(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 104426849 A
(43)申请公布日 2015.03.18

(21)申请号 201310370477.4

(22)申请日 2013.08.22

(71)申请人 深圳中兴网信科技有限公司
地址 518000 广东省深圳市南山区高新区南区科技南路中兴通讯一期A座

(72)发明人 张亮

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 张振伟 王黎延

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

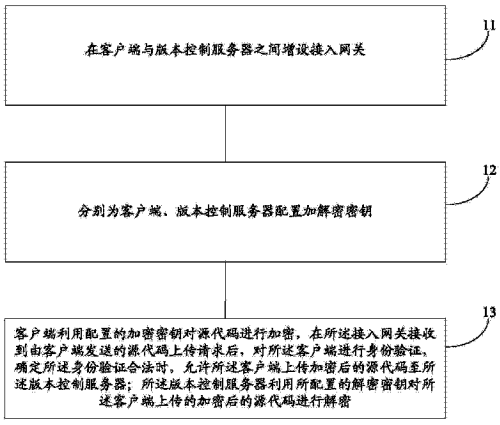
权利要求书1页 说明书6页 附图2页

(54)发明名称

一种实现数据安全保护的方法及系统

(57)摘要

本发明公开了一种实现数据安全保护的方法，所述方法包括：在客户端与版本控制服务器之间增设接入网关，所述方法还包括：所述客户端利用配置的加密密钥对源代码进行加密，所述接入网关接收到由所述客户端发送的源代码上传请求后，对所述客户端进行身份验证，确定所述身份验证合法时，允许所述客户端上传加密后的源代码至所述版本控制服务器；所述版本控制服务器利用配置的解密密钥对所述客户端上传的加密后的源代码进行解密。同时，本发明还公开了一种实现数据安全保护的系统。利用本发明的技术方案，提高了数据传输的安全性，保证了数据应用的可靠性。



CN 104426849 A

1. 一种实现数据安全保护的方法，其特征在于，在客户端与版本控制服务器之间增设接入网关，所述方法还包括：

所述客户端利用配置的加密密钥对源代码进行加密，所述接入网关接收到由所述客户端发送的源代码上传请求后，对所述客户端进行身份验证，确定所述身份验证合法时，允许所述客户端上传加密后的源代码至所述版本控制服务器；所述版本控制服务器利用配置的解密密钥对所述客户端上传的加密后的源代码进行解密。

2. 根据权利要求 1 所述的实现数据安全保护的方法，其特征在于，所述方法还包括：

在所述接入网关接收到由客户端发送的源代码下载请求后，对所述客户端进行身份验证，确定所述身份验证合法时，通知所述版本控制服务器将源代码传送至所述客户端。

3. 根据权利要求 2 所述的实现数据安全保护的方法，其特征在于，在所述接入网关通知所述版本控制服务器将源代码传送至所述客户端之后，所述方法还包括：

所述版本控制服务器利用配置的加密密钥对待传送的源代码进行加密后传送至所述客户端，所述客户端利用配置的解密密钥对所接收到的源代码进行解密。

4. 根据权利要求 1 至 3 任一项所述的实现数据安全保护的方法，其特征在于，所述方法还包括：

所述接入网关确定所述客户端当前身份验证的次数超出预设的最大次数时，禁止所述客户端上传加密后的源代码至所述版本控制服务器，或禁止所述版本控制服务器传送源代码至所述客户端。

5. 一种实现数据安全保护的系统，其特征在于，所述系统包括：客户端、接入网关及版本控制服务器；其中，

所述客户端，用于利用配置的加密密钥对源代码进行加密，并发送源代码上传请求至所述接入网关；

所述接入网关，用于对所述客户端进行身份验证，并在确定所述身份验证合法时，允许所述客户端上传加密后的源代码至所述版本控制服务器；

所述版本控制服务器，用于利用配置的解密密钥对所述加密后的源代码进行解密。

6. 根据权利要求 5 所述的实现数据安全保护的系统，其特征在于，所述客户端，还用于发送源代码下载请求至所述接入网关；

利用配置的解密密钥对接收到的源代码进行解密；

相应的，所述接入网关，还用于对发送所述源代码下载请求的客户端进行身份验证，确定所述身份验证合法时，通知所述版本控制服务器将源代码传送至所述客户端；

所述版本控制服务器，还用于利用配置的加密密钥对待传送的源代码进行加密后，传送至所述客户端。

7. 根据权利要求 6 所述的实现数据安全保护的系统，其特征在于，所述客户端，还用于对解密后的源代码进行显示。

8. 根据权利要求 5 至 7 任一项所述的实现数据安全保护的系统，其特征在于，所述接入网关，还用于确定所述客户端当前身份验证的次数超出预设的最大次数时，禁止所述客户端上传加密后的源代码至所述版本控制服务器，或禁止所述版本控制服务器传送源代码至所述客户端。

一种实现数据安全保护的方法及系统

技术领域

[0001] 本发明涉及数据安全技术，具体涉及一种实现数据安全保护的方法及系统。

背景技术

[0002] 在具有自主研发能力的企业中，一个工程项目的开发往往需要多个研发人员。每个研发人员将自身负责的部分实现后，需将所实现的项目源代码上传到版本控制服务器中。由版本控制服务器将所述多个研发人员各自完成的项目源代码进行融合，生成能够适应项目需求的应用程序。

[0003] 但是，项目源代码由客户端传送至版本控制服务器的过程中，或是下载版本控制服务器中的源代码到客户端供研发人员使用时，均采用明文形式，并没有对源代码数据采用安全保护措施，如此便存在以下两方面风险：

[0004] 1、具有版本控制服务器访问权限的企业内部员工可轻易将版本控制服务器的应用程序文件全盘拷贝，并泄漏给竞争对手；

[0005] 2、黑客很容易入侵该版本控制服务器，窃取版本控制服务器上的所有应用程序文件。

发明内容

[0006] 有鉴于此，本发明实施例的主要目的在于提供一种实现数据安全保护的方法及系统，可提高数据传输的安全性、保证数据应用的可靠性。

[0007] 为达到上述目的，本发明实施例的技术方案是这样实现的：

[0008] 本发明实施例提供了一种实现数据安全保护的方法，在客户端与版本控制服务器之间增设接入网关，所述方法还包括：

[0009] 所述客户端利用配置的加密密钥对源代码进行加密，所述接入网关接收到由所述客户端发送的源代码上传请求后，对所述客户端进行身份验证，确定所述身份验证合法时，允许所述客户端上传加密后的源代码至所述版本控制服务器；所述版本控制服务器利用配置的解密密钥对所述客户端上传的加密后的源代码进行解密。

[0010] 上述方案中，所述方法还包括：

[0011] 在所述接入网关接收到由客户端发送的源代码下载请求后，对所述客户端进行身份验证，确定所述身份验证合法时，通知所述版本控制服务器将源代码传送至所述客户端。

[0012] 上述方案中，在所述接入网关通知所述版本控制服务器将源代码传送至所述客户端之后，所述方法还包括：

[0013] 所述版本控制服务器利用配置的加密密钥对待传送的源代码进行加密后传送至所述客户端，所述客户端利用配置的解密密钥对所接收到的源代码进行解密。

[0014] 上述方案中，所述方法还包括：

[0015] 所述接入网关确定所述客户端当前身份验证的次数超出预设的最大次数时，禁止所述客户端上传加密后的源代码至所述版本控制服务器，或禁止所述版本控制服务器传送

源代码至所述客户端。

[0016] 本发明实施例还提供了一种实现数据安全保护的系统，所述系统包括：客户端、接入网关及版本控制服务器；其中，

[0017] 所述客户端，用于利用配置的加密密钥对源代码进行加密，并发送源代码上传请求至所述接入网关；

[0018] 所述接入网关，用于对所述客户端进行身份验证，并在确定所述身份验证合法时，允许所述客户端上传加密后的源代码至所述版本控制服务器；

[0019] 所述版本控制服务器，用于利用配置的解密密钥对所述加密后的源代码进行解密。

[0020] 上述方案中，所述客户端，还用于发送源代码下载请求至所述接入网关；

[0021] 利用配置的解密密钥对接收到的源代码进行解密；

[0022] 相应的，所述接入网关，还用于对发送所述源代码下载请求的客户端进行身份验证，确定所述身份验证合法时，通知所述版本控制服务器将源代码传送至所述客户端；

[0023] 所述版本控制服务器，还用于利用配置的加密密钥对待传送的源代码进行加密后，传送至所述客户端。

[0024] 上述方案中，所述客户端，还用于对解密后的源代码进行显示。

[0025] 上述方案中，所述接入网关，还用于确定所述客户端当前身份验证的次数超出预设的最大次数时，禁止所述客户端上传加密后的源代码至所述版本控制服务器，或禁止所述版本控制服务器传送源代码至所述客户端。

[0026] 本发明实施例提供的实现数据安全保护的方法及系统，分别为客户端及版本控制服务器配置加解密密钥；并在客户端与版本控制服务器之间增设接入网关；客户端利用配置的加密密钥对源代码进行加密，在所述接入网关接收到由客户端发送的源代码上传请求后，对所述客户端进行身份验证，确定所述身份验证合法时，允许所述客户端上传加密后的源代码至所述版本控制服务器；所述版本控制服务器利用所配置的解密密钥对加密后的源代码进行解密。本发明的技术方案，将源代码进行了加密处理后上传至版本控制服务器，同时增设了接入网关，只有在接入网关确定发起源代码上传 / 下载请求客户端的身份验证为合法时，才允许客户端上传源代码、或允许客户端下载版本控制服务器中保存的源代码到客户端。由此可见，利用本发明的技术方案，提高了数据传输的安全性、保证了数据应用的可靠性。

附图说明

[0027] 图 1 为本发明实施例的实现数据安全保护的方法的流程示意图；

[0028] 图 2 为本发明实施例的实现数据安全保护的系统的组成结构示意图。

具体实施方式

[0029] 本发明实施例记载了一种实现数据安全保护的方法，如图 1 所示，所述方法包括：

[0030] 步骤 11：在客户端与版本控制服务器之间增设接入网关。

[0031] 步骤 12：分别为客户端、版本控制服务器配置加解密密钥。

[0032] 本发明实施例中，对源代码进行加解密的算法包括以下至少一种：高级加密标准

(AES,Advanced Encryption Standard)、或公钥加密 RSA 算法、或 AES 与 RSA 组合算法等。

[0033] 在源代码由所述客户端上传到所述版本控制服务器时,所述客户端使用所配置的加密密钥对所述源代码进行加密;相应的,所述版本控制服务器利用所述解密密钥,对接收到的加密后的源代码进行解密。

[0034] 在所述版本控制服务器传送源代码至所述客户端时,所述版本控制服务器利用所配置的加密密钥先对源代码进行加密,然后再将加密后的源代码传送至所述客户端;相应的,所述客户端利用所述解密密钥对接收到的源代码进行解密并显示。

[0035] 这里,步骤 11 与步骤 12 无严格的先后顺序,还可以并行进行。

[0036] 步骤 13:客户端利用配置的加密密钥对源代码进行加密,在所述接入网关接收到由客户端发送的源代码上传请求后,对所述客户端进行身份验证,确定所述身份验证合法时,允许所述客户端上传加密后的源代码至所述版本控制服务器;所述版本控制服务器利用所配置的解密密钥对所述客户端上传的加密后的源代码进行解密。

[0037] 相应的,在所述接入网关接收到由客户端发送的源代码下载请求后,对所述客户端进行身份验证,确定所述身份验证合法时,通知所述版本控制服务器将源代码传送至所述客户端;所述版本控制服务器利用所配置的加密密钥对自身保存的源代码进行加密,并传送至所述客户端;所述客户端利用所配置的解密密钥对所接收到的源代码进行相应的解密,并显示解密后的源代码。其中,所述版本控制服务器可以以应用程序文件的形式保存各客户端上传的源代码。

[0038] 在上述客户端请求上传加密后的源代码到版本服务器过程中、或客户端请求下载版本控制服务器的源代码到客户端的过程中,接入网关可以设置身份验证的最高次数,当所述接入网关确定所述客户端当前身份验证的次数超出预设的最大次数时,禁止所述客户端上传加密后的源代码至所述版本控制服务器,或禁止所述版本控制服务器传送源代码至所述客户端。

[0039] 所述身份验证方式包括以下至少一种:用户名与密码组合方式,用户名、密码与验证码三者组合的方式,客户端个人证书,动态口令牌,短信口令、硬件数字证书载体(USB Key,Universal Serial Bus Key)等。

[0040] 下面以身份验证方式为用户名与密码的组合方式为例,并结合实施例一、实施例二对本发明实施例的技术方案作进一步说明。

[0041] 实施例一

[0042] 当前客户端利用配置的加密密钥 A 对源代码进行加密,并发送源代码上传请求至所述接入网关,所述接入网关接收到所述源代码上传请求,对所述当前客户端进行身份验证,当确定所述当前客户端输入的用户名与密码均正确时,返回所述源代码上传请求的允许应答消息至所述当前客户端,所述当前客户端接收到所述允许上传的应答消息后,上传加密后的源代码至所述版本控制服务器,所述版本控制服务器利用配置的解密密钥 A'对加密后的源代码进行解密,并保存。

[0043] 这里,还可以在接入网关中设置在指定周期内允许当前客户端输入用户名与密码的最大次数,如指定周期为一天、允许输入的最大次数为 3 次。

[0044] 当接入网关确定所述当前客户端第一次和/或第二次输入的用户名与密码不正确时,返回所述源代码上传请求的重试应答消息至所述当前客户端,所述当前客户端重新

输入用户名与密码。当所述接入网关确定所述当前客户端当前输入次数小于等于 3 次且当前输入次数下输入的用户名与密码均正确后，返回所述源代码上传请求的允许应答消息至所述当前客户端；所述当前客户端接收到所述允许上传的应答消息后，上传加密后的源代码至所述版本控制服务器，所述版本控制服务器利用配置的解密密钥 A’对加密后的源代码进行解密，并保存。

[0045] 接入网关确定在该天内当前客户端的当前输入次数超出 3 次时，所述接入网关返回禁止上传的应答消息至当前客户端，在该天内当前客户端不可再进行用户名与密码的输入，该天内当前客户端无法将加密后的源代码文件上传至所述版本控制服务器。

[0046] 在实施例一中，配置当前客户端的加密密钥为 A，相应的，配置版本控制服务器的解密密钥 A’。

[0047] 实施例二

[0048] 当前客户端想要下载版本控制服务器中保存的源代码（应用程序文件）时，当前客户端发送源代码下载请求至所述接入网关，所述接入网关接收到所述源代码下载请求后，对所述当前客户端进行身份验证，当确定所述当前客户端输入的用户名与密码均正确时，返回所述源代码下载请求的允许应答消息至所述当前客户端，并通知所述版本控制服务器将所述版本控制服务器保存的源代码传送至当前客户端。所述版本控制服务器利用配置的加密密钥 A 对源代码进行加密后，传送至所述当前客户端，当前客户端利用配置的解密密钥 A’对加密后的源代码进行解密，并显示解密后的所述源代码。

[0049] 这里，还可以在所述接入网关中设置在指定周期内允许客户端输入用户名与密码的最大次数，如指定周期为一天、所述最大次数为 3 次。

[0050] 当接入网关确定当前客户端第一次和 / 或第二次输入的用户名与密码不正确时，返回所述源代码下载请求的重试应答消息至所述当前客户端，所述当前客户端重新输入用户名与密码，当所述接入网关确定所述当前客户端当前输入次数小于等于 3 次且当前输入次数下输入的用户名与密码均正确后，返回所述源代码下载请求的允许应答消息至所述当前客户端，并通知所述版本控制服务器传送源代码至所述当前客户端。所述版本控制服务器利用配置的加密密钥 A 对源代码进行加密后，传送至所述当前客户端，当前客户端利用配置的解密密钥 A’对加密后的源代码进行解密，并显示解密后的所述源代码。

[0051] 接入网关确定在该天内当前客户端当前的输入次数超出最大次数 3 次时，所述接入网关返回所述源代码下载请求的禁止下载应答消息至所述当前客户端，在该天内所述当前客户端不可再进行用户名与密码的输入，进而在该天内所述当前客户端无法下载所述版本控制服务器中保存的源代码。

[0052] 在实施例二中，配置版本控制服务器的加密密钥为 A，相应的，配置当前客户端的解密密钥 A’。

[0053] 基于上述实现数据安全保护的方法，本发明实施例还记载了一种实现数据安全保护的系统，如图 2 所示，所述系统包括：客户端 21、接入网关 22 及版本控制服务器 23；其中，

[0054] 所述客户端 21，用于利用配置的加密密钥对源代码进行加密，并发送源代码上传请求至所述接入网关 22；

[0055] 所述接入网关 22，用于对发送源代码上传请求的所述客户端 21 进行身份验证，并在确定所述身份验证合法时，允许所述客户端 21 上传加密后的源代码至所述版本控制服

务器 23；

[0056] 所述版本控制服务器 23，用于接收所述客户端 21 上传的加密后的源代码，并利用配置的解密密钥对所述加密后的源代码进行解密；

[0057] 所述客户端 21，还用于发送源代码下载请求至所述接入网关 22，利用配置的解密密钥对接收到的源代码进行解密，并显示解密后的源代码；

[0058] 相应的，所述接入网关 22，用于对发送源代码下载请求的所述客户端 21 进行身份验证，并在确定所述身份验证合法时，通知所述版本控制服务器 23 传送源代码至所述客户端 21；

[0059] 所述版本控制服务器 23，还用于利用配置的加密密钥对源代码进行加密后，传送加密后的源代码至所述客户端 21。

[0060] 其中，所述版本控制服务器 23 可以以应用程序文件形式保存各客户端上传的源代码。

[0061] 本发明实施例中，所提及的加解密算法与身份验证方式请参见前述方法的描述，这里不再赘述。

[0062] 下面以身份验证方式为用户名与密码的组合方式为例，并结合应用场景一、应用场景二对本发明实施例的技术方案作进一步说明。

[0063] 应用场景一

[0064] 当前客户端 21 利用配置的加密密钥 A 对源代码进行加密，并发送源代码上传请求至所述接入网关 22，所述接入网关 22 接收到所述源代码上传请求，对所述当前客户端 21 进行身份验证，当确定所述当前客户端 21 输入的用户名与密码均正确时，返回所述源代码上传请求的允许应答消息至所述当前客户端 21，所述当前客户端 21 接收到所述允许上传的应答消息后，上传加密后的源代码至所述版本控制服务器 23，所述版本控制服务器 23 利用配置的解密密钥 A’ 对加密后的源代码进行解密，并保存。

[0065] 所述接入网关 22 可设置有指定周期内允许客户端输入用户名与密码的最大次数，如指定周期为一天、允许输入的最大次数为 3 次。

[0066] 当接入网关 22 确定所述当前客户端 21 第一次和 / 或第二次输入的用户名与密码不正确时，返回所述源代码上传请求的重试应答消息至所述当前客户端 21，所述当前客户端 21 重新输入用户名与密码。当所述接入网关 22 确定所述当前客户端 21 当前输入次数小于等于 3 次且当前输入次数下输入的用户名与密码均正确后，返回所述源代码上传请求的允许应答消息至所述当前客户端 21，所述当前客户端 21 接收到所述允许上传的应答消息后，上传加密后的源代码至所述版本控制服务器 23，所述版本控制服务器 23 利用配置的解密密钥 A’ 对加密后的源代码进行解密，并保存。

[0067] 所述接入网关 22 确定在该天内当前客户端 21 当前输入次数超出预设的最高次数 3 次时，所述接入网关 22 返回禁止上传的应答消息至当前客户端 21，在该天内当前客户端 21 不可再进行用户名与密码的输入，该天内当前客户端 21 无法将加密后的源代码文件上传至所述版本控制服务器 23。

[0068] 在应用场景一中，配置当前客户端 21 的加密密钥为 A，相应的，配置版本控制服务器 23 的解密密钥为 A’。

[0069] 应用场景二

[0070] 当前客户端 21 想要下载版本控制服务器 23 中保存的源代码(应用程序文件)时，当前客户端 21 发送源代码下载请求至所述接入网关 22，所述接入网关 22 接收到所述源代码下载请求后，对所述当前客户端 21 进行身份验证，当确定所述当前客户端 21 输入的用户名与密码均正确时，返回所述源代码下载请求的允许应答消息至所述当前客户端 21，并通知所述版本控制服务器 23 下载所述源代码到当前客户端 21。所述版本控制服务器 23 利用配置的加密密钥 A 对源代码进行加密后，发送至所述当前客户端 21，当前客户端 21 利用配置的解密密钥 A' 对加密后的源代码进行解密，并显示解密后的所述源代码。

[0071] 所述接入网关 22 还可以设置指定周期内允许客户端输入用户名与密码的最大次数，如指定周期为一天、所述最大次数为 3 次。

[0072] 当接入网关 22 确定当前客户端 21 第一次和 / 或第二次输入的用户名与密码不正确时，返回所述源代码下载请求的重试应答消息至所述当前客户端 21，所述当前客户端 21 重新输入用户名与密码，当所述接入网关 22 确定所述当前客户端当前输入次数小于等于 3 次且当前输入次数下输入的用户名与密码均正确后，返回所述源代码下载请求的允许应答消息至所述当前客户端 21，并通知所述版本控制服务器 23 传送源代码至所述当前客户端 21。所述版本控制服务器 23 利用配置的加密密钥 A 对源代码进行加密后，再至所述当前客户端 21，当前客户端 21 利用配置的解密密钥 A' 对加密后的源代码进行解密，并显示解密后的所述源代码。

[0073] 接入网关 22 确定在该天内当前客户端 21 当前的输入次数超出最大次数第 3 次时，所述接入网关 22 返回所述源代码下载请求的禁止下载应答消息至所述当前客户端 21，在该天内所述当前客户端 21 不可再进行用户名与密码的输入，进而在该天内所述当前客户端 21 无法下载所述版本控制服务器 23 中保存的源代码。

[0074] 在应用场景二中，配置版本控制服务器 23 的加密密钥为 A，相应的，配置当前客户端 21 的解密密钥 A'。

[0075] 本领域技术人员应当理解，图 2 中所示的实现数据安全保护的系统中的各处理模块的实现功能可参照前述实现数据安全保护的方法的相关描述而理解。本领域技术人员应当理解，图 2 所示的实现数据安全保护的系统中各处理单元的功能可通过运行于处理器上的程序而实现，也可通过具体的逻辑电路而实现。

[0076] 本发明实施例提供的实现数据安全保护的方法与系统，分别为客户端及版本控制服务器配置加解密密钥；并在客户端与版本控制服务器之间增设接入网关；客户端利用配置的加密密钥对源代码进行加密，在所述接入网关接收到由客户端发送的源代码上传请求后，对所述客户端进行身份验证，确定所述身份验证合法时，允许所述客户端上传加密后的源代码至所述版本控制服务器；所述版本控制服务器利用所配置的解密密钥对加密后的源代码进行解密。本发明的技术方案，将源代码进行了加密处理后上传至版本控制服务器，同时增设了接入网关，只有在接入网关确定发起源代码上传 / 下载请求客户端的身份验证为合法时，才允许客户端上传源代码、或允许客户端下载版本控制服务器中保存的源代码到客户端。由此可见，利用本发明的技术方案，提高了数据传输的安全性、保证了数据应用的可靠性。

[0077] 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

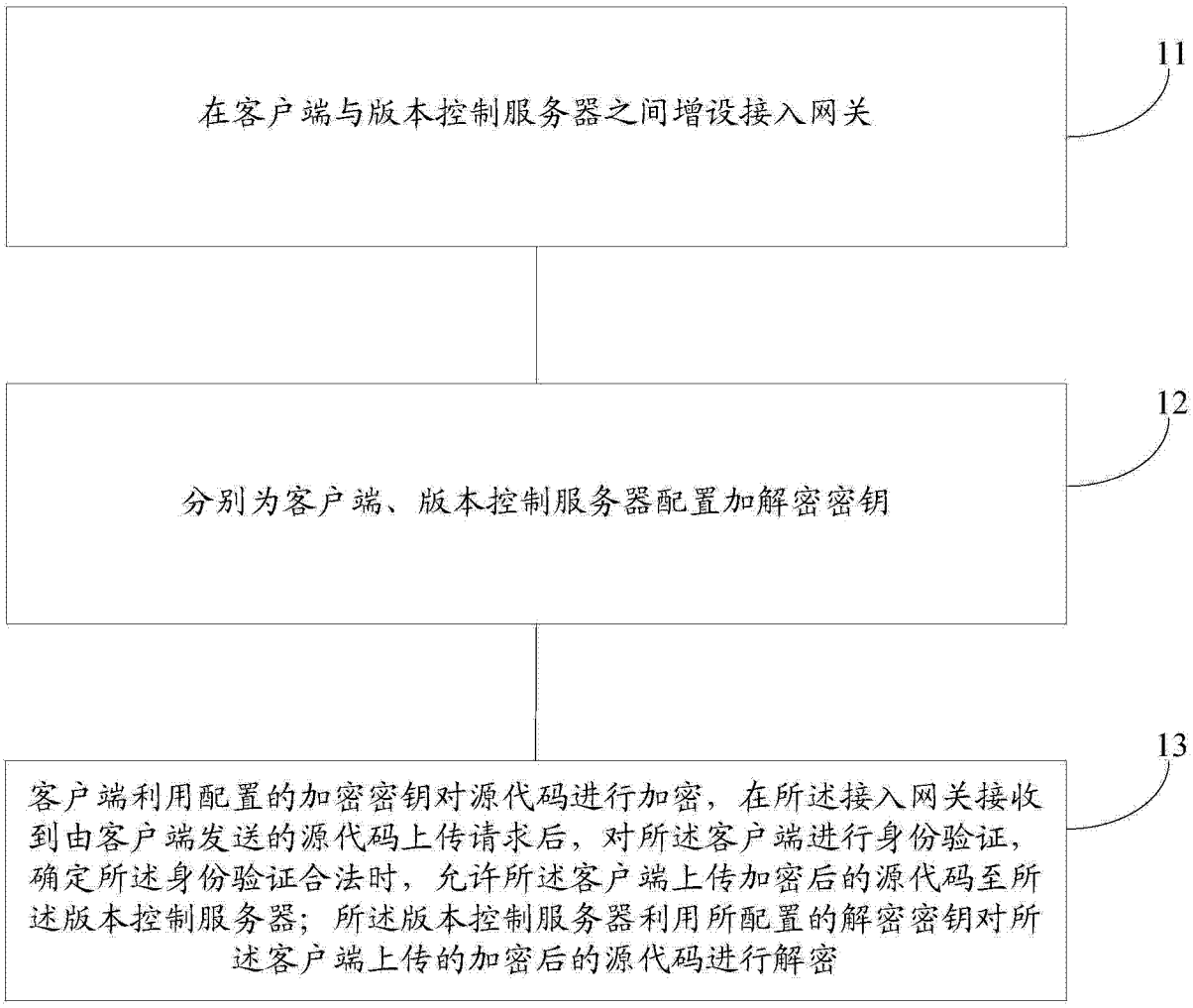

在客户端与版本控制服务器之间增设接入网关
11
分别为客户端、版本控制服务器配置加解密密钥
12
客户端利用配置的加密密钥对源代码进行加密，在所述接入网关接收到由客户端发送的源代码上传请求后，对所述客户端进行身份验证，确定所述身份验证合法时，允许所述客户端上传加密后的源代码至所述版本控制服务器；所述版本控制服务器利用所配置的解密密钥对所述客户端上传的加密后的源代码进行解密
13

图 1

图 2