(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 112671762 A
(43)申请公布日 2021.04.16

(21)申请号 202011538252.1

(22)申请日 2020.12.23

(71)申请人 福建正孚软件有限公司
地址 350001 福建省福州市鼓楼区软件大道89号福州软件园C区38号楼三楼

(72)发明人 倪时龙 李桥木 曾伟波 谢海强 吴烜

(74)专利代理机构 福州市景弘专利代理事务所(普通合伙) 35219
代理人 魏小霞 林祥翔

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
G06F 21/46(2013.01)

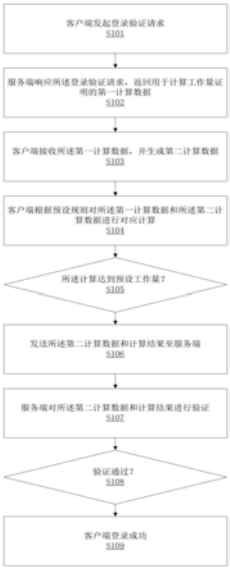
权利要求书1页 说明书5页 附图2页

(54)发明名称

一种基于工作量证明实现防暴力破解的登录认证方法和系统

(57)摘要

本发明涉及加解密技术领域,特别涉及一种基于工作量证明实现防暴力破解的登录认证方法和系统。所述一种基于工作量证明实现防暴力破解的登录认证方法,包括步骤:客户端发起登录验证请求;服务端响应所述登录验证请求,返回用于计算工作量证明的第一计算数据;客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算,当所述计算达到预设工作量后,发送所述第二计算数据和计算结果至服务端;服务端对所述第二计算数据和计算结果进行验证。客户端需要做一定难度的工作来得出一个结果,可大大降低攻击者使用暴力破解的速度,同时既不需要人工进行验证码输入操作,也不会因为误操作就被限制登录,大大提升了用户体验。



CN 112671762 A

1.一种基于工作量证明实现防暴力破解的登录认证方法,其特征在于,包括步骤:

客户端发起登录验证请求;

服务端响应所述登录验证请求,返回用于计算工作量证明的第一计算数据;

客户端接收所述第一计算数据,并生成第二计算数据;

客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算,当所述计算达到预设工作量后,发送所述第二计算数据和计算结果至服务端;

服务端对所述第二计算数据和计算结果进行验证,若验证通过,则客户端登录成功。

2.根据权利要求1所述的一种基于工作量证明实现防暴力破解的登录认证方法,其特征在于,

所述第一计算数据和所述第二计算数据为随机字符串;

所述“客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算”,具体还包括步骤:

客户端对所述第一计算数据和所述第二计算数据进行哈希运算,哈希运算完后,修改或增加随机数继续进行哈希运算直至达到预设工作量。

3.根据权利要求1所述的一种基于工作量证明实现防暴力破解的登录认证方法,其特征在于,所述“服务端对所述第二计算数据和计算结果进行验证,若验证通过,则客户端登录成功”,具体还包括步骤:

服务端根据第一计算数据和第二计算数据进行哈希运算直至到达预设工作量得验证结果,将所述验证结果与客户端发送的计算结果进行比对,若二者相同,则验证通过,客户端登录成功。

4.一种基于工作量证明实现防暴力破解的登录认证系统,其特征在于,包括:客户端和服务端;

客户端向服务端发起登录验证请求;

服务端响应所述登录验证请求,返回用于计算工作量证明的第一计算数据;

客户端接收所述第一计算数据,并生成第二计算数据;

客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算,当所述计算达到预设工作量后,发送所述第二计算数据和计算结果至服务端;

服务端对所述第二计算数据和计算结果进行验证,若验证通过,则客户端登录成功。

5.根据权利要求4所述的一种基于工作量证明实现防暴力破解的登录认证系统,其特征在于,

所述第一计算数据和所述第二计算数据为随机字符串;

所述客户端还用于:对所述第一计算数据和所述第二计算数据进行哈希运算,哈希运算完后,修改或增加随机数继续进行哈希运算直至达到预设工作量。

6.根据权利要求4所述的一种基于工作量证明实现防暴力破解的登录认证系统,其特征在于,

所述服务端还用于:根据第一计算数据和第二计算数据进行哈希运算直至到达预设工作量得验证结果,将所述验证结果与客户端发送的计算结果进行比对,若二者相同,则验证通过,客户端登录成功。

一种基于工作量证明实现防暴力破解的登录认证方法和系统

技术领域

[0001] 本发明涉及加解密技术领域,特别涉及一种基于工作量证明实现防暴力破解的登录认证方法和系统。

背景技术

[0002] 随着互联网和5G的普及,人们越来越多在不同的网站上注册自己的账户,填写个人隐私,随之而来的是更多的网络安全问题。黑客等其他攻击人员经常会利用不同的技术手段非法获取个人账户资料。最常用的方式包括了暴力破解,暴力破解攻击是指攻击者通过系统地组合所有可能性(例如登录时用到的账户名、密码),尝试所有的可能性破解用户的账户名、密码等敏感信息。攻击者会经常使用自动化脚本组合出正确的用户名和密码。目前的防御暴力破解攻击,包括以下几种:验证码:通过短信、图形码进行验证。IP提交次数限制:限制同一IP或对同一帐号提交验证的错误次数。

[0003] 验证码防止暴力破解,设计出发点是易于被人类解决而不易被计算机解决,需要用户进行人为输入验证码,不太人性化。IP提交次数限制,则因为用户存在多个密码,正常输入错误后,被限制登录,导致不必要的解锁和运维问题。

发明内容

[0004] 为此,需要提供一种基于工作量证明实现防暴力破解的登录认证方法,用以解决现有防暴力破解方式操作复杂、人性化差的技术问题。具体技术方案如下:

[0005] 一种基于工作量证明实现防暴力破解的登录认证方法,包括步骤:

[0006] 客户端发起登录验证请求;

[0007] 服务端响应所述登录验证请求,返回用于计算工作量证明的第一计算数据;

[0008] 客户端接收所述第一计算数据,并生成第二计算数据;

[0009] 客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算,当所述计算达到预设工作量后,发送所述第二计算数据和计算结果至服务端;

[0010] 服务端对所述第二计算数据和计算结果进行验证,若验证通过,则客户端登录成功。

[0011] 进一步的,所述第一计算数据和所述第二计算数据为随机字符串;

[0012] 所述“客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算”,具体还包括步骤:

[0013] 客户端对所述第一计算数据和所述第二计算数据进行哈希运算,哈希运算完后,修改或增加随机数继续进行哈希运算直至达到预设工作量。

[0014] 进一步的,所述“服务端对所述第二计算数据和计算结果进行验证,若验证通过,则客户端登录成功”,具体还包括步骤:

[0015] 服务端根据第一计算数据和第二计算数据进行哈希运算直至到达预设工作量得验证结果,将所述验证结果与客户端发送的计算结果进行比对,若二者相同,则验证通过,

客户端登录成功。

[0016] 为解决上述技术问题，还提供了一种基于工作量证明实现防暴力破解的登录认证系统，具体技术方案如下：

[0017] 一种基于工作量证明实现防暴力破解的登录认证系统，包括：客户端和服务端；

[0018] 客户端向服务端发起登录验证请求；

[0019] 服务端响应所述登录验证请求，返回用于计算工作量证明的第一计算数据；

[0020] 客户端接收所述第一计算数据，并生成第二计算数据；

[0021] 客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算，当所述计算达到预设工作量后，发送所述第二计算数据和计算结果至服务端；

[0022] 服务端对所述第二计算数据和计算结果进行验证，若验证通过，则客户端登录成功。

[0023] 进一步的，所述第一计算数据和所述第二计算数据为随机字符串；

[0024] 所述客户端还用于：对所述第一计算数据和所述第二计算数据进行哈希运算，哈希运算完后，修改或增加随机数继续进行哈希运算直至达到预设工作量。

[0025] 进一步的，所述服务端还用于：根据第一计算数据和第二计算数据进行哈希运算直至到达预设工作量得验证结果，将所述验证结果与客户端发送的计算结果进行比对，若二者相同，则验证通过，客户端登录成功。

[0026] 本发明的有益效果是：通过客户端发起登录验证请求；服务端响应所述登录验证请求，返回用于计算工作量证明的第一计算数据；客户端接收所述第一计算数据，并生成第二计算数据；客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算，当所述计算达到预设工作量后，发送所述第二计算数据和计算结果至服务端；服务端对所述第二计算数据和计算结果进行验证，若验证通过，则客户端登录成功。客户端需要做一定难度的工作来得出一个结果，可大大降低攻击者使用暴力破解的速度，同时既不需要人工进行验证码输入操作，也不会因为误操作就被限制登录，大大提升了用户体验。

附图说明

[0027] 图1为具体实施方式所述一种基于工作量证明实现防暴力破解的登录认证方法的流程图；

[0028] 图2为具体实施方式所述一种基于工作量证明实现防暴力破解的登录认证系统的模块示意图。

[0029] 附图标记说明：

[0030] 200、一种基于工作量证明实现防暴力破解的登录认证系统，

[0031] 201、客户端，

[0032] 202、服务端。

具体实施方式

[0033] 为详细说明技术方案的技术内容、构造特征、所实现目的及效果，以下结合具体实施例并配合附图详予说明。

[0034] 本申请的核心技术思想是：通过工作量证明算法来防止暴力破解的登录验证，工

作量证明算法，是一种应对拒绝服务攻击和其他服务滥用的经济对策。主要特征是客户端需要做一定难度的工作得出一个结果，验证方却很容易通过结果来检查出客户端是不是做了相应的工作。要求发起者进行一定量的运算，也就意味着需要消耗计算机一定的时间，这种方案的一个核心特征是不对称性：工作对于请求方是适中的，对于验证方则是易于验证的。

[0035] 暴力破解的本质就是通过枚举法不断的尝试验证口令的正确性，直到尝试到正确的口令。过程中需要尝试的无数次。每次尝试的时间越短，攻击者的破解的速度就越快，难度和概率就越高。使用工作量证明可以加长每次验证口令的时间。从而降低攻击者使用暴力破解的速度。

[0036] 请参阅图1，在本实施方式中，一种基于工作量证明实现防暴力破解的登录认证方法具体实施方式如下：

[0037] 步骤S101：客户端发起登录验证请求。

[0038] 步骤S102：服务端响应所述登录验证请求，返回用于计算工作量证明的第一计算数据。

[0039] 步骤S103：客户端接收所述第一计算数据，并生成第二计算数据。

[0040] 步骤S104：客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算。

[0041] 步骤S105：所述计算达到预设工作量？

[0042] 步骤S106：发送所述第二计算数据和计算结果至服务端。

[0043] 步骤S107：服务端对所述第二计算数据和计算结果进行验证。

[0044] 步骤S108：验证通过？

[0045] 步骤S109：客户端登录成功。

[0046] 在本实施方式中，优选地，所述第一计算数据和所述第二计算数据为随机字符串；

[0047] 所述“客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算”，具体还包括步骤：

[0048] 客户端对所述第一计算数据和所述第二计算数据进行哈希运算，哈希运算完后，修改或增加随机数继续进行哈希运算直至达到预设工作量。

[0049] 其中预设工作量的判断条件可为：根据预设的规则进行判断。比如要求计算的结果头几位必须为(0000)，客户端判断出达到计算要求后停止计算。提交至服务端，服务端也可以很快的根据客户端提交的随机字符串和计算结果进行校验。

[0050] 具体可为：所述“服务端对所述第二计算数据和计算结果进行验证，若验证通过，则客户端登录成功”，具体还包括步骤：

[0051] 服务端根据第一计算数据和第二计算数据进行哈希运算直至到达预设工作量得验证结果，将所述验证结果与客户端发送的计算结果进行比对，若二者相同，则验证通过，客户端登录成功。

[0052] 通过客户端发起登录验证请求；服务端响应所述登录验证请求，返回用于计算工作量证明的第一计算数据；客户端接收所述第一计算数据，并生成第二计算数据；客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算，当所述计算达到预设工作量后，发送所述第二计算数据和计算结果至服务端；服务端对所述第二计算数据和计

算结果进行验证，若验证通过，则客户端登录成功。客户端需要做一定难度的工作来得出一个结果，可大大降低攻击者使用暴力破解的速度，同时既不需要人工进行验证码输入操作，也不会因为误操作就被限制登录，大大提升了用户体验。

[0053] 在本实施方式中，哈希算法是一类算法的总称。常见的加密算法可分为对称加密、非对称加密、及哈希算法。哈希算法中包含了MD5,SHA-1,SHA-2,SHA-256,SHA-512,RIPEMD-160等。

[0054] 请参阅图2，在本实施方式中，一种基于工作量证明实现防暴力破解的登录认证系统200的具体实施方式如下：

[0055] 一种基于工作量证明实现防暴力破解的登录认证系统200，包括：客户端201和服务端202；

[0056] 客户端201向服务端202发起登录验证请求；

[0057] 服务端202响应所述登录验证请求，返回用于计算工作量证明的第一计算数据；

[0058] 客户端201接收所述第一计算数据，并生成第二计算数据；

[0059] 客户端201根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算，当所述计算达到预设工作量后，发送所述第二计算数据和计算结果至服务端202；

[0060] 服务端202对所述第二计算数据和计算结果进行验证，若验证通过，则客户端201登录成功。

[0061] 进一步的，所述第一计算数据和所述第二计算数据为随机字符串；

[0062] 所述客户端201还用于：对所述第一计算数据和所述第二计算数据进行哈希运算，哈希运算完后，修改或增加随机数继续进行哈希运算直至达到预设工作量。

[0063] 其中预设工作量的判断条件可为：根据预设的规则进行判断。比如要求计算的结果头几位必须为(0000)，客户端201判断出达到计算要求后停止计算。提交至服务端202，服务端202也可以很快的根据客户端201提交的随机字符串和计算结果进行校验。

[0064] 进一步的，所述服务端202还用于：根据第一计算数据和第二计算数据进行哈希运算直至到达预设工作量得验证结果，将所述验证结果与客户端201发送的计算结果进行比对，若二者相同，则验证通过，客户端201登录成功。

[0065] 通过客户端201发起登录验证请求；服务端202响应所述登录验证请求，返回用于计算工作量证明的第一计算数据；客户端201接收所述第一计算数据，并生成第二计算数据；客户端201根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算，当所述计算达到预设工作量后，发送所述第二计算数据和计算结果至服务端202；服务端202对所述第二计算数据和计算结果进行验证，若验证通过，则客户端201登录成功。客户端201需要做一定难度的工作来得出一个结果，可大大降低攻击者使用暴力破解的速度，同时既不需要人工进行验证码输入操作，也不会因为误操作就被限制登录，大大提升了用户体验。

[0066] 在本实施方式中，哈希算法是一类算法的总称。常见的加密算法可分为对称加密、非对称加密、及哈希算法。哈希算法中包含了MD5,SHA-1,SHA-2,SHA-256,SHA-512,RIPEMD-160等。

[0067] 需要说明的是，尽管在本文中已经对上述各实施例进行了描述，但并非因此限制本发明的专利保护范围。因此，基于本发明的创新理念，对本文所述实施例进行的变更和修改，或利用本发明说明书及附图内容所作的等效结构或等效流程变换，直接或间接地将以

上技术方案运用在其他相关的技术领域,均包括在本发明的专利保护范围之内。

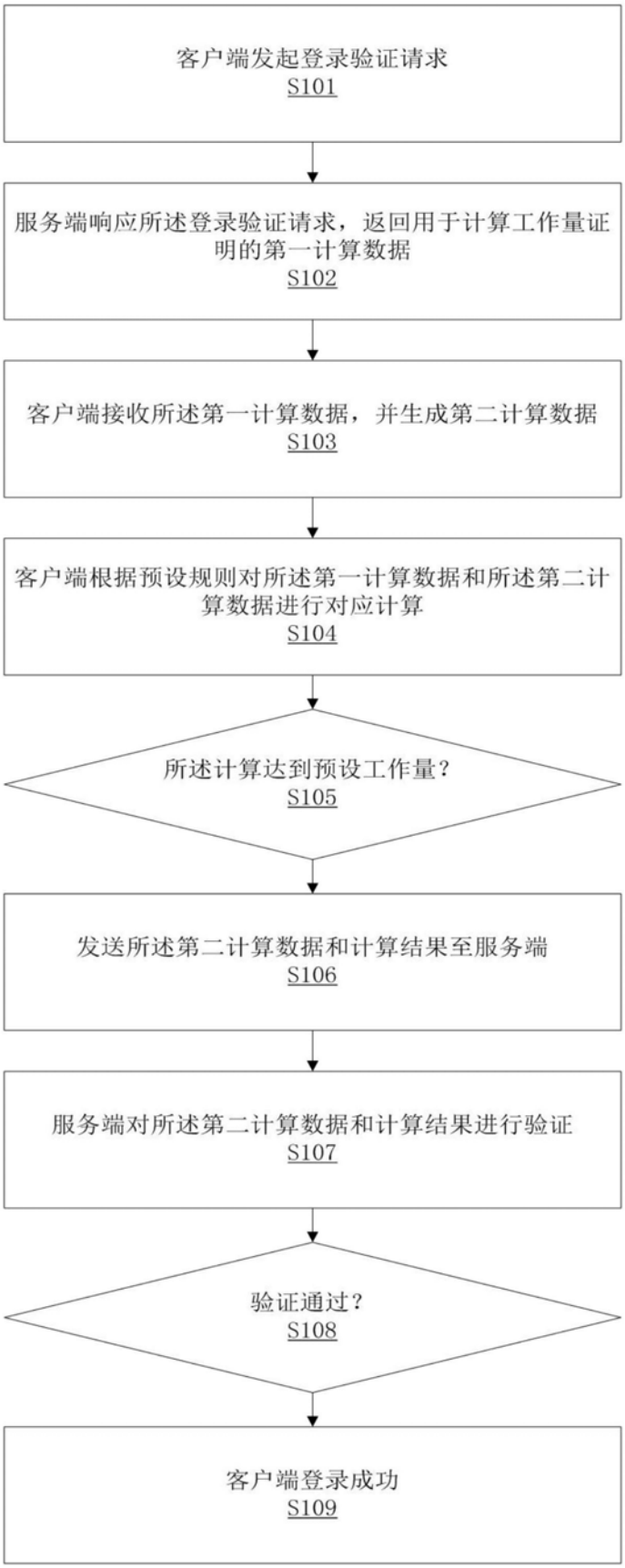

客户端发起登录验证请求
S101
服务端响应所述登录验证请求，返回用于计算工作量证明的第一计算数据
S102
客户端接收所述第一计算数据，并生成第二计算数据
S103
客户端根据预设规则对所述第一计算数据和所述第二计算数据进行对应计算
S104
所述计算达到预设工作量？
S105
发送所述第二计算数据和计算结果至服务端
S106
服务端对所述第二计算数据和计算结果进行验证
S107
验证通过？
S108
客户端登录成功
S109

图1

图2