(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 104243494 B
(45)授权公告日 2018.01.23

(21)申请号 201410532214.3

(22)申请日 2014.10.11

(65)同一申请的已公布的文献号
申请公布号 CN 104243494 A

(43)申请公布日 2014.12.24

(73)专利权人 上海众人网络安全技术有限公司
地址 201821 上海市嘉定工业区叶城路1411号4幢211室

(72)发明人 谈剑锋 郑建华

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 孟金喆

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

(56)对比文件
CN 101917270 A,2010.12.15,
CN 101917270 A,2010.12.15,
CN 104079413 A,2014.10.01,
CN 1625101 A,2005.06.08,
freud_lv.TC、ARQC、AAC及ARPC校验方式.《www.aiuxian.com/article/p-1044444.html》.2014,全文.

审查员 孙丽

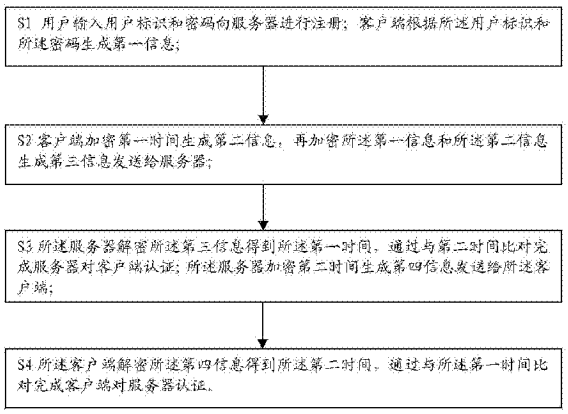
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种数据处理方法

(57)摘要

本发明公开一种数据处理方法，包括步骤：用户输入用户标识和密码向服务器进行注册；客户端根据所述用户标识和所述密码生成第一信息；客户端加密第一时间生成第二信息，再加密所述第一信息和所述第二信息生成第三信息发送给服务器；所述服务器解密所述第三信息得到所述第一时间，通过与第二时间比对完成服务器对客户端认证；所述服务器加密所述第二时间生成第四信息发送给所述客户端。本发明实现了网络身份认证、数据加密传输、数据完整性校验，具有更好的技术前景。



CN 104243494 B

1.一种数据处理方法,其特征在于,包括如下步骤:

S1用户输入用户标识和密码向服务器进行注册;客户端根据所述用户标识和所述密码生成第一信息;

S2客户端加密第一时间生成第二信息,再加密所述第一信息和所述第二信息生成第三信息发送给服务器;

S3所述服务器解密所述第三信息得到所述第一时间,通过与第二时间比对完成服务器对客户端认证;所述服务器加密所述第二时间生成第四信息发送给所述客户端;

S4所述客户端解密所述第四信息得到所述第二时间,通过与所述第一时间比对完成客户端对服务器认证;

S5,所述客户端和所述服务器分别生成会话密钥并使用所述会话密钥加密会话数据进行数据会话;

所述S1步骤具体为:用户输入所述用户标识和其一一对应的所述密码;所述客户端采用第一算法计算所述用户标识和所述密码生成所述第一信息,并将所述用户标识以及所述第一信息发送至所述服务器;

所述服务器产生随机的第一密钥和第二密钥,所述服务器将所述第一密钥与加密算法结合,生成一个与所述第一密钥相关的加密函数,并且所述服务器将所述第二密钥与解密算法结合,生成一个与所述第二密钥相关的解密函数,所述服务器将所述加密函数与所述解密函数发送至所述客户端;

所述服务器存储所述第一密钥、所述第二密钥、所述加密算法、所述解密算法、所述用户标识以及所述第一信息;

所述客户端存储所述加密函数和所述解密函数;

所述S2步骤具体为:所述客户端通过所述加密函数对所述第一时间加密生成所述第二信息;

所述客户端采用第二算法对所述第二信息和所述第一信息进行计算后并通过所述加密函数再次加密生成所述第三信息;

所述客户端发送所述用户标识和所述第三信息给所述服务器;

所述S3步骤具体为:所述服务器存储有用户标识档案,所述用户标识档案为存储所有用户标识的列表;

所述服务器接收到所述客户端发送的所述用户标识,并判断所述用户标识是否存在于所述用户标识档案内,如果是,则用户身份的初步认证成功;

所述服务器通过所述加密算法和所述第二密钥对所述第二时间加密生成第四信息;

所述服务器接收到所述客户端发送的所述第三信息,通过所述解密算法和所述第一密钥对所述第三信息进行解密,再与其存储的所述第一信息通过所述第二算法进行计算得到所述第二信息;所述服务器再次通过所述解密算法和所述第一密钥对所述第二信息进行解密,得到所述第一时间;

所述服务器判断得到的所述第一时间和所述第二时间的时间差,如果所述时间差小于预设值,则所述服务器对所述客户端认证成功,否则认证失败,结束认证;

所述服务器将所述第四信息发送给所述客户端;

所述S4步骤具体为:所述客户端接收到所述服务器发送的所述第四信息,通过所述解

密函数解密所述第四信息得到所述第二时间；

所述客户端判断得到的所述第二时间和所述第一时间的时间差，如果所述时间差小于预设值，则所述客户端对所述服务器认证成功，继续执行以下步骤，否则认证失败，结束认证；

所述S5步骤具体为：所述客户端采用第三算法计算所述第二信息生成第五信息，通过所述加密函数对所述第二信息以及所述第五信息加密生成所述会话密钥；

所述服务器采用所述第三算法计算解密得到的所述第二信息生成所述第五信息，通过所述加密算法和所述第一密钥对所述第二信息以及所述第五信息加密生成会话密钥；

所述客户端和所述服务器还存储有公用加密算法和公用解密算法；

所述客户端使用所述会话密钥和所述公用加密算法加密所述会话数据生成第一数据；所述客户端采用所述第一算法对所述会话数据进行计算生成第二数据；所述客户端发送所述第一数据和所述第二数据给所述服务器；

所述服务器接收所述第一数据和所述第二数据，通过所述公用解密算法

和所述会话密钥解密所述第一数据，得到所述会话数据；

所述服务器通过所述第一算法计算所述会话数据，并将计算结果与接收到的所述第二数据进行比对，如果相同，则所述会话数据具有完整性，否则所述会话数据不完整，为不合法；

其中，所述第一算法为哈希算法，所述第二算法为异或运算以及所述第三算法为取反运算。

2.如权利要求1所述的一种数据处理方法，其特征在于：

所述第一时间为所述客户端选取的当前时间。

3.如权利要求1所述的一种数据处理方法，其特征在于：

所述第二时间为所述服务器选取的当前时间。

4.如权利要求1所述的一种数据处理方法，其特征在于：

所述客户端和所述服务器生成相同的所述第一信息。

5.如权利要求1所述的一种数据处理方法，其特征在于：

所述用户标识包括用于唯一标识用户的信息。

一种数据处理方法

技术领域

[0001] 本发明涉及网络信息安全领域，尤其涉及数据处理方法。

背景技术

[0002] 随着互联网的不断发展，越来越多的人们开始尝试在线交易。然而病毒、黑客、网络钓鱼以及网页仿冒诈骗等恶意威胁，给在线交易的安全性带来了极大的挑战。层出不穷的网络犯罪，引起了人们对网络身份的信任危机，如何在网络交易中认证真实身份，防止身份冒用、网络中传输的信息保密等问题又一次成为人们关注的焦点。

[0003] 在互联网中进行数据交互存在许多不安全因素，尤其是一些机密数据更易遭到黑客的入侵。因此，数据在进行网络传输前需要先进行身份的认证，防止冒充。数据在传输时，需要采用安全的加密算法进行加密才能保证数据即使被黑客截获，其内容也不会泄露。同时，需要在接收数据时能够对数据进行校验，检查数据是否被篡改，防止中间人冒充。

发明内容

[0004] 本发明的目的，就是提出一种能够实现网络身份认证、数据加密以及数据完整性校验的数据处理方法。

[0005] 本发明的技术方案包括如下步骤：

[0006] S1用户输入用户标识和密码向服务器进行注册；客户端根据所述用户标识和所述密码生成第一信息；

[0007] S2客户端加密第一时间生成第二信息，再加密所述第二信息和所述第一信息生成第三信息发送给服务器；

[0008] S3所述服务器解密所述第三信息得到所述第一时间，通过与第二时间比对完成服务器对客户端认证；所述服务器加密第二时间生成第四信息发送给所述客户端；

[0009] S4所述客户端解密所述第四信息得到所述第二时间，通过与所述第一时间比对完成客户端对服务器认证。

[0010] 本发明能够实现网络中身份识别、传输的数据加密，具有更优的技术效果。

[0011] 进一步优选地，所述第一时间为所述客户端选取的当前时间。

[0012] 进一步优选地，所述第二时间为所述服务器选取的当前时间。

[0013] 进一步优选地，所述S1步骤具体为：用户输入所述用户标识和其一一对应的所述密码；所述客户端采用第一算法计算所述用户标识和所述密码生成所述第一信息，并将所述用户标识以及所述第一信息发送至所述服务器；

[0014] 所述服务器产生随机的第一密钥和第二密钥，所述服务器将所述第一密钥与加密算法结合，生成一个与所述第一密钥相关的加密函数，并且所述服务器将所述第二密钥与解密算法结合，生成一个与所述第二密钥相关的解密函数，所述服务器将所述加密函数与所述解密函数发送至所述客户端；

[0015] 所述服务器存储所述第一密钥、所述第二密钥、所述加密算法、所述解密算法、所

述用户标识以及所述第一信息；

[0016] 所述客户端存储所述加密函数和所述解密函数；

[0017] 所述S2步骤具体为：所述客户端通过所述加密函数对所述第一时间加密生成所述第二信息；所述客户端采用第一算法计算用户输入的所述用户标识和所述密码生成所述第一信息；

[0018] 所述客户端采用第二算法对所述第二信息和所述第一信息进行计算后并通过加密函数再次加密生成所述第三信息；

[0019] 所述客户端发送所述用户标识和所述第三信息给所述服务器；

[0020] 所述S3步骤具体为：所述服务器存储有用户标识档案，所述用户标识档案为存储所有用户标识的列表；所述服务器接收到所述客户端发送的所述用户标识，并判断所述用户标识是否存在于所述用户标识档案内，如果是，则用户身份的初步认证成功。本发明通过增加初步身份认证，提高了身份认证的安全性。

[0021] 所述服务器通过所述加密算法和所述第二密钥对所述第二时间加密生成第四信息；

[0022] 所述服务器接收到所述客户端发送的所述第三信息，通过所述解密算法和所述第一密钥对所述第三信息进行解密，再与其存储的所述第一信息通过所述第二算法进行计算得到所述第二信息；所述服务器再次通过所述解密算法和所述第一密钥对所述第二信息进行解密，得到所述第一时间；

[0023] 所述服务器判断得到的所述第一时间和所述第二时间的时间差，如果所述时间差小于预设值(此预设值视网络延迟情况而定)，则所述服务器对所述客户端认证成功，否则认证失败，结束认证；

[0024] 所述服务器对所述客户端认证成功后，所述服务器将所述第四信息发送给所述客户端；

[0025] 所述S4步骤具体为：所述客户端接收到所述服务器发送的所述第四信息，通过解密函数解密所述第四信息得到所述第二时间；

[0026] 所述客户端判断得到的所述第二时间和所述第一时间的时间差，如果所述时间差小于预设值(此预设值视网络延迟而定)，则所述客户端对所述服务器认证成功，继续执行以下步骤，否则认证失败，结束认证。

[0027] 本发明的客户端与服务器端采取双向认证，防止假冒攻击。

[0028] 进一步优选地，所述S5步骤具体为：所述客户端采用第三算法计算所述第二信息生成第五信息，通过所述加密函数对所述第二信息以及所述第五信息加密生成所述会话密钥；

[0029] 所述服务器采用所述第三算法计算解密得到的所述第二信息生成所述第五信息，通过所述加密算法和所述第一密钥对所述第二信息以及所述第五信息加密生成会话密钥；

[0030] 所述客户端和所述服务器还存储有公用加密算法和公用解密算法；

[0031] 所述客户端和所述服务器通过公用加密算法和所述会话密钥对所述会话数据进行加密，以及所述客户端和所述服务器通过所述公用解密算法和所述会话密钥对加密后的所述会话数据进行解密，整个会话过程全称加密保护，防止会话数据内容泄露。

[0032] 具体的，所述客户端/服务器使用所述会话密钥和所述公用加密算法加密所述会

话数据生成第一数据；所述客户端/服务器采用所述第一算法对所述会话数据进行计算生成第二数据；所述客户端/服务器发送所述第一数据和所述第二数据给所述服务器/客户端；所述服务器/客户端接收所述第一数据和所述第二数据，通过所述公用解密算法和所述会话密钥解密所述第一数据，得到所述会话数据；所述服务器/客户端通过所述第一算法计算所述会话数据，并将计算结果与接收到的所述第二数据进行比对，如果相同，则所述会话数据具有完整性，否则所述会话数据不完整，为不合法。

[0033] 进一步优选地，所述客户端和所述服务器生成相同的所述第一信息，所述服务器存储第一信息。

[0034] 进一步优选地，所述客户端和所述服务器生成的所述会话密钥是相同的，在会话数据进行加密传输时，减少密钥的传输，能够保证密钥的安全。

[0035] 进一步优选地，所述用户标识包括用于唯一标识用户的信息。

[0036] 进一步优选地，所述用户标识档案为存储所有合法用户的用户标识的列表。

[0037] 本发明提供的一种数据处理方法能够带来以下至少一种有益效果：

[0038] 1、本发明中进行身份认证时采用加解密算法和密钥融合在一起，不分算法和密钥，避开了密钥存储的安全问题。

[0039] 2、本发明中客户端的加解密函数是由服务器端结合随机产生的密钥和加解密算法得来的，所以每个客户端的算法不一样，一个客户的安全插件泄露不影响系统的整体安全性。

[0040] 3、本发明中的客户端与服务器端采取双向认证，能够有效防止假冒攻击。

[0041] 4、本发明在进行数据会话过程时，客户端与服务器端分别生成相同的密钥，结合公用加密算法和解密算法进行数据加密传输，能够防止数据泄露，并且减少密钥传输的问题，能够有效保证密钥的安全。

[0042] 5、本发明通过对数据进行完整性校验，可检验数据的内容是否被篡改，可防抵赖，防止中间人攻击。

附图说明

[0043] 下面结合附图和具体实施方式对本发明作进一步详细说明：

[0044] 图1为本发明中数据处理方法实施例的步骤示意图。

具体实施方式

[0045] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来说，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。

[0046] 作为本发明的一个具体实施例，图1为本发明提供的数据处理方法实施例步骤示意图。本发明提供了一种数据处理方法，包括如下步骤：

[0047] S1用户输入用户标识和密码向服务器进行注册；客户端根据所述用户标识和所述密码生成第一信息；

[0048] S2客户端加密第一时间生成第二信息，再加密所述第二信息和所述第一信息生成

第三信息发送给服务器；

[0049] S3所述服务器解密所述第三信息得到所述第一时间，通过与第二时间比对完成服务器对客户端认证；所述服务器加密所述第二时间生成第四信息发送给所述客户端；

[0050] S4所述客户端解密所述第四信息得到所述第二时间，通过与所述第一时间比对完成客户端对服务器认证。

[0051] 对实施例一进行改进，得到优选的实施例二，其中，第一时间(记为T_{ui})为客户端选取的当前时间。

[0052] 对实施例一进行改进，得到优选的实施例三，其中，第二时间(记为T_{si})为所述服务器选取的当前时间。

[0053] 对上述实施例进行改进，得到优选的实施例四，所述步骤S1具体为：

[0054] 用户输入用户标识uid和其一一对应的密码pw向服务器进行注册，每个用户具有唯一的用户标识uid和与用户标识对应的密码pw。客户端采用第一算法计算密码pw生成第一信息(记为M_1)，本发明中采用的第一算法为哈希算法，通过对密码pw进行哈希计算得到第一信息M_1为一单向安全的散列函数H(pw)，即$M_1=H(pw)$。客户端将用户标识uid和第一信息M_1发送至服务器。

[0055] 所述服务器存储用户标识uid和密码pw。服务器产生随机的第一密钥K和第二密钥K'，并将第一密钥K与加密算法E结合，生成一个与所述第一密钥k相关的加密函数E_K。服务器将第二密钥K'与解密算法D结合，生成一个与第二密钥K'相关的解密函数$D_{K'}$。服务器将加密函数E_K与解密函数$D_{K'}$发送至客户端。

[0056] 客户端存储有加密函数E_K和解密函数D_K。

[0057] 所述S2步骤具体为：

[0058] 客户端通过加密函数E_K对第一时间T_{ui}加密生成第二信息(记为M_2)，即$M_2=E_K(T_{ui})$。客户端采用第一算法计算密码pw生成第一信息(记为M_1)，本发明中采用的第一算法为哈希算法，通过对密码pw进行哈希计算得到第一信息M_1为一单向安全的散列函数H(pw)，即$M_1=H(pw)$。

[0059] 客户端采用第二算法对第二信息M_2和第一信息M_1进行计算，本发明中采用的第二算法为异或运算，即$M_1 \oplus M_2$，客户端再次使用加密函数对异或结果加密生成第三信息(记为M_3)，即$M_3=E_k(M_1 \oplus M_2)=E_k(E_K(T_{ui}) \oplus H(pw))$。

[0060] 客户端将用户标识uid和第三信息M_3发送给服务器。

[0061] 所述S3步骤具体为：

[0062] 服务器端存储有用户标识档案(记为List)，是一个存储有所有合法客户端用户标识uid的列表。

[0063] 服务器接收到客户端发送的用户标识uid，并判断服务器存储的用户标识档案List中是否存在此用户标识uid，即判断uid∈List。如果存在，则判断此用户为合法用户，用户身份的初步认证成功。通过增加初步身份认证，提高了网络身份认证的安全性。

[0064] 服务器通过加密算法E和第二密钥K'对第二时间T_{si}加密，生成第四信息(记为M_4)，即$M_4=E_{K'}(T_{si})$。

[0065] 服务器接收到客户端发送的第三信息M_3，$M_3=E_k(E_K(T_{ui}) \oplus H(pw))$。服务器通过解密算法D和第一密钥K对第三信息$M_3$进行解密，即$D_K(M_3)=D_K(E_K(E_K(T_{ui}) \oplus H(pw)))$，得到$E_K$

$(T_{ui}) \oplus H(pw)$。服务器存储有第一信息$M_1=H(pw)$，通过第二算法即异或运算对解密得到的结果和第一信息M_1进行计算，即$E_K(T_{ui}) \oplus H(pw) \oplus H(pw)$，得到第二信息$M_2$，$M_2=E_K(T_{ui})$。服务器再次通过解密算法D和第一密钥K对第二信息$M_2$进行解密，即$D_K(M_2)=D_K(E_K(T_{ui}))$，得到第一时间$T_{ui}$。

[0066] 服务器判断得到的第一时间T_{ui}和第二时间T_{si}的时间差，即$T_{si}-T_{ui}$，如果时间差小于预设值，$T_{si}-T_{ui}<10min$(本发明中选取预设值为10min，仅作为本发明的一个优选的预设值，具体预设值应视网络延时而定)，则服务器对客户端认证成功。

[0067] 服务器将第四信息$M_4=E_{K'}(T_{si})$发送给客户端。

[0068] 所述S4步骤具体为：

[0069] 客户端接收到服务器发送的第四信息M_4，通过解密函数D_K解密第四信息M_4，$D_K(M_4)=D_K(E_{K'}(T_{si}))$，得到第二时间$T_{si}$。

[0070] 客户端判断得到的第二时间T_{si}和第一时间T_{ui}的时间差，即$T_{si}-T_{ui}$，如果时间差小于预设值，$T_{si}-T_{ui}<10min$(本发明中选取预设值为10min，仅作为本发明的一个优选的预设值，具体预设值应视网络延时而定)，则客户端对服务器认证成功，继续执行以下步骤。

[0071] 对上述实施例进行改进，得到优选的实施例五，还包括步骤S5，客户端和服务器分别生成会话密钥(记为K_i)并使用会话密钥K_i加密会话数据进行数据会话，以及，对接收到的数据进行完整性校验。具体为：

[0072] 首先，客户端生成会话密钥K_i：客户端采用第三算法，本发明中采用的第三算法为取反运算。客户端对第二信息M_2进行取反运算生成第五信息M_5，$M_2=E_K(T_{ui})$，对M_2取反即得到$M_5=M_2'=E_{K'}(T_{ui})$。客户端通过加密函数E_K对第二信息M_2以及第五信息M_5加密生成会话密钥K_i，即$K_i=E_K(M_2+M_5)=E_K(E_K(T_{ui})+E_{K'}(T_{ui}))$。

[0073] 服务器生成会话密钥K_i：服务器端接收到客户端发送的第三信息M_3，$M_3=E_K(E_K(T_{ui}) \oplus H(pw))$，服务器通过解密算法D和第一密钥K解密第三信息$M_3$，即$D_K(E_K(E_K(T_{ui}) \oplus H(pw)))$，得到$E_K(T_{ui}) \oplus H(pw)$，服务器采用第二算法即异或运算对解密得到的结果和存储的第一信息M_1进行计算，即$E_K(T_{ui}) \oplus H(pw) \oplus H(pw)$，由此得到第二信息$M_2$，即$E_K(T_{ui})$。

[0074] 服务器得到第二信息M_2后采用第三算法即取法运算计算第二信息M_2。服务器对M_2进行取反运算，$M_2'=E_{K'}(T_{ui})$，生成第五信息M_5，$M_5=E_{K'}(T_{ui})$。

[0075] 服务器通过加密算法E和第一密钥K对第二信息M_2以及第五信息M_5加密生成会话密钥K_i，即$K_i=E_K(E_K(T_{ui})+E_{K'}(T_{ui}))$。

[0076] 此时，客户端和服务器端分别生成相同的会话密钥K_i，用以进行数据会话。

[0077] 客户端和服务器还存储有公用加密算法e和公用解密算法d，本发明中选用的公用加密算法e和对应的公用解密算法d为AES-128算法。

[0078] 客户端和服务器端分别通过公用加密算法e和会话密钥K_i对会话数据(记为M)加密，以及，通过公用解密算法d和会话密钥K_i对加密后的会话数据M解密。

[0079] 会话数据M加密具体为：客户端/服务器发送的会话数据M，首先客户端/服务器使用会话密钥K_i和公用加密算法e加密会话数据M，生成第一数据，即$e_{Ki}(M)$。客户端/服务器采用第一算法(即哈希算法)对会话数据M进行计算生成第二数据，即第二数据为H(M)。客户端/服务器向服务器/客户端发送第一数据和第二数据，即$e_{Ki}(M)+H(M)$。

[0080] 会话数据M解密具体为：服务器/客户端接收第一数据和第二数据，即$e_{Ki}(M)+H(M)$。

服务器/客户端通过公用解密算法d和会话密钥K_i解密第一数据$e_{Ki}(M)$，即$d_{Ki}(e_{Ki}(M))$，得到一会话数据S(与客户端/服务器发送的原始会话数据M进行区分)。

[0081] 会话数据M完整性校验:服务器/客户端再通过第一算法(即哈希算法)对解密得到的会话数据S进行计算，即H(S)。服务器/客户端将H(S)与接收到的第二数据H(M)进行比对，如果H(S)＝H(M)相同，则表示服务器/客户端接收到的会话数据S就是客户端/服务器发送的会话数据M,会话数据具有完整性，否则会话数据S不完整，为不合法。

[0082] 本发明中步骤S5中的数据会话过程为客户端向服务器端发送加密的会话数据，服务器端接收会话数据并解密，最后进行会话数据完整性校验。本发明提供的数据处理方法在数据进行会话时，数据加密、解密以及数据校验过程是客户端和服务器端双向的，相反过程为，服务器端对会话数据M加密发送给客户端，客户端接收会话数据并解密，最后进行会话数据完整性校验。

[0083] 本发明能够实现网络身份认证、数据加密传输以及数据完整性校验，防止中间人攻击，安全系数高，防止交易内容的泄露与篡改，防抵赖，具有更优的技术效果。

[0084] 对上述实施例进行改进，得到优选的实施例六，其中客户端和服务器生成相同的第一信息M_1。客户端采用哈希算法对用户输入的用户标识uid和密码pw进行计算得到的，M_1＝H(pw)。服务器采用第一算法即哈希算法对接收到的用户标识uid以及其存储的与用户标识uid唯一对应的密码pw进行计算，生成与客户端相同的第一信息M_1并存储。服务器在进行第二算法即异或运算时将其存储的第一信息M_1与解密后的第三信息M_3进行计算，得到第二信息M_2。

[0085] 对上述实施例进行改进，得到优选的实施例七，其中，客户端和所述服务器生成的所述会话密钥K_i是相同的，减少密钥传输，使得密钥保存更安全。

[0086] 对上述实施例进行改进，得到优选的实施例八，其中，所述用户标识uid包括用于唯一标识用户的信息。

[0087] 对上述实施例进行改进，得到优选的实施例九，所述用户标识档案List为存储所有合法用户的用户标识uid的列表，在服务器接收到客户端发送的用户标识uid时，服务器根据存储的用户标识档案List判断用户标识uid是否存在用户标识档案List中，如果存在，说明此用户是合法的。

[0088] 以上对本发明的具体实施例进行了详细描述，但本发明并不限制于以上描述的具体实施例，其只是作为范例。对于本领域技术人员而言，任何对本发明进行的等同修改和替代也都在本发明的范畴之中。因此，在不脱离发明的精神和范围下所做出的均等变换和修改，都应涵盖在本发明的范围内。

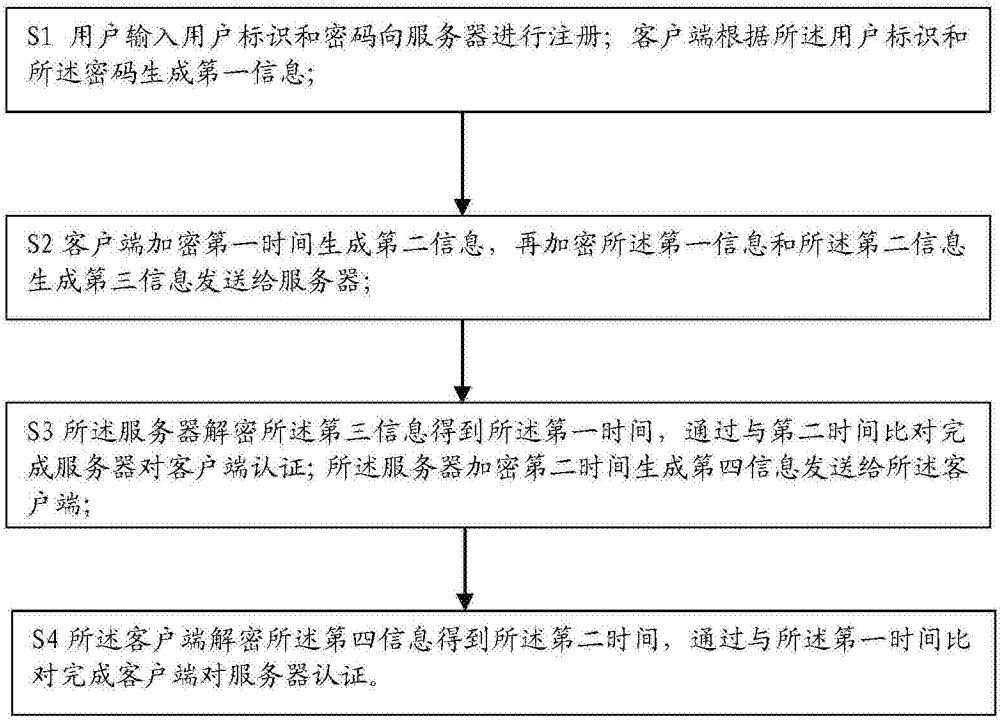

S1 用户输入用户标识和密码向服务器进行注册；客户端根据所述用户标识和所述密码生成第一信息；
S2 客户端加密第一时间生成第二信息，再加密所述第一信息和所述第二信息生成第三信息发送给服务器；
S3 所述服务器解密所述第三信息得到所述第一时间，通过与第二时间比对完成服务器对客户端认证；所述服务器加密第二时间生成第四信息发送给所述客户端；
S4 所述客户端解密所述第四信息得到所述第二时间，通过与所述第一时间比对完成客户端对服务器认证。

图1