(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 106452730 A
(43)申请公布日 2017.02.22

(21)申请号 201610824324.6

(22)申请日 2016.09.14

(71)申请人 上海烟草集团有限责任公司
地址 200082 上海市杨浦区长阳路717号

(72)发明人 胡庭川 郑捷 杨继东 樊火平
祝玉倩 陆筱蔚 王华

(74)专利代理机构 上海光华专利事务所 31219
代理人 徐秋平

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 29/12(2006.01)

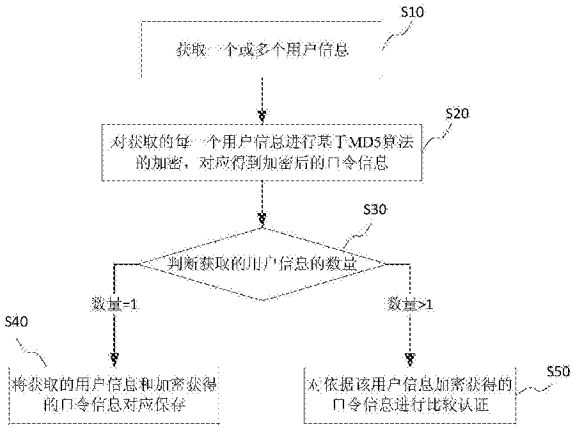
权利要求书2页 说明书7页 附图3页

(54)发明名称

基于轻量目录访问协议的MD5加密认证方法和系统

(57)摘要

本发明提供一种基于轻量目录访问协议的MD5加密认证方法和系统，包括：获取一个或多个用户信息；对获取的每一个用户信息进行基于MD5算法的加密，对应得到加密后的口令信息；判断获取的用户信息的数量：当获取的是多个用户信息时，则将获取的用户信息和加密获得的口令信息对应保存；当获取的是一个用户信息时，则对依据该用户信息加密获得的口令信息进行比较认证。本发明既可以将所有用户信息从F5 Fire Pass中迁移到Sun LDAP中，实现了跨产品的数据迁移，又可以在Sun LDAP中对用户信息进行基于MD5的比较认证，解决了Sun LDAP无法进行基于MD5认证的问题。



CN 106452730 A

1.一种基于轻量目录访问协议的MD5加密认证方法,其特征在于,包括:

获取一个或多个用户信息;

对获取的每一个用户信息进行基于MD5算法的加密,对应得到加密后的口令信息。

2.根据权利要求1所述的基于轻量目录访问协议的MD5加密认证方法,其特征在于:用户信息包括用户名和密码。

3.根据权利要求1所述的基于轻量目录访问协议的MD5加密认证方法,其特征在于:多个所述用户信息是通过导入的方式而获取的。

4.根据权利要求1所述的基于轻量目录访问协议的MD5加密认证方法,其特征在于:所述对获取的每一个用户信息进行基于MD5算法的加密,对应得到加密后的口令信息的步骤包括:

对用户信息进行基于MD5算法的加密,得到加密字符串;

对所述加密字符串进行BASE64编码转换,得到编码字符串;

在所述编码字符串上添加标识,得到口令信息。

5.根据权利要求1所述的基于轻量目录访问协议的MD5加密认证方法,其特征在于:所述基于轻量目录访问协议的MD5加密认证方法还包括:

判断获取的用户信息的数量:

当获取的是多个用户信息时,则将获取的用户信息和加密获得的口令信息对应保存;

当获取的是一个用户信息时,则对依据该用户信息加密获得的口令信息进行比较认证。

6.根据权利要求5所述的基于轻量目录访问协议的MD5加密认证方法,其特征在于:所述对依据该用户信息加密获得的口令信息进行比较认证的步骤包括:

获取该用户信息加密获得的口令信息的长度;

采用循环算法,对该用户信息加密获得的口令信息的每一个字符与该用户信息对应保存的口令信息的每一个字符进行比较:

若所有字符都相同,则认证成功;

否则,则认证失败。

7.一种基于轻量目录访问协议的MD5加密认证系统,其特征在于:包括:

获取单元,用于获取一个或多个用户信息;

加密单元,用于对获取的每一个用户信息进行基于MD5算法的加密处理,得到相应的口令信息。

8.根据权利要求7所述的基于轻量目录访问协议的MD5加密认证系统,其特征在于:所述加密单元包括:

加密子单元,用于基于MD5算法对所述获取单元获取的每一个用户信息进行加密,得到对应的加密字符串;

编码子单元,用于对所述加密字符串进行BASE64编码转换,得到编码字符串;

标识子单元,用于在所述编码字符串上添加标识,得到口令信息。

9.根据权利要求7所述的基于轻量目录访问协议的MD5加密认证系统,其特征在于:所述基于轻量目录访问协议的MD5加密认证系统还包括:处理单元、用于对应保存用户信息和口令信息的存储单元、以及用于对口令信息进行比较认证的比较认证单元;

处理单元，用于判断所述获取单元获取的用户信息的数量：

当用户信息的数量为多个时，则所述存储单元将用户信息和加密获得的口令信息对应保存；

当用户信息的数量为一个时，所述比较认证单元将依据用户信息加密获得的口令信息与所述存储单元中保存的该用户信息对应的口令信息进行比较认证。

10.根据权利要求7所述的基于轻量目录访问协议的MD5加密认证系统，其特征在于：用户信息包括用户名和密码。

基于轻量目录访问协议的MD5加密认证方法和系统

技术领域

[0001] 本发明涉及加密认证领域，特别是涉及一种基于SUN LDAP(Lightweight Directory Access Protocol，轻量目录访问协议)的MD5(Message-Digest Algorithm 5，消息摘要算法五)加密认证方法和系统。

背景技术

[0002] 基于SSL(Security Socket Layer，安全套接字层)协议构建的VPN(Virtual Private Network，虚拟专用网)技术是为远程用户安全访问企业内网的一项网络通信技术。SSL协议通过对计算机之间的整个会话进行加密，保证了在互联网上传输数据的保密性和完整性；VPN是企业或其它团体在公共网络资源中通过私有的隧道技术建立的点到点的专线，可以确保数据的机密性并且具有一定的访问控制功能，将两者结合起来形成“SSL VPN”技术，可以在公共网络中为企业设定一个有明确边界定义的网络。用户通过登录服务器并获得认证后，就能够访问相应的内网资源。

[0003] 但是，在对整个系统进行升级的过程中，需要对基于F5设备的SSL VPN认证进行升级：要将所有的用户信息(用户名和密码等等)从F5Fire Pass中迁移到Sun LDAP中。其中，F5Fire Pass通过支持现有的网络基础设施、身份管理系统和客户端/服务器操作系统，为所有应用提供了类似LAN的网络访问能力，使用户能够通过任何设备或网络安全地远程访问企业应用和数据，保证了用户的轻松访问，实现了统一的安全策略执行和访问控制，从而提高了工作人员的敏捷性和工作效率。在实现用户信息从F5Fire Pass迁移到Sun LDAP的过程中，Sun Java System Directory Server Enterprise Edition 5.2缺省用户信息的存储模式为SSHA，没有提供基于MD5的用户口令存储模式(默认是SSHA模式)。从而导致从已有基于MD5加密的用户信息，迁移到Sun LDAP中后不能正常认证。且由于用户量巨大、涉及面积广，采用直接导入后通过用户去修改密码的方式困难大，迫切需要实现MD5算法认证。

发明内容

[0004] 鉴于以上所述现有技术的缺点，本发明的目的在于提供一种基于轻量目录访问协议的MD5加密认证方法和系统，用于解决现有技术中Sun LDAP中没有提供基于MD5加密的用户信息的认证的问题。

[0005] 为实现上述目的及其他相关目的，本发明提供一种基于轻量目录访问协议的MD5加密认证方法，包括：获取一个或多个用户信息；对获取的每一个用户信息进行基于MD5算法的加密，对应得到加密后的口令信息。

[0006] 于本发明的一实施例中，用户信息包括用户名和密码。

[0007] 于本发明的一实施例中，多个所述用户信息是通过导入的方式而获取的。

[0008] 于本发明的一实施例中，所述对获取的每一个用户信息进行基于MD5算法的加密，对应得到加密后的口令信息的步骤包括：对用户信息进行基于MD5算法的加密，得到加密字符串；对所述加密字符串进行BASE64编码转换，得到编码字符串；在所述编码字符串上添加

标识，得到口令信息。

[0009] 于本发明的一实施例中，所述基于轻量目录访问协议的MD5加密认证方法还包括：判断获取的用户信息的数量：当获取的是多个用户信息时，则将获取的用户信息和加密获得的口令信息对应保存；当获取的是一个用户信息时，则对依据该用户信息加密获得的口令信息进行比较认证。

[0010] 于本发明的一实施例中，所述对依据该用户信息加密获得的口令信息进行比较认证的步骤包括：获取该用户信息加密获得的口令信息的长度；采用循环算法，对该用户信息加密获得的口令信息的每一个字符与该用户信息对应保存的口令信息的每一个字符进行比较：若所有字符都相同，则认证成功；否则，则认证失败。

[0011] 本发明还公开了一种基于轻量目录访问协议的MD5加密认证系统，包括：获取单元，用于获取一个或多个用户信息；加密单元，用于对获取的每一个用户信息进行基于MD5算法的加密处理，得到相应的口令信息。

[0012] 于本发明的一实施例中，所述加密单元包括：加密子单元，用于基于MD5算法对所述获取单元获取的每一个用户信息进行加密，得到对应的加密字符串；编码子单元，用于对所述加密字符串进行BASE64编码转换，得到编码字符串；标识子单元，用于在所述编码字符串上添加标识，得到口令信息。

[0013] 于本发明的一实施例中，所述基于轻量目录访问协议的MD5加密认证系统还包括：处理单元、用于对应保存用户信息和口令信息的存储单元、以及用于对口令信息进行比较认证的比较认证单元；处理单元，用于判断所述获取单元获取的用户信息的数量：当用户信息的数量为多个时，则所述存储单元将用户信息和加密获得的口令信息对应保存；当用户信息的数量为一个时，所述比较认证单元将依据用户信息加密获得的口令信息与所述存储单元中保存的该用户信息对应的口令信息进行比较认证。

[0014] 于本发明的一实施例中，用户信息包括用户名和密码。

[0015] 如上所述，本发明的一种基于轻量目录访问协议的MD5加密认证方法和系统，实现了基于LDAP的MD5认证算法，实现了Sun Java System Directory Server Enterprise Edition的MD5存储模式，确保了已有的基于MD5加密的用户信息能够批量导入到现有的Sun LDAP的产品中，实现了跨铲平的数据迁移；并且，本发明还解决了Sun LDAP不能提供基于MD5认证的问题，实现了用户信息的正常认证操作。

附图说明

[0016] 图1显示为本发明实施例公开的一种基于轻量目录访问协议的MD5加密认证方法的流程示意图。

[0017] 图2显示为本发明实施例公开的一种基于轻量目录访问协议的MD5加密认证方法中对用户信息进行基于MD5算法加密，获得口令信息的流程示意图。

[0018] 图3显示为本发明实施例公开的一种基于轻量目录访问协议的MD5加密认证方法中对用户信息进行比较认证的流程示意图。

[0019] 图4显示为本发明实施例公开的一种基于轻量目录访问协议的MD5加密认证系统的原理结构示意图。

[0020] 元件标号说明

[0021] S10～S50,S21～S23, 步骤

[0022] S51～S52

[0023] 410 获取单元

[0024] 420 加密单元

[0025] 421 加密子单元

[0026] 422 编码子单元

[0027] 423 标识子单元

[0028] 430 存储单元

[0029] 440 比较认证单元

[0030] 450 处理单元

具体实施方式

[0031] 以下通过特定的具体实例说明本发明的实施方式,本领域技术人员可由本说明书所揭露的内容轻易地了解本发明的其他优点与功效。本发明还可以通过另外不同的具体实施方式加以实施或应用,本说明书中的各项细节也可以基于不同观点与应用,在没有背离本发明的精神下进行各种修饰或改变。需说明的是,在不冲突的情况下,以下实施例及实施例中的特征可以相互组合。

[0032] 请参阅附图。需要说明的是,以下实施例中所提供的图示仅以示意方式说明本发明的基本构想,遂图式中仅显示与本发明中有关的组件而非按照实际实施时的组件数目、形状及尺寸绘制,其实际实施时各组件的型态、数量及比例可为一种随意的改变,且其组件布局型态也可能更为复杂。

[0033] 本发明的一种基于轻量目录访问协议的MD5加密认证方法和系统,通过对用户信息构成的密码文本进行基于MD5算法的加密,从而实现了对已有的基于MD5加密的用户信息的批量导入;进一步地,本发明还解决了Sun LDAP下基于MD5的认证的问题:对用户信息进行基于MD5算法的加密处理后,再进行比较认证,实现了用户信息的认证。

[0034] 实施例1

[0035] 本实施例公开了一种应用于系统升级过程中的基于LDAP(轻量目录访问协议)的MD5加密认证方法,尤其是在对基于F5设备的SSL VPN认证进行升级时,使用本实施例的基于LDAP的MD5加密认证方法可以将所有用户信息从F5Fire Pass中迁移到Sun LDAP中。

[0036] 为了要解决所有用户信息的迁移导入问题,需要根据Sun LDAP提供的接口,单独开发算法来实现MD5的加密和认证。

[0037] 如图1所示,本实施例的基于LDAP的MD5加密认证方法包括:

[0038] 步骤S10,获取多个用户信息;

[0039] 其中,用户信息包括但不限于用户名和密码等等。

[0040] 通常情况下,多个用户信息是已经存在于F5设备中。多个用户信息的获取是直接将多个用户信息从F5设备导入到Sun LDAP中。

[0041] 在本实施例中,是通过以下指令代码来实现已有的用户信息从F5设备导入至Sun LDAP中:

[0042] dsconf create-suffix dc=hntel,dc=com

[0043] dsconf create-suffix ou＝people,dc＝hntel,dc＝com

[0044] ldapmodify-a-D"cn＝Directory Manager"-w Hn8tel3E-f 134.ldif

[0045] ldapmodify-a-D"cn＝Directory Manager"-w Hn8tel3E-c-f 135.ldif

[0046] 进一步地,在导入了多个用户信息后,在本实施例中,还需要对导入的用户信息进行验证,验证其是否可用:

[0047] ldapsearch-L-b dc＝hntel,dc＝com-D"cn＝Directory Manager"-w Hn8tel3E cn＝ly-test

[0048] ldapsearch-L 390-b dc＝hntel,dc＝com-D"cn＝Directory Manager"-w Hn8tel3E cn＝ly-test

[0049] 步骤S20,对获取的每一个用户信息进行基于MD5算法的加密,对应得到加密后的口令信息。如图2所示,具体包括:

[0050] 步骤S21,对用户信息进行基于MD5算法的加密,得到加密字符串:

[0051] MD5算法用于确保信息传输的完整和一致,是计算机广泛使用的杂凑算法之一(又译摘要算法、哈希算法),是让大容量信息在用数字签名软件签署私人密钥前被"压缩"成一种保密的格式(就是把一个任意长度的字节串变换成一定长的十六进制数字串)。目前,该算法已经非常成熟,因此,在本实施例中不再详细赘述。本实施例只是简单的通过调用开源的MD5算法函数对用户信息进行加密,从而得到加密字符串。

[0052] 步骤S22,对加密字符串进行BASE64编码转换,得到编码字符串:

[0053] 对加密后的加密字符串进行BASE64编码,再对编码后的数据进行转换,得到编码字符串。其中,采用BASE64进行编码,具有不可读性,即所编码的数据不会被直接看到。

[0054] 步骤S23,在编码字符串上添加标识,得到口令信息。

[0055] 在转换后得到的编码字符串前加上标识,以确保最终的加密格式和原始数据中的密码串相同。标识是在编写算法时人为设定的,其具有唯一性。在本实施例中,标识为{MD5}。

[0056] 由步骤S21～步骤S23不难看出,步骤S20其实是对每一个用户信息的基于MD5算法的加密处理。在本实施例中,步骤S20所对应的程序代码为:

[0057] String password;

[0058] MessageDigest md＝MessageDigest.getInstance("MD5");

[0059] md.update(password.getBytes());

[0060] byte[]bs＝md.digest();

[0061] byte[]base64MD5Password＝Base64.encode(bs)

[0062] 进一步地,由于导入的多个用户信息是F5设备中已经存在的,因此,本实施例的基于LDAP的MD5加密认证方法还包括:

[0063] 步骤S30,判断获取的用户信息的数量:

[0064] 步骤S40,当获取的用户信息为多个时,则将多个用户信息和加密获得的口令信息对应保存。

[0065] 当获取的用户信息为多个时,表示此时执行的是多个用户信息的导入操作,因此,需要将依据多个用户信息加密获得的口令信息与对应的用户信息配对保存,以便于以后的用户信息的比较认证。

[0066] 实施例2

[0067] 本实施例公开了一种基于LDAP(轻量目录访问协议)的MD5加密认证方法,用于在Sun LDAP中对用户信息进行基于MD5的比较认证,从而实现用户信息的认证。

[0068] 如图1所示,本实施例的基于LDAP的MD5加密认证方法包括:

[0069] 步骤S10,获取一个用户信息:

[0070] 其中,用户信息包括但不限于用户名和密码等等。

[0071] 在本实施例中,一个用户信息的获取通常情况下是用户通过显示界面直接输入的。

[0072] 步骤S20,对获取的用户信息进行基于MD5算法的加密,对应得到加密后的口令信息。

[0073] 步骤S20与实施例1中的步骤S20的处理过程完全相同,在此不再赘述。

[0074] 步骤S30,判断获取的用户信息的数量:

[0075] 步骤S50,当获取的用户信息的数量为一个时,对依据该用户信息加密获得的口令信息与该用户信息对应保存的口令信息进行比较认证:如果相同,则认证成功;否则,则认证失败。

[0076] 其中,如图3所示,步骤S50具体包括:

[0077] 步骤S51,获取加密获得的口令信息的长度;

[0078] 由步骤S23可知,口令信息其实是一个字符串,因此,首先需要获取加密获得的口令信息对应的字符串的长度;

[0079] 步骤S52,采用循环算法,对加密获得的口令信息的每一个字符与保存的口令信息的每一个字符进行比较:

[0080] 若所有字符都相同,则认证成功;

[0081] 否则,则认证失败。

[0082] 在本实施例中,是采用如下程序代码实现比较认证的,且最后通过输出“0”来表示认证成功,输出“1”表示认证不成功:

[0083]
```
char * userpwd, char * dbpwd
int i, len = strlen(userpwd);
for (i = 0; i < len; i++) {
if ((userpwd[i] ^ 42) != dbpwd[i])
```

[0084]
```
return 1;                    }
return 0;
```

[0085] 上面各种方法的步骤划分,只是为了描述清楚,实现时可以合并为一个步骤或者对某些步骤进行拆分,分解为多个步骤,只要包含相同的逻辑关系,都在本专利的保护范围内;对算法中或者流程中添加无关紧要的修改或者引入无关紧要的设计,但不改变其算法和流程的核心设计都在该专利的保护范围内。

[0086] 此外,需要说明的是,实施例1和实施例2中的基于LDAP的MD5加密认证方法其实是MD5加密认证方法的两种不同情况而已。并且,在实际使用中,为了使得本发明的基于LDAP的MD5加密认证方法有效,需要在Sun Java System Directory Server Enterprise

Edition5.2服务器上进行基于LDAP的MD5加密认证方法Plug-in的注册与Entry的创建;并最后重新启动Directory Server服务并验证基于LDAP的MD5加密认证方法生效:

[0087] 首先,要从F5设备中导出原始数据并进行数据的格式转换;

[0088] 其次,编写基于MD5算法的加密程序(步骤S20)和比较认证程序(步骤S50),并根据Sun LDAP提供的接口编写相应的基于LDAP的MD5加密认证方法Plug-in,并完成编译,生成可执行的Plug-in;

[0089] 然后,配置基于Sun LDAP的MD5加密认证算法Plug-in,使之生效:

[0090] dsadm start'/sunldap/dsee/dsinst'

[0091] dsconf create-plugin-H/sunldap/dsee/ds6/examples/md5test-plugin.so-F md5_init-Y pwdstoragescheme"MD5"

[0092] dsconf set-plugin-prop"MD5"feature:md5-password-storage-scheme version:6.3desc:"Exclusive-or example(MD5)"

[0093] dsconf enable-plugin"MD5"

[0094] dsadm stop'/sunldap/dsee/dsinst'

[0095] dsadm start'/sunldap/dsee/dsinst'

[0096] dsconf set-server-prop pwd-storage-scheme:MD5

[0097] 最后,验证基于LDAP的MD5加密认证算法配置的正确性:

[0098] pwdhash-D/sunldap/dsee/dsinst-s MD5password

[0099] pwdhash-D/sunldap/dsee/dsinst-c"{md5}X03MO1qnZdYdgyfeuILPmQ==" password

[0100] 实施例3

[0101] 本实施例公开了一种基于LDAP的MD5加密认证系统,如图4所示,包括:

[0102] 获取单元410,用于获取一个或多个用户信息;其中,用户信息包括但不限于用户名和密码等等。

[0103] 加密单元420,用于对获取的每一个用户信息进行基于MD5算法的加密处理,得到相应的口令信息。

[0104] 在本实施例中,加密单元420包括:加密子单元421、编码子单元422和标识子单元423。其中,

[0105] 加密子单元421,用于基于MD5算法对获取单元410获取的每一个用户信息进行加密,得到对应的加密字符串;

[0106] 编码子单元422,用于对加密字符串进行BASE64编码转换,得到编码字符串;

[0107] 标识子单元423,用于在所述编码字符串上添加标识,得到口令信息。

[0108] 存储单元430,用于将用户信息和加密获得的口令信息对应保存;

[0109] 比较认证单元440,用于将依据用户信息对加密获得口令信息进行比较认证。

[0110] 处理单元450,用于对获取单元410获取的用户信息的数量进行判断,从而控制加密单元420、存储单元430和比较认证单元440:

[0111] 当处理单元450判断获取单元410获取的用户信息的数量为多个时,则控制加密单元420对获取的每一个用户信息进行基于MD5算法的加密,获得对应的口令信息,并最终将所有用户信息和加密获得的口令信息对应保存至存储单元430中;

[0112] 当处理单元450判断获取单元410获取的用户信息的数量为一个时，则控制加密单元420对获取的该用户信息进行基于MD5算法的加密，获得对应的口令信息；然后比较认证单元440将获得的口令信息与存储单元460中保存的该用户信息对应的口令信息进行比较认证。

[0113] 此外，为了突出本发明的创新部分，本实施例中并没有将与解决本发明所提出的技术问题关系不太密切的单元引入，但这并不表明本实施例中不存在其它的单元。

[0114] 并且，本实施例为与实施例1或者实施例2相对应的系统实施例，本实施例可与实施例1或者实施例2互相配合实施。实施例1或者实施例2中提到的相关技术细节在本实施例中依然有效，为了减少重复，这里不再赘述。相应地，本实施例中提到的相关技术细节也可应用在实施例1或者实施例2中。

[0115] 综上所述，本发明的一种基于轻量目录访问协议的MD5加密认证方法和系统，实现了基于LDAP的MD5认证算法，实现了Sun Java System Directory Server Enterprise Edition的MD5存储模式，确保了已有的基于MD5加密的用户信息能够批量导入到现有的Sun LDAP的产品中，实现了跨铲平的数据迁移；并且，本发明还解决了Sun LDAP不能提供基于MD5认证的问题，实现了用户信息的正常认证操作所以，本发明有效克服了现有技术中的种种缺点而具高度产业利用价值。

[0116] 上述实施例仅例示性说明本发明的原理及其功效，而非用于限制本发明。任何熟悉此技术的人士皆可在不违背本发明的精神及范畴下，对上述实施例进行修饰或改变。因此，举凡所属技术领域中具有通常知识者在未脱离本发明所揭示的精神与技术思想下所完成的一切等效修饰或改变，仍应由本发明的权利要求所涵盖。

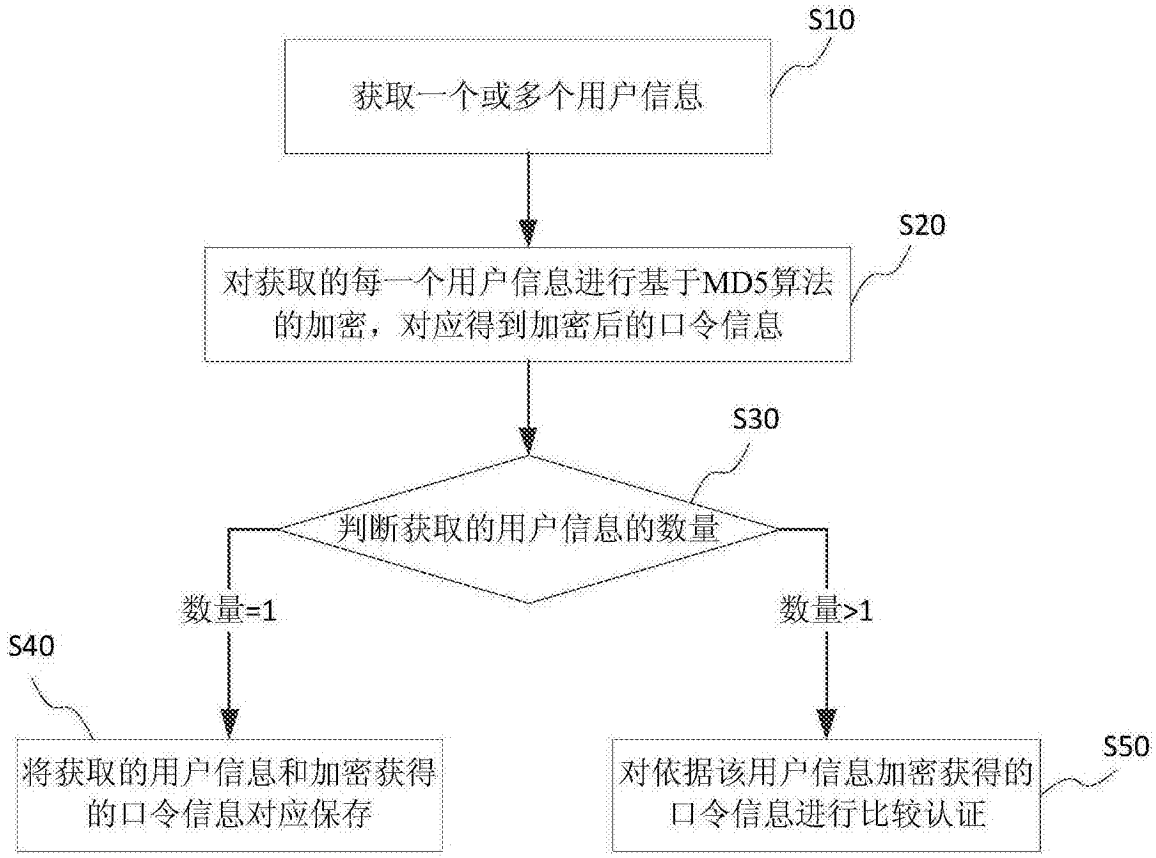

S10
获取一个或多个用户信息
S20
对获取的每一个用户信息进行基于MD5算法的加密，对应得到加密后的口令信息
S30
判断获取的用户信息的数量
数量=1
数量>1
S40
将获取的用户信息和加密获得的口令信息对应保存
对依据该用户信息加密获得的口令信息进行比较认证
S50

图1

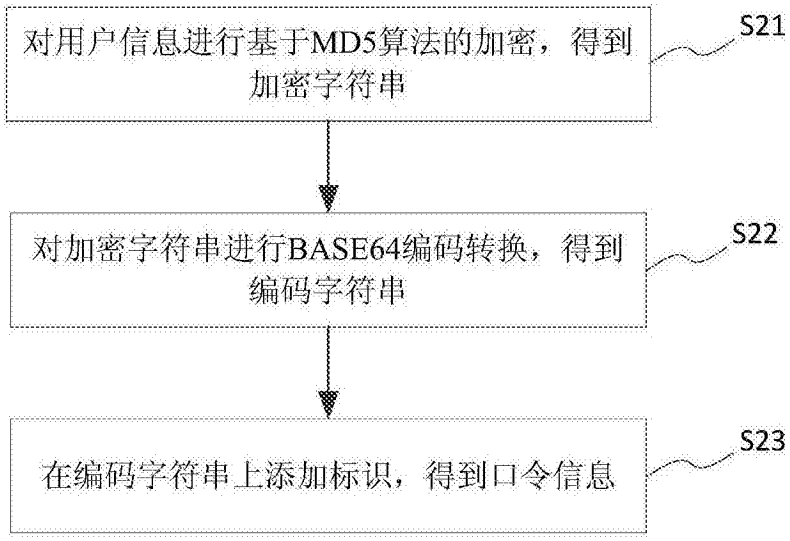

对用户信息进行基于MD5算法的加密，得到加密字符串
S21
对加密字符串进行BASE64编码转换，得到编码字符串
S22
在编码字符串上添加标识，得到口令信息
S23

图2

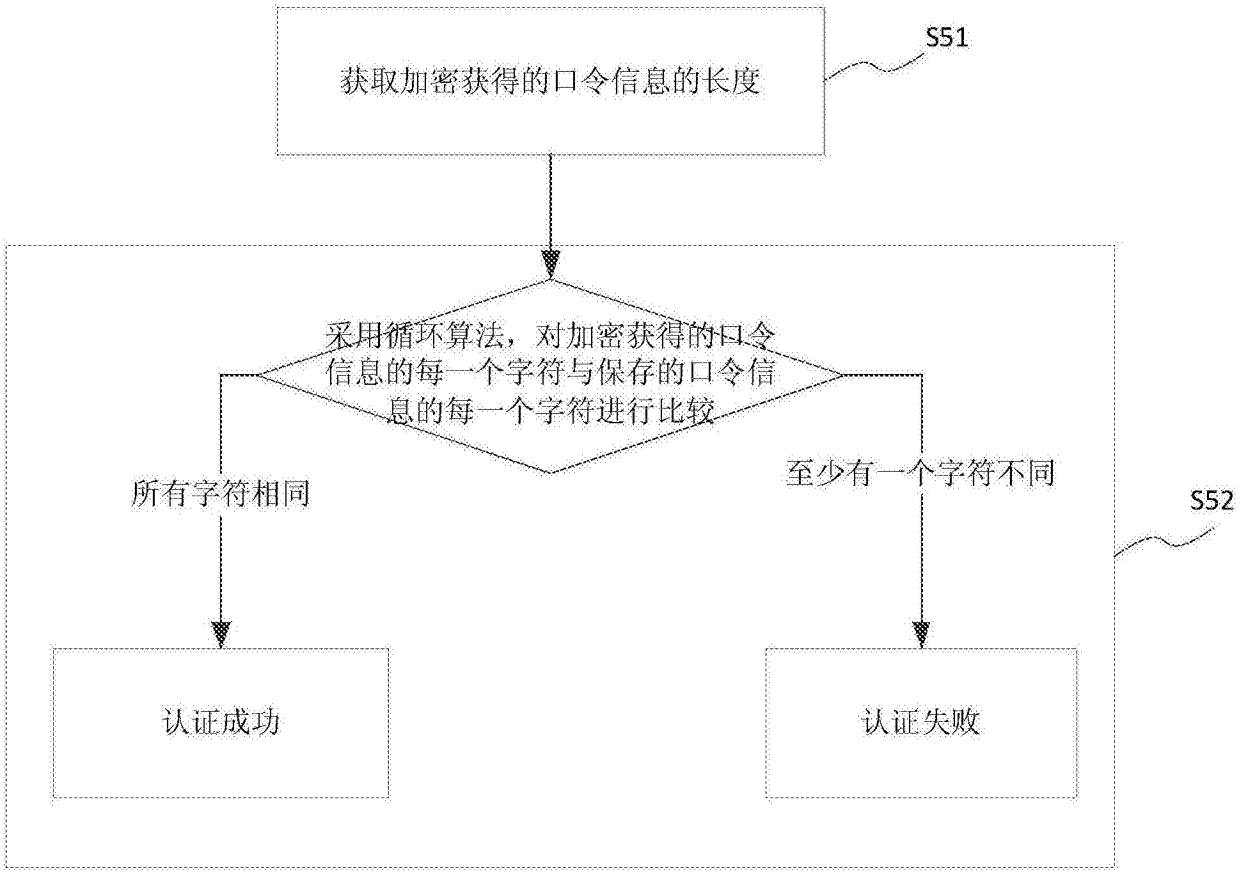

获取加密获得的口令信息的长度
S51
采用循环算法，对加密获得的口令信息的每一个字符与保存的口令信息的每一个字符进行比较
所有字符相同
至少有一个字符不同
S52
认证成功
认证失败

图3

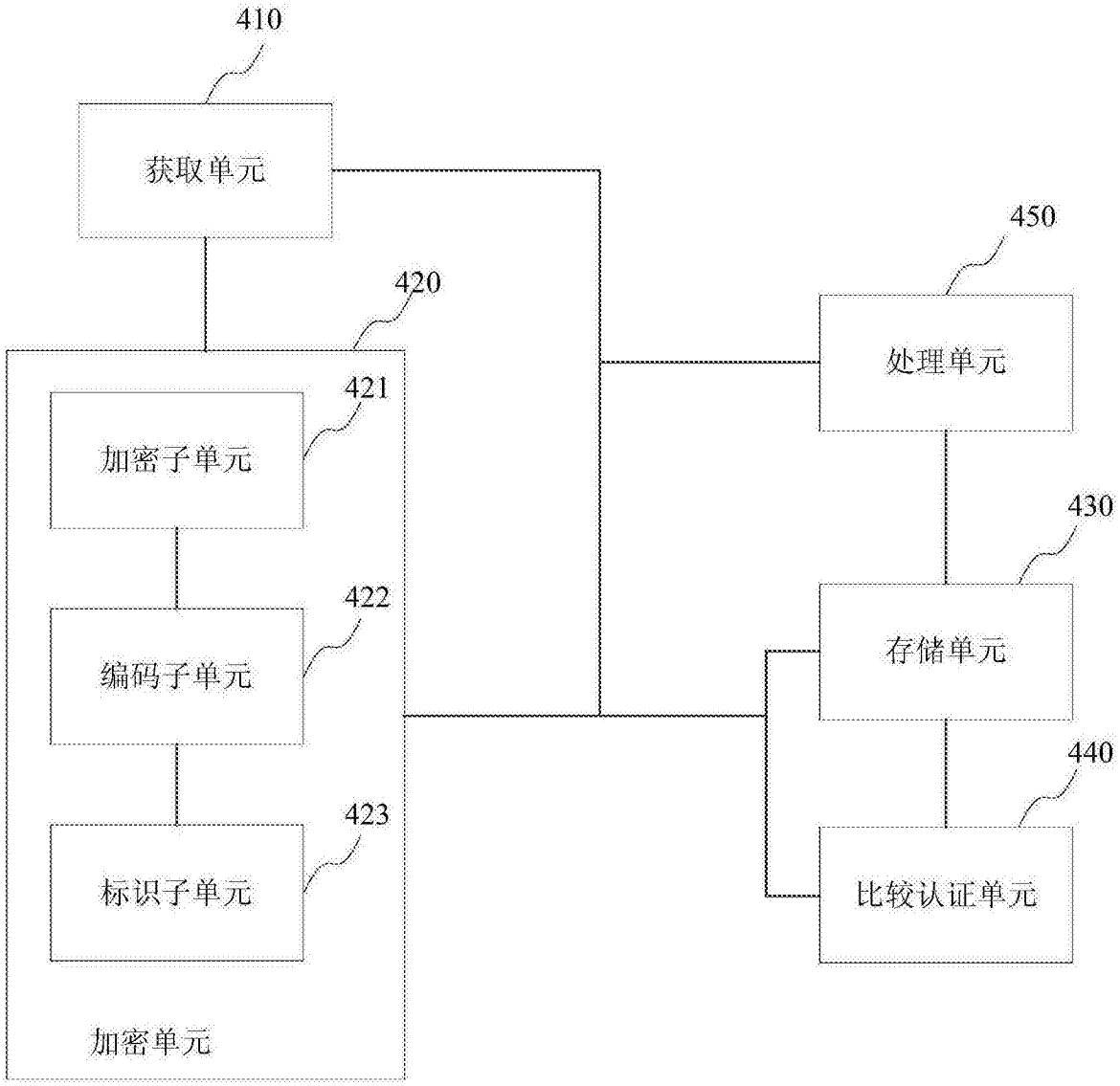

410
获取单元
420
加密子单元
421
编码子单元
422
标识子单元
423
加密单元
450
处理单元
430
存储单元
440
比较认证单元

图4