(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 112035855 A
(43)申请公布日 2020.12.04

(21)申请号 202010816890.9

(22)申请日 2020.08.14

(71)申请人 吴小兵
地址 638500 四川省广安市岳池县新场镇保慈寺村45号

(72)发明人 吴小兵

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)

权利要求书1页 说明书3页

(54)发明名称

一种基于众筹平台上隐私信息的访问控制系统

(57)摘要

本发明涉及隐私信息访问控制技术领域，且公开了一种基于众筹平台上隐私信息的访问控制系统，包括：运行有客户信息访问系统软件且架设在众筹云平台上的云认证服务器S_{CA}，运行有众筹云平台系统软件且用于上传客户信息的移动终端MT_S，运行有众筹云平台系统软件且用于收集客户信息的本地服务器LS_R；云认证服务器S_{CA}分别与移动终端MT_S和本地服务器LS_R进行通信连接，本地服务器LS_R与移动终端MT_S进行通信连接；当移动终端MT_S上的用户U_S在众筹云平台上输入客户信息M时，移动终端MT_S上的用户U_S在客户信息访问系统上对客户信息M进行加密，并且指定本地服务器LS_R上的众筹项目管理用户U_R为唯一解密者。本发明解决了众筹平台在合法合规收集客户信息的同时，如何防止客户信息泄漏问题。

CN 112035855 A

1.一种基于众筹平台上隐私信息的访问控制系统，其特征在于，包括：运行有客户信息访问系统软件的云认证服务器S_{CA}，用于上传客户信息的移动终端MT_S，用于收集客户信息的本地服务器LS_R；

云认证服务器S_{CA}分别与移动终端MT_S和本地服务器LS_R进行通信连接，本地服务器LS_R与移动终端MT_S进行通信连接；

移动终端MT_S上的用户U_S在客户信息访问系统上对客户信息M进行加密，并且指定本地服务器LS_R上的众筹项目管理用户U_R为唯一解密者，具体包括：

①客户信息访问系统向移动终端MT_S上的用户U_S公开以下参数：群G，G_1的阶是素数q，双线性映射$\hat{e}: G\times G\to G_1$，点P的阶是q；

②移动终端MT_S上的用户U_S选取$s\in Z_q$，计算$Q_S=sP$，并将Q_S发送给本地服务器LS_R上的众筹项目管理用户U_R；

③本地服务器LS_R上的众筹项目管理用户U_R选取$r\in Z_q$，计算$Q_R=rP$，并将Q_R发送给移动终端MT_S上的用户U_S；

④移动终端MT_S上的用户U_S计算并发送共享密钥$\hat{e}(sQ_R,Q_S)$给本地服务器LS_R上的众筹项目管理用户U_R；

⑤本地服务器LS_R上的众筹项目管理用户U_R计算并发送共享密钥$\hat{e}(rQ_S,Q_R)$给移动终端MT_S上的用户U_S；

⑥经过上述一轮数据交换之后，移动终端MT_S上的用户U_S和本地服务器LS_R上的众筹项目管理用户U_R得到同一密钥$K=\hat{e}(P,P)^{sr}$；

⑦移动终端MT_S上的用户U_S选取素数κ，π，使得$\kappa\times\pi=K$，并且使x满足$\frac{\chi}{\kappa}=\frac{\chi}{\pi}=-1$；

⑧移动终端MT_S上的用户U_S选取$\varphi_i(i=1,\cdots,s)$，并且开始计算客户信息$M=(M,\cdots,M_s)\in\{0,1\}^s$的加密密文$C=(C_1,\cdots,C_l)$，其中$C_i=\begin{cases}\chi\varphi_i^2 \bmod K, & M_i=1\\ \varphi_i^2 \bmod K, & M_i=0\end{cases}$；

将密文C发送给本地服务器LS_R上的众筹项目管理用户U_R。

2.根据权利要求1所述的基于众筹平台上隐私信息的访问控制系统，其特征在于，所述本地服务器LS_R上的众筹项目管理用户U_R对客户信息M的密文C进行解密，计算出明文$M_i'=\frac{1-\left(\frac{C_i}{\kappa}\right)}{2}, i=1,\cdots,l$。

3.根据权利要求2所述的基于众筹平台上隐私信息的访问控制系统，其特征在于，所述云认证服务器S_{CA}架设在众筹云平台上。

4.根据权利要求3所述的基于众筹平台上隐私信息的访问控制系统，其特征在于，所述移动终端MT_S和本地服务器LS_R上均运行有众筹云平台系统软件。

一种基于众筹平台上隐私信息的访问控制系统

技术领域

[0001] 本发明涉及隐私信息访问控制技术领域，具体为一种基于众筹平台上隐私信息的访问控制系统。

背景技术

[0002] 随着互联网金融业的快速发展，众筹成为当下热门的融资模式，众筹平台吸引了越来越多的创业型企业，很多个人创业者都开始通过众筹平台来满足创业发展的资金需求，互联网企业与金融机构也纷纷上线众筹平台。当投资者、融资人进入众筹平台使用真实身份信息注册，并且需要绑定手机号码和银行卡时，如何在合乎法律法规的基础之上收集客户信息，防止客户信息泄漏，避免未经客户同意擅自将客户信息用作众筹项目以外的用途。

发明内容

[0003] (一)解决的技术问题

[0004] 针对现有技术的不足，本发明提供一种基于众筹平台上隐私信息的访问控制系统，以解决众筹平台在合法合规收集客户信息的同时，如何防止客户信息泄漏问题。

[0005] (二)技术方案

[0006] 为实现上述目的，本发明提供如下技术方案：

[0007] 一种基于众筹平台上隐私信息的访问控制系统，包括：运行有客户信息访问系统软件的云认证服务器S_{CA}，用于上传客户信息的移动终端MT_S，用于收集客户信息的本地服务器LS_R；

[0008] 云认证服务器S_{CA}分别与移动终端MT_S和本地服务器LS_R进行通信连接，本地服务器LS_R与移动终端MT_S进行通信连接；

[0009] 移动终端MT_S上的用户U_S在客户信息访问系统上对客户信息M进行加密，并且指定本地服务器LS_R上的众筹项目管理用户U_R为唯一解密者，具体包括：

[0010] ①客户信息访问系统向移动终端MT_S上的用户U_S公开以下参数：群G，G_1的阶是素数q，双线性映射$\hat{e}$：$G\times G\rightarrow G_1$，点P的阶是q；

[0011] ②移动终端MT_S上的用户U_S选取$s\in Z_q$，计算$Q_S=sP$，并将Q_S发送给本地服务器LS_R上的众筹项目管理用户U_R；

[0012] ③本地服务器LS_R上的众筹项目管理用户U_R选取$r\in Z_q$，计算$Q_R=rP$，并将Q_R发送给移动终端MT_S上的用户U_S；

[0013] ④移动终端MT_S上的用户U_S计算并发送共享密钥$\hat{e}(sQ_R,Q_S)$给本地服务器LS_R上的众筹项目管理用户U_R；

[0014] ⑤本地服务器LS_R上的众筹项目管理用户U_R计算并发送共享密钥$\hat{e}(rQ_S,Q_R)$给移动终端MT_S上的用户U_S；

[0015] ⑥经过上述一轮数据交换之后，移动终端MT_S上的用户U_S和本地服务器LS_R上的众筹项目管理用户U_R得到同一密钥$K=\hat{e}(P,P)^{sr}$；

[0016] ⑦移动终端MT_S上的用户U_S选取素数κ，π，使得κ×π＝K，并且使x满足$\frac{\chi}{\kappa}=\frac{\chi}{\pi}=-1$；

[0017] ⑧移动终端MT_S上的用户U_S选取$\varphi_i(i=1,\cdots,s)$，并且开始计算客户信息M＝(M，…，M_s)∈{0，1}^{s}的加密密文C＝(C_1，…，C_l)，其中$C_i=\begin{cases}\chi\varphi_i^2 \bmod K, & M_i=1\\ \varphi_i^2 \bmod K, & M_i=0\end{cases}$；

[0018] 将密文C发送给本地服务器LS_R上的众筹项目管理用户U_R。

[0019] 进一步的，所述本地服务器LS_R上的众筹项目管理用户U_R对客户信息M的密文C进行解密，计算出明文$M_i'=\frac{1-\left(\frac{C_i}{\kappa}\right)}{2},i=1,\cdots,l$。

[0020] 进一步的，所述云认证服务器S_{CA}架设在众筹云平台上。

[0021] 进一步的，所述移动终端MT_S和本地服务器LS_R上均运行有众筹云平台系统软件。

[0022] (三)有益的技术效果

[0023] 与现有技术相比，本发明具备以下有益的技术效果：

[0024] 本发明通过在众筹云平台上架设运行有客户信息访问系统的云认证服务器，当客户在众筹云平台上输入真实身份信息、绑定手机号码和银行卡时，用户在客户信息访问系统上对客户信息进行加密，并且指定本地服务器上的众筹项目管理用户为唯一解密者，用户与本地服务器上的众筹项目管理用户采用交互验证的方式产生同一密钥$K=\hat{e}(P,P)^{sr}$，即只有拥有密钥$K=\hat{e}(P,P)^{sr}$的本地服务器上的众筹项目管理用户才能将用户的客户信息的密文恢复出正确的明文，其他用户即使非法获取了客户信息密文，也无法解密出正确的明文信息，从而解决了客户信息泄漏问题。

具体实施方式

[0025] 下面将结合本发明实施例，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

[0026] 一种基于众筹平台上隐私信息的访问控制系统，包括：运行有客户信息访问系统软件且架设在众筹云平台上的云认证服务器S_{CA}，运行有众筹云平台系统软件且用于上传客户信息的移动终端MT_S，运行有众筹云平台系统软件且用于收集客户信息的本地服务器LS_R；

[0027] 云认证服务器S_{CA}通过网络通信设备分别与移动终端MT_S和本地服务器LS_R进行通信连接，本地服务器LS_R与移动终端MT_S通过网络通信设备进行通信连接；

[0028] 当移动终端MT_S上的用户U_S在众筹云平台上输入客户信息M时，移动终端MT_S上的用户U_S在客户信息访问系统上对客户信息M进行加密，并且指定本地服务器LS_R上的众筹项目管理用户U_R为唯一解密者，具体包括：

[0029] ①客户信息访问系统向移动终端MT_S上的用户U_S公开以下参数：群G，G_1的阶是素数q，双线性映射$\hat{e}$：G×G→G_1，点P的阶是q；

[0030] ②移动终端MT_S上的用户U_S选取s∈Z_q，计算Q_S＝sP，并将Q_S发送给本地服务器LS_R上的众筹项目管理用户U_R；

[0031] ③本地服务器LS_R上的众筹项目管理用户U_R选取r∈Z_q，计算Q_R＝rP，并将Q_R发送给移动终端MT_S上的用户U_S；

[0032] ④移动终端MT_S上的用户U_S计算并发送共享密钥$\hat{e}(sQ_R,Q_S)$给本地服务器LS_R上的众筹项目管理用户U_R；

[0033] ⑤本地服务器LS_R上的众筹项目管理用户U_R计算并发送共享密钥$\hat{e}(rQ_S,Q_R)$给移动终端MT_S上的用户U_S；

[0034] ⑥经过上述一轮数据交换之后，移动终端MT_S上的用户U_S和本地服务器LS_R上的众筹项目管理用户U_R得到同一密钥$K=\hat{e}(P,P)^{sr}$；

[0035] ⑦移动终端MT_S上的用户U_S选取素数κ，π，使得κ×π＝K，并且使x满足$\frac{\chi}{\kappa}=\frac{\chi}{\pi}=-1$；

[0036] ⑧移动终端MT_S上的用户U_S选取$\varphi_i(i=1,\cdots,s)$，并且开始计算客户信息M＝(M，…，M_s)∈{0，1}^{s}的加密密文C＝(C_1，…，C_l)，其中$C_i=\begin{cases}\chi\varphi_i^2 \bmod K, & M_i=1\\ \varphi_i^2 \bmod K, & M_i=0\end{cases}$；

[0037] 之后，将密文C发送给本地服务器LS_R上的众筹项目管理用户U_R；

[0038] ⑨本地服务器LS_R上的众筹项目管理用户U_R对客户信息M的密文C进行解密，计算出明文$M_i'=\frac{1-\left(\frac{C_i}{\kappa}\right)}{2},i=1,\cdots,l$；

[0039] 当移动终端MT_S上的用户U_S指定本地服务器LS_R上的众筹项目管理用户U_R为唯一解密者时，移动终端MT_S上的用户U_S与本地服务器LS_R上的众筹项目管理用户U_R采用交互验证的方式产生同一密钥$K=\hat{e}(P,P)^{sr}$，即只有拥有密钥$K=\hat{e}(P,P)^{sr}$的本地服务器LS_R上的众筹项目管理用户U_R才能将移动终端MT_S上的用户U_S的客户信息M的密文C恢复出正确的明文M_i'。

[0040] 尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同物限定。