(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 102325026 A
(43)申请公布日 2012.01.18

(21)申请号 201110197449.8

(22)申请日 2011.07.14

(71)申请人 易讯天空计算机技术(深圳)有限公司

地址 518057 广东省深圳市南山区高新中区科技中二路 1 号深圳软件园(二期)9 栋 602-B

(72)发明人 张世杰 方勇 陈辉

(74)专利代理机构 深圳市中知专利商标代理有限公司 44101

代理人 孙皓 林虹

(51)Int.Cl.

H04L 9/32(2006.01)

H04L 29/06(2006.01)

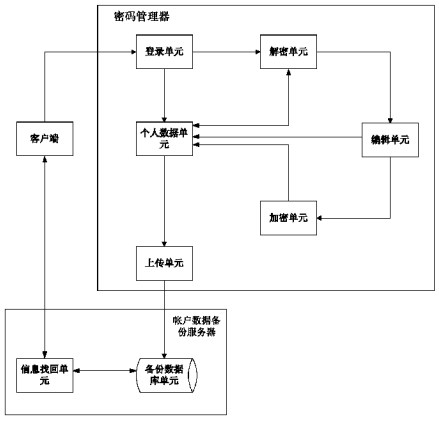
权利要求书 2 页 说明书 7 页 附图 3 页

(54)发明名称

账号密码安全加密系统

(57)摘要

本发明公开了一种账号密码安全加密系统，要解决的技术问题是提高账户密码的安全性。本发明采用以下技术方案：一种账号密码安全加密系统，其特征在于：所述账号密码安全加密系统由账户数据备份服务器、客户端和密码管理器组成，所述密码管理器连接在客户端上，客户端经互联网与账户数据备份服务器连接。与现有技术相比，采用密码管理器对账户和密码的信息进行加密后保存在密码管理器及网络服务器中，防止因密码管理器丢失导致账户和密码泄露，用户通过网络服务器可以找回自己的账号信息，提高了用户密码的安全性。



CN 102325026 A

1. 一种账号密码安全加密系统，其特征在于：所述帐号密码安全加密系统由帐户数据备份服务器、客户端和密码管理器组成，所述密码管理器连接在客户端上，客户端经互联网与帐户数据备份服务器连接；

所述密码管理器由登陆单元、解密单元、编辑单元、加密单元、个人数据单元和上传单元组成，其中：

所述登陆单元，用于验证客户端输入的登陆密码是否与密码管理器中个人数据单元中存储的默认的登陆密码一致，并将解密指令发送到解密单元；

所述解密单元，在登陆单元验证客户端输入的登陆密码后，提取保存在个人数据单元中加密的账户信息数据，并使用私钥文件进行解密操作，将解密后的帐户信息数据发送到编辑单元进行用户编辑操作；

所述编辑单元，收到解密单元解密后的帐户信息数据后，判断用户是否进行新增、修改、删除操作，是则将编辑用户新增、修改、删除账户的信息数据的帐户信息数据发送到加密单元进行加密操作，否则直接退出编辑操作，并将未修改指令发送到个人数据单元；

所述加密单元，编辑单元将编辑后的帐户信息数据发送到加密单元，加密单元接收后，将用户经过新增、修改、删除后的账户信息数据进行加密，并将加密后的帐户信息数据发送到个人数据单元，并替换编辑前的帐户信息数据；

所述个人数据单元，接收加密单元加密后的帐户信息数据，替换编辑前的帐户信息数据，并存储个人的公钥文件、私钥文件，将存储后的帐户信息数据发送到上传单元；

所述帐户数据备份服务器包括备份数据库单元，其中：

所述备份数据库单元，接收到个人数据单元中发送来的公钥文件、私钥文件、用户加密后的帐户信息数据后，备份存储到备份数据库单元的备份表中。

2. 根据权利要求 1 所述的帐号密码安全加密系统，其特征在于：所述帐户数据备份服务器还包括信息找回单元；

所述信息找回单元，当用户丢失帐户信息数据、公钥文件及私钥文件后，用户通过客户端发送信息找回指令，信息找回单元接收到指令后，将保存在备份数据库单元的帐户信息数据、公钥文件及私钥文件发送到客户端，客户端将帐户信息数据、公钥文件及私钥文件保存在个人数据单元中。

3. 根据权利要求 2 所述的帐号密码安全加密系统，其特征在于：所述编辑单元，收到解密单元解密后的帐户信息数据后，用户未进行新增、修改、删除操作，则直接退出。

4. 根据权利要求 3 所述的帐号密码安全加密系统，其特征在于：所述备份数据库单元的备份表以列表的形式存储账户信息数据。

5. 根据权利要求 4 所述的帐号密码安全加密系统，其特征在于：所述备份表存储用户的密码管理器登录密码、公钥文件、私钥文件、帐户信息数据、用户使用客户端的 MAC 地址和用户的真实姓名。

6. 根据权利要求 5 所述的帐号密码安全加密系统，其特征在于：所述加密单元进行账户信息数据加密，由文本文件转换成二进制文件，并将加密后的用户账户信息数据保存在个人数据单元的中。

7. 根据权利要求 6 所述的帐号密码安全加密系统，其特征在于：所述加密单元保存加密后的账户信息数据后，将加密后的账户信息数据通过公钥文件使用 RSA 加密算法，再次

加密并发送到上传单元。

8. 根据权利要求 7 所述的帐号密码安全加密系统，其特征在于：所述客户端的密码为 6-20 位。

9. 根据权利要求 8 所述的帐号密码安全加密系统，其特征在于：所述用户通过客户端输入错误密码次数达到三次后，登录单元关闭。

10. 根据权利要求 9 所述的帐号密码安全加密系统，其特征在于：所述客户端与帐户数据备份服务器之间使用超文本传输协议 HTTP 通信协议。

账号密码安全加密系统

技术领域

[0001] 本发明涉及一种账户安全系统，特别是一种网络账号密码的加密系统。

背景技术

[0002] 目前管理公众各种个人网络账户密码最常用的应用工具是密码管理器，它能有效的保存一些个人的帐户信息和密码。在 Internet 时代，用户通常到一个网站注册一个用户名和信息，再到另一个网站注册另一个用户名和信息，最后自己都记不住到底自己申请了多少用户名了，通常用户会使用同一个密码作为每个帐户的密码，用户的这个账户密码一旦被盗，等于其所有注册的账户都被盗了。现有技术的密码管理器加密后的个人数据采用的加密算法简单、很容易被暴力破解；加密内容是存储在用户的个人电脑上，加密的数据文件一旦都丢或者被病毒修改，用户的所有账户信息再也不能找回。

发明内容

[0003] 本发明的目的是提供一种帐号密码安全加密系统，要解决的技术问题是提高帐户密码的安全性。

[0004] 本发明采用以下技术方案：一种账号密码安全加密系统，其特征在于：所述帐号密码安全加密系统由帐户数据备份服务器、客户端和密码管理器组成，所述密码管理器连接在客户端上，客户端经互联网与帐户数据备份服务器连接；

[0005] 所述密码管理器由登陆单元、解密单元、编辑单元、加密单元、个人数据单元和上传单元组成，其中：

[0006] 所述登陆单元，用于验证客户端输入的登陆密码是否与密码管理器中个人数据单元中存储的默认的登陆密码一致，并将解密指令发送到解密单元；

[0007] 所述解密单元，在登陆单元验证客户端输入的登陆密码后，提取保存在个人数据单元中加密的账户信息数据，并使用私钥文件进行解密操作，将解密后的帐户信息数据发送到编辑单元进行用户编辑操作；

[0008] 所述编辑单元，收到解密单元解密后的帐户信息数据后，判断用户是否进行新增、修改、删除操作，是则将编辑用户新增、修改、删除账户的信息数据的帐户信息数据发送到加密单元进行加密操作，否则直接退出编辑操作，并将未修改指令发送到个人数据单元；

[0009] 所述加密单元，编辑单元将编辑后的帐户信息数据发送到加密单元，加密单元接收后，将用户经过新增、修改、删除后的账户信息数据进行加密，并将加密后的帐户信息数据发送到个人数据单元，并替换编辑前的帐户信息数据；

[0010] 所述个人数据单元，接收加密单元加密后的帐户信息数据，替换编辑前的帐户信息数据，并存储个人的公钥文件、私钥文件，将存储后的帐户信息数据发送到上传单元；

[0011] 所述帐户数据备份服务器包括备份数据库单元，其中：

[0012] 所述备份数据库单元，接收到个人数据单元中发送来的公钥文件、私钥文件、用户加密后的帐户信息数据后，备份存储到备份数据库单元的备份表中。

[0013] 本发明的帐户数据备份服务器还包括信息找回单元；

[0014] 所述信息找回单元，当用户丢失帐户信息数据、公钥文件及私钥文件后，用户通过客户端发送信息找回指令，信息找回单元接收到指令后，将保存在备份数据库单元的帐户信息数据、公钥文件及私钥文件发送到客户端，客户端将帐户信息数据、公钥文件及私钥文件保存在个人数据单元中。

[0015] 本发明的编辑单元，收到解密单元解密后的帐户信息数据后，用户未进行新增、修改、删除操作，则直接退出。

[0016] 本发明的备份数据库单元的备份表以列表的形式存储账户信息数据。

[0017] 本发明的备份表存储用户的密码管理器登录密码、公钥文件、私钥文件、帐户信息数据、用户使用客户端的 MAC 地址和用户的真实姓名。

[0018] 本发明的加密单元进行账户信息数据加密，由文本文件转换成二进制文件，并将加密后的用户账户信息数据保存在个人数据单元的中。

[0019] 本发明的加密单元保存加密后的账户信息数据后，将加密后的账户信息数据通过公钥文件使用 RSA 加密算法，再次加密并发送到上传单元。

[0020] 本发明的客户端的密码为 6-20 位。

[0021] 本发明的用户通过客户端输入错误密码次数达到三次后，登录单元关闭。

[0022] 本发明的客户端与帐户数据备份服务器之间使用超文本传输协议 HTTP 通信协议。

[0023] 本发明与现有技术相比，采用密码管理器对帐户和密码的信息进行加密后保存在密码管理器及网络服务器中，防止因密码管理器丢失导致帐户和密码泄露，用户通过网络服务器可以找回自己的帐号信息，提高了用户密码的安全性。

附图说明

[0024] 图 1 是本发明网络拓扑图。

[0025] 图 2 是本发明的账号密码安全加密系统的结构示意图。

[0026] 图 3-1 是本发明的工作流程图。

[0027] 图 3-2 是本发明信息找回的流程图。

具体实施方式

[0028] 下面结合附图和实施例对本发明的技术方案作进一步的详细说明。

[0029] 如图 1 所示，本发明的帐号密码安全加密系统由帐户数据备份服务器、客户端和密码管理器组成，所述密码管理器连接在客户端上，客户端经互联网与帐户数据备份服务器连接。

[0030] 如图 2 所示，所述密码管理器由以下部件组成：

[0031] 登陆单元，用于验证客户端输入的登陆密码是否与密码管理器中个人数据单元中的私钥文件中的登陆密码一致，并将解密指令发送到解密单元；

[0032] 解密单元，在登陆单元验证客户端输入的登陆密码后，提取保存在个人数据单元中加密的账户信息数据，并使用私钥文件进行解密操作，将解密后的帐户信息数据发送到编辑单元进行用户编辑操作；

[0033] 编辑单元，收到解密单元解密后的帐户信息数据后，判断用户是否进行新增、修改、删除操作，是则将编辑用户新增、修改、删除账户的信息数据的帐户信息数据发送到加密单元进行加密操作，否则直接退出编辑操作，并将未修改指令发送到个人数据单元；

[0034] 加密单元，编辑单元将编辑后的帐户信息数据发送到加密单元，加密单元接收后，将用户经过新增、修改、删除后的账户信息数据进行加密，并将加密后的帐户信息数据发送到个人数据单元，并替换编辑前的帐户信息数据；

[0035] 个人数据单元，接收加密单元加密后的帐户信息数据，替换编辑前的帐户信息数据，并存储个人的公钥文件、私钥文件，将存储后的帐户信息数据发送到上传单元；所述公钥文件、私钥文件采用微软的视窗 windows 二进制文件，所述公钥文件为公用的公钥文件，将加密后的用户账户信息数据通过 RSA 加密算法加密；私钥文件是用户登录的时候根据用户输入的登录密码和私钥文件密码是否一致，如果一致，加密单元使用私钥文件解密用户的帐户信息数据，不一致则为登录密码错误，错误三次将退出登录单元；个人数据单元采 mysql 数据库，数据存储的格式为表存储；

[0036] 上传单元，收到个人数据单元发送来的帐户信息数据后，通过互联网将存储在个人数据单元中的公钥文件、私钥文件、用户的帐户信息数据发送到帐户数据备份服务器的备份数据库。

[0037] 所述帐户数据备份服务器由以下部件组成：

[0038] 备份数据库单元，接收到个人数据单元中发送来的公钥文件、私钥文件、用户加密后的帐户信息数据后，备份存储到备份数据库单元的备份表中，所述备份数据库单元采用 mysql 数据库，数据存储的格式为表存储。；

[0039] 信息找回单元，当用户丢失帐户信息数据、公钥文件及私钥文件后，用户通过客户端发送信息找回指令，信息找回单元接收到指令后，将保存在备份数据库单元的帐户信息数据、公钥文件及私钥文件发送到客户端，客户端将帐户信息数据、公钥文件及私钥文件保存在个人数据单元中。

[0040] 如图 3-1 所示，本发明的帐号密码安全加密系统的实现，包括以下步骤：

[0041] 一、用户通过客户端输入登陆密码，此登陆密码是由密码管理器的分发者初始化的一个 6-20 位的密码，可以由数字 (0-9)、大小写字母及特殊字符任意组合，登录单元通过对比登录密码和个人数据单元中存放的私钥文件中的登陆密码是否一致，如果不一致，登录单元则提示重新输入登录密码，用户通过客户端输入错误密码次数达到三次后，登录单元关闭，结束登陆，一致则进入下一步；

[0042] 二、登录单元发送解密指令到解密单元，解密单元收到解密指令后，提取存储在个人数据单元中的用户账户信息数据，使用私钥文件对用户的账户信息数据进行解密，解密后，解密单元将用户账户信息数据由二进制文件转换成文本文件，并且保存在客户端的的临时存储单元中，同时将该解密后的用户帐户信息数据明文显示在客户端的显示单元上，如果此时客户端关闭或掉电，存储在临时存储单元中的解密后的用户账户信息数据明文信息会自动消失，此时需要重新通过登录单元正常登录后，重复步骤二，进行下一步操作；

[0043] 三、用户通过编辑单元对解密后的用户账户信息数据进行新增、修改、删除及查看等操作，当用户结束操作后，编辑单元判断用户是否进行了新增、修改及删除操作，否则结束，是则将修改后的用户账户信息数据暂存在客户端的临时存储单元中；

[0044] 四、用户关闭客户端时，加密单元提取暂存在临时存储单元中的用户账户信息数据进行加密，由文本文件转换成二进制文件，并将加密后的用户账户信息数据保存在个人数据单元的中；

[0045] 五、加密单元保存加密后的用户账户信息数据后，将加密后的用户账户信息数据通过公用的加密公钥文件使用 RSA 加密算法，再次加密并发送到上传单元，上传单元通过客户端的通讯单元将加密后的用户帐户信息、公钥文件及私钥文件发送至帐户数据备份服务器，帐户数据备份服务器接收到数据后，将新的用户帐户信息数据、公钥文件及私钥文件备份并替换到备份数据库单元的备份表中，结束操作。

[0046] 所述客户端与帐户数据备份服务器之间采用超文本传输协议 HTTP 通信协议。

[0047] 所述备份表存储用户的密码管理器登录密码、公钥文件、私钥文件、帐户信息数据、用户使用客户端的 MAC 地址和用户的真实姓名。一旦用户的密码管理器登录密码忘记或者帐户信息数据被病毒毁坏或者被盗，盗用者拿到盗用的资料后，必需要有用户的登录密码才能破解用户的信息数据，通过帐户数据备份服务器的信息找回单元，就可以找回用户的帐户信息数据、密码管理器登录密码、公钥文件及私钥文件。

[0048] 如图 3-2 所示，本发明的帐号密码安全加密系统的信息找回，有以下步骤：一、用户通过客户端的浏览器访问帐户数据备份服务器，输入用户的真实姓名；二、帐户数据备份服务器接收到用户输入的真实姓名，将信息发送到信息找回单元；三、信息找回单元收到指令后，将用户的真实姓名在备份数据库单元的备份表中查找是否存在与用户输入的真实姓名相匹配的最近更新的信息记录，此时，若存在相同的真实姓名时，可以通过用户正在使用的 MAC 地址和真实用户名称在备份数据库单元的备份表中查找，MAC 地址只是上传保存用户数据时区分哪个用户信息的标识，因为不同的用户的姓名可能相同，但是 MAC 地址是全球唯一的，起到辅助信息找回单元进行查找使用，否则结束操作，是则进入下一步；四、信息找回单元将备份表中相关的公钥文件、私钥文件、用户帐户信息数据提取出来，将下载信息发送到给客户端，用户通过客户端将公钥文件、私钥文件、用户帐户信息数据下载并保存到个人数据单元中；五、结束操作。

[0049] 本发明的解密、加密单元采用国际通用的公钥加密算法 RSA 加解密算法。

[0050] 如表一所示，本发明的备份数据库单元的备份表以列表的形式存储账户信息数据，备份数据库的备份表 PersonData_Bak 包括：客户端的 MAC 地址编号 MacId，用以保存客户端的 MAC 地址，如：BC-30-5B-C2-99-CB；用户名称 Username，用以保存公众的个人名称，如“张三”，待到需要找回个人资料时，通过找回单元，匹配用户名称数据找回公众的账户信息数据；登陆密码 LoginPS，如：“123456”；个人公钥文件 PublicKey，如：PublicKey.dat 文件，；个人私钥文件 Privatekey，如：PrivateKey.dat 文件；个人数据文件 PersonData，如 PersonData.dat 文件。本实例中，上传单元可以是由 delphi2009 语言编写的程序，利用 php5.0 编写的数据上传接口服务将 MAC 地址、用户名称、登陆密码、个人公钥文件、个人私钥文件、个人数据文件保存至备份数据库中的备份表中。

[0051] 实施例一：客户端硬件采用中央处理器 CPU 为 P2 以上，内存 64M 以上，硬盘空间 80G 以上，操作系统为微软 Win98 以上，浏览器为 IE5.0、Netscape4.0、火狐 Firefox1.0 或者三者的更高版本，网卡为 10M 以上，带宽为 56K 以上；账户数据备份服务端的计算机采用：操作系统为红帽子 Red Hat Enterprise Linux 4U2，加装 Tomcat5.5，数据库为 MySQL5.0，

2.0G 双核 CPU,4G 内存,100G 硬盘,100M 网卡,2M 带宽,存储装置空间为 20M 以上 ;密码管理器采样加密型 U 盘,可以是朗科科技生产的 U228 型的硬件加密型优盘闪存盘,该闪存盘具有错误密码一定次数之后能自动销毁数据,不需要安装额外的软件即可使用 ;网络通讯协议为 HTTP1.0。

[0052] 实施例二 :应用开发环境参数 :Delphi2009。可以构建基于 C/S 构架的帐号密码安全加密系统。

[0053] 登陆单元验证登陆密码正确,发送指令给解密单元的命令 :

[0054] tmpStr: = DesDecryptStr(tmpStr) ;

[0055] 当解密单元接收到解密指令后,解密单元将存储在个人数据单元中的加密帐户信息数据提取并解密的命令 :

[0056]

```
try
  Result := TDesEncrypt.DecryptStr(sText, C_USERLOGINKEY)
except
  Result := '';
end;
```

[0057] 当解密单元将帐户信息数据解密后,将解密后的帐户信息数据发送到编辑单元进行编辑的命令 :

[0058] gSysVariant.DataConfig.txInitXMLFromString(tmpStr) ;

[0059] 当编辑完毕后,编辑单元判断帐户信息数据修改过,并将修改后的帐户信息数据发送给加密单元加密,加密单元进行加密的命令 :

[0060] strList.Text: = DesEncryptStr(FXml) ;

[0061] 当加密单元对帐户信息数据进行加密后,将加密后的帐户信息数据发送到个人数据单元,个人数据单元保存后并将该信息数据上传的命令 :

[0062]

```
if UploadDataToServer(GetMacAddress, //mac  明文
                      gSysVariant.SoftConfig.UpLoadUserName,
//truename 明文
                      EncryptStr(gSysVariant.PassWord),
                      //pws 上传公匙加密后

GetTxtFromFile(gSysVariant.SoftConfig.PublicKeyFile),
                      //pubfile base64
```

[0063]

```
      GetTxtFromFile(gSysVariant.SoftConfig.PrivateKeyFile),
                            //prifile base64

      GetTxtFromFile(gSysVariant.SoftConfig.PersonDataFile),
                            //perfile base64
                            sXML) then
```

[0064] 当上传单元上传帐户信息数据到帐户数据备份服务器,帐户数据备份服务器的备份数据库单元接收并保存的命令：

[0065]

```
        public static function insertPasswordToolsInfo($macaddr,
$trueName, $password, $pubkey, $prvkey, $fileData) {
            $args = array(
                'f_macadd' =>$macaddr,
                'f_truename' =>$trueName,
                'f_password' =>$password,
                'f_pubkey' => $pubkey,
                'f_prvkey' => $prvkey,
                'f_filedata' =>$fileData
            );

$rs=Db_DBbase::getDb("passwd")->insert('t_passwordtools',$args);
            return $rs;
        }
```

[0066] 表一

[0067]

表名	字段	属性	备注
PersonData_Bak	MacId	string	Mac 地址
	UserName	string	用户名
	LoginPS	string	登陆密码
	PublicKey	string	公钥文件
	PrivateKey	string	私钥文件
	PersonDate	string	数据文件

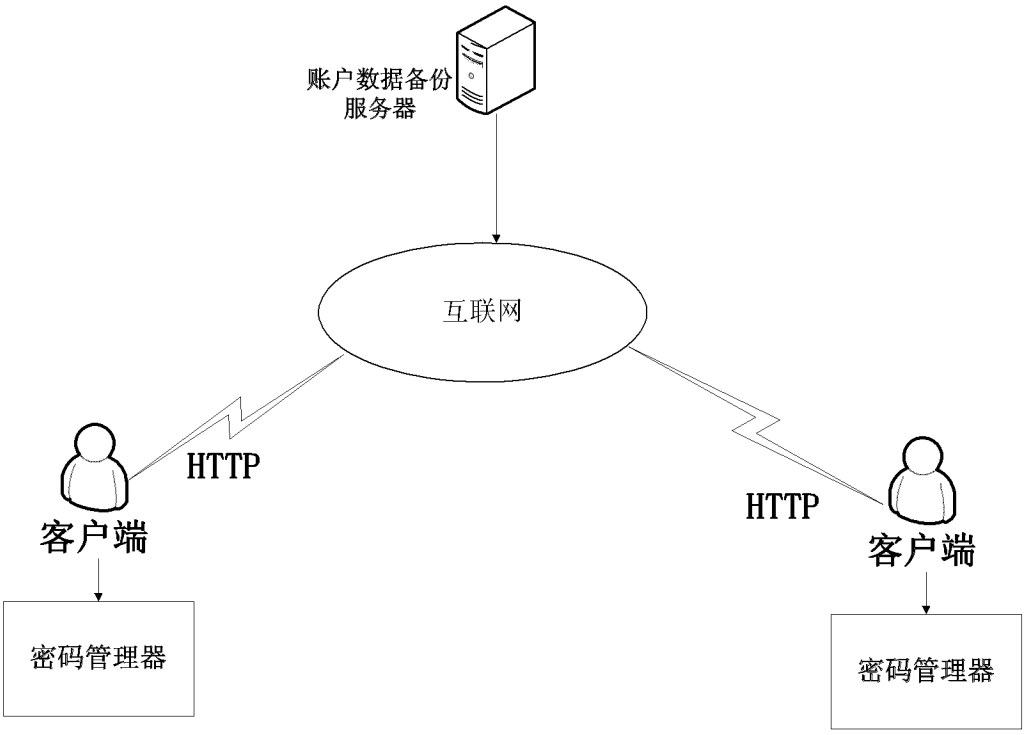


图 1

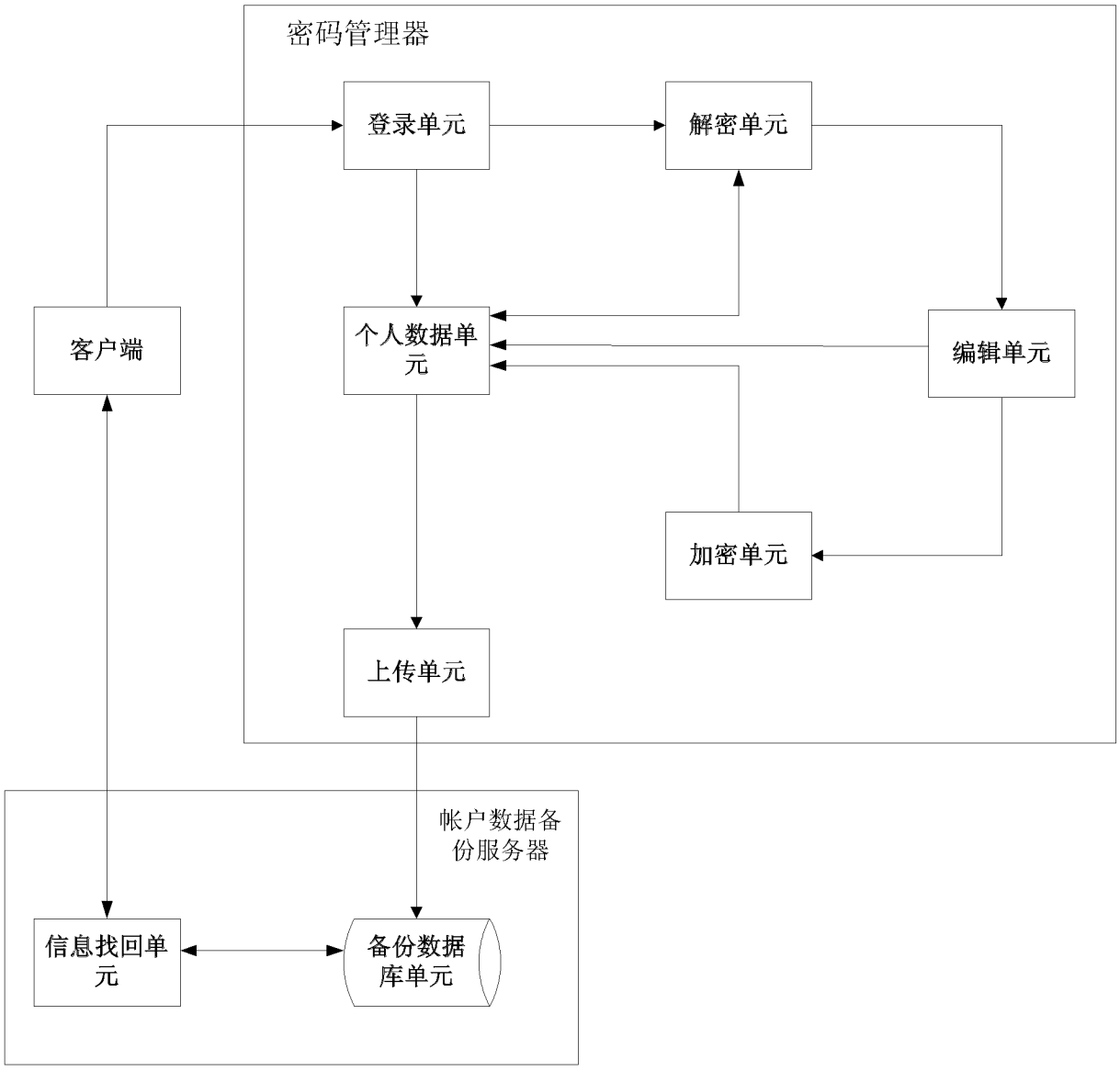

密码管理器
登录单元
解密单元
客户端
个人数据单元
编辑单元
加密单元
上传单元
帐户数据备份服务器
信息找回单元
备份数据库单元

图 2

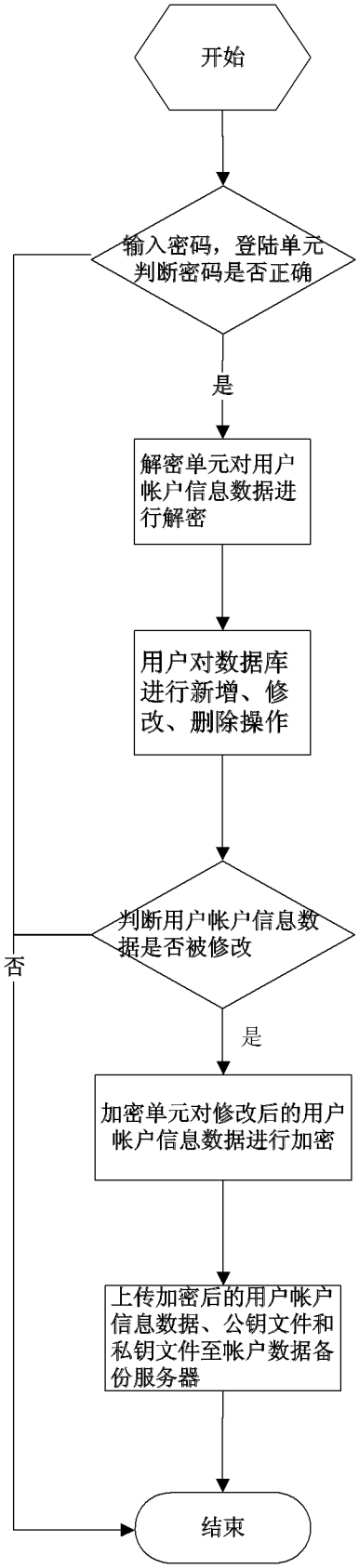

开始
输入密码，登陆单元判断密码是否正确
是
否
解密单元对用户帐户信息数据进行解密
用户对数据库进行新增、修改、删除操作
判断用户帐户信息数据是否被修改
是
否
加密单元对修改后的用户帐户信息数据进行加密
上传加密后的用户帐户信息数据、公钥文件和私钥文件至帐户数据备份服务器
结束

图 3-1

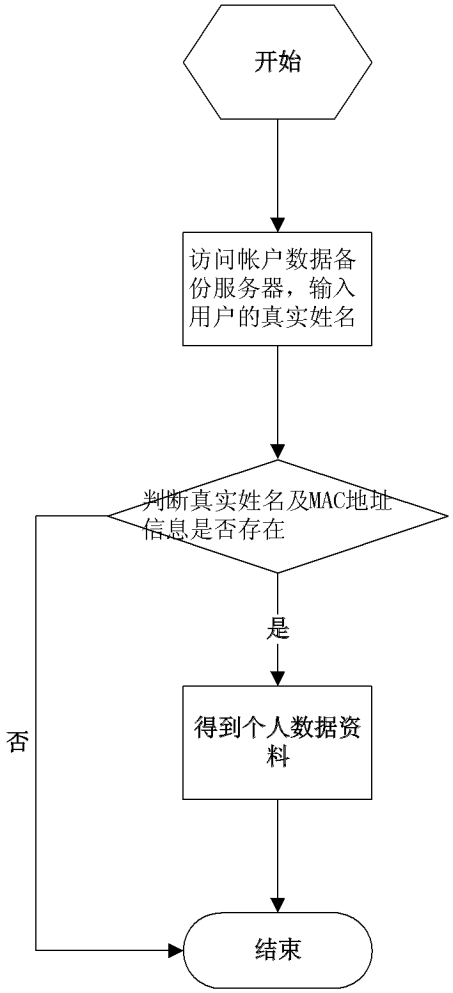

开始
访问帐户数据备份服务器，输入用户的真实姓名
判断真实姓名及MAC地址信息是否存在
是
否
得到个人数据资料
结束

图 3-2