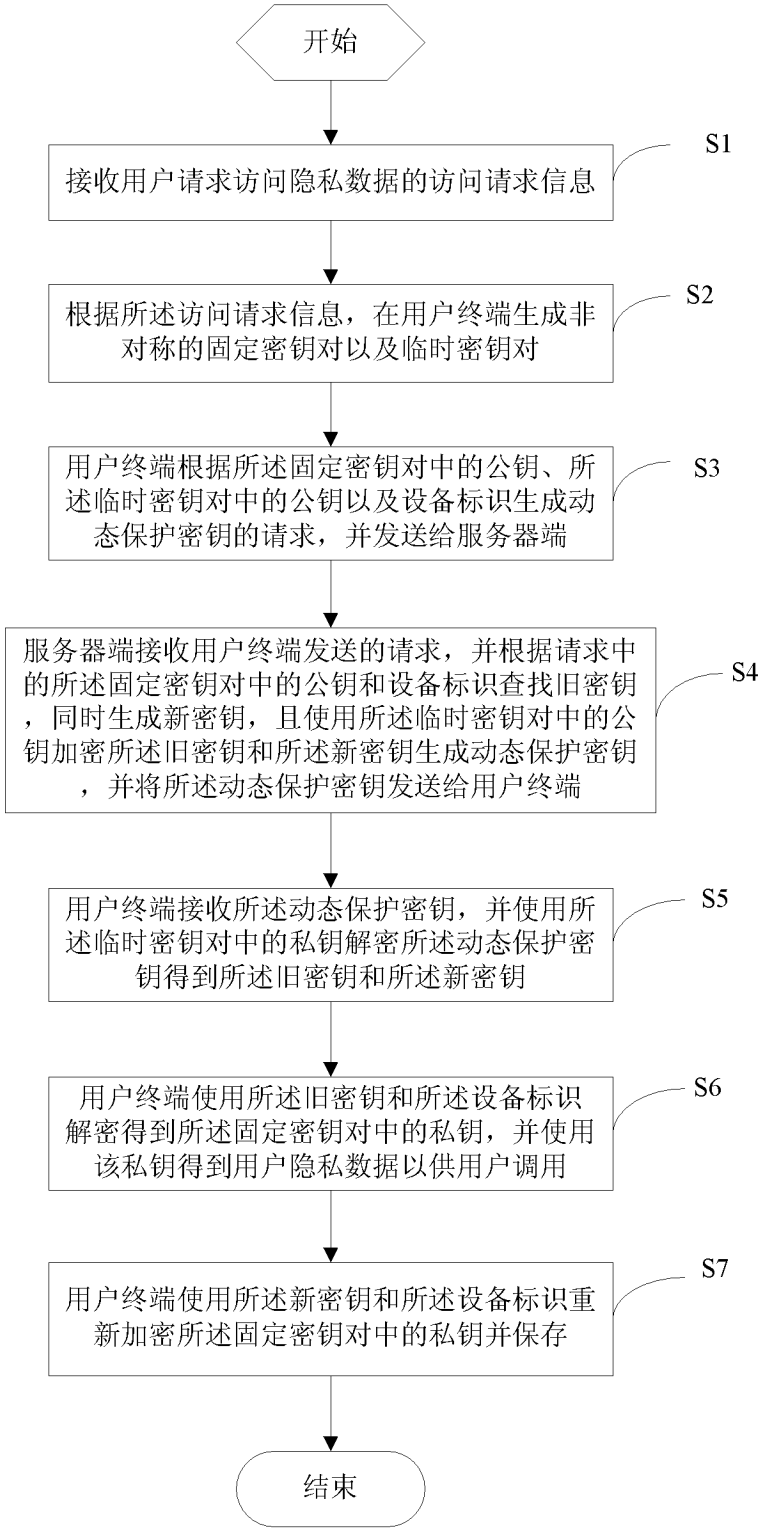

开始
接收用户请求访问隐私数据的访问请求信息
S1
根据所述访问请求信息，在用户终端生成非对称的固定密钥对以及临时密钥对
S2
用户终端根据所述固定密钥对中的公钥、所述临时密钥对中的公钥以及设备标识生成动态保护密钥的请求，并发送给服务器端
S3
服务器端接收用户终端发送的请求，并根据请求中的所述固定密钥对中的公钥和设备标识查找旧密钥，同时生成新密钥，且使用所述临时密钥对中的公钥加密所述旧密钥和所述新密钥生成动态保护密钥，并将所述动态保护密钥发送给用户终端
S4
用户终端接收所述动态保护密钥，并使用所述临时密钥对中的私钥解密所述动态保护密钥得到所述旧密钥和所述新密钥
S5
用户终端使用所述旧密钥和所述设备标识解密得到所述固定密钥对中的私钥，并使用该私钥得到用户隐私数据以供用户调用
S6
用户终端使用所述新密钥和所述设备标识重新加密所述固定密钥对中的私钥并保存
S7
结束

图 1

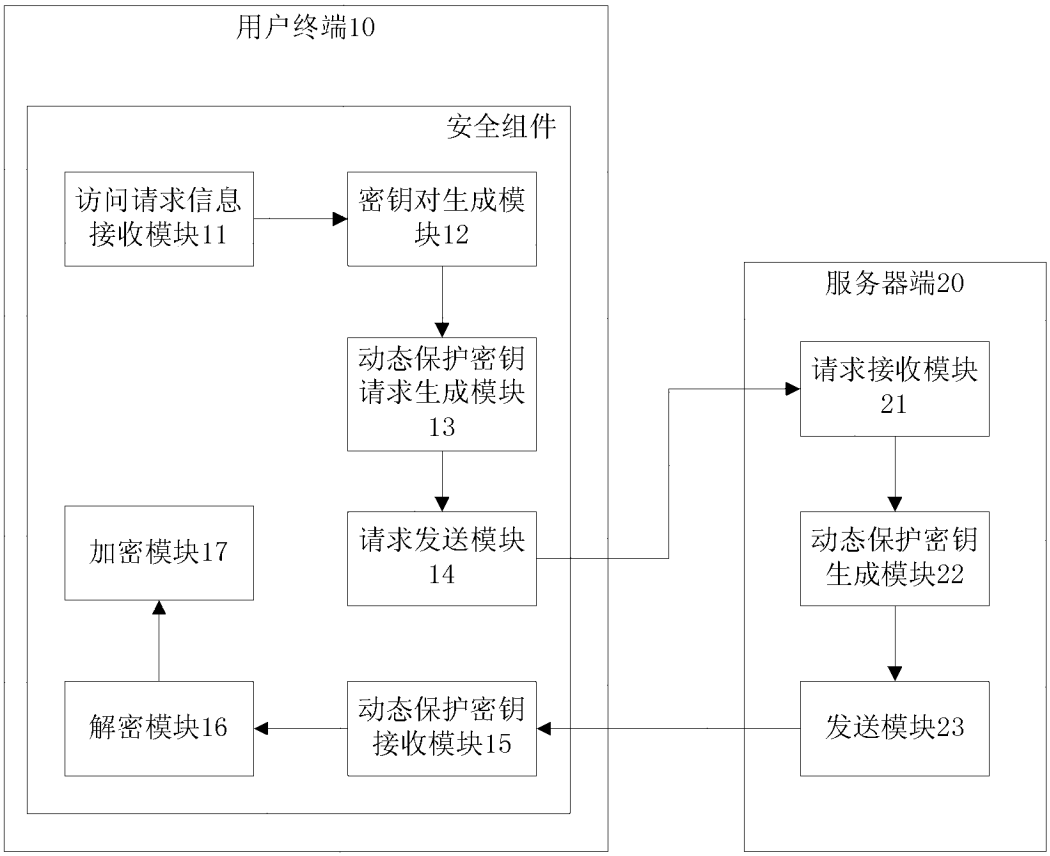

用户终端10
安全组件
访问请求信息接收模块11
密钥对生成模块12
动态保护密钥请求生成模块13
请求发送模块14
加密模块17
解密模块16
动态保护密钥接收模块15
服务器端20
请求接收模块21
动态保护密钥生成模块22
发送模块23

图 2