(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 105027131 A
(43)申请公布日 2015.11.04

(21)申请号 201380073968.0
(22)申请日 2013.06.28
(30)优先权数据
10-2012-0155630 2012.12.27 KR
10-2013-0074461 2013.06.27 KR
(85)PCT国际申请进入国家阶段日
2015.08.27
(86)PCT国际申请的申请数据
PCT/KR2013/005764 2013.06.28
(87)PCT国际申请的公布数据
WO2014/104507 KO 2014.07.03
(71)申请人 罗文有限公司
地址 韩国首尔
(72)发明人 梁基昊 黄在烨
(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 徐川 武晨燕
(51)Int.Cl.
G06F 21/30(2006.01)

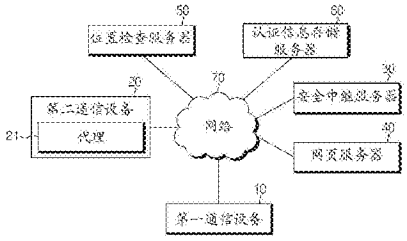
权利要求书6页 说明书21页 附图11页

(54)发明名称

用于安全登录的系统、方法及其设备

(57)摘要

本发明公开了一种用于允许与多个设备相关联的用户进行登录的安全登录系统、方法及其设备。用于允许访问网站的通信设备进行安全登录的安全登录方法包括：认证数据提供设备确定所述认证数据提供设备与所述通信设备是否位于同一地点；当确定的结果为所述认证数据提供设备与所述通信设备位于同一地点时，所述认证数据提供设备获取所述通信设备的认证相关数据；以及所述认证数据提供设备将获取的认证相关数据提供给所述通信设备或所述网站。



10:第一通信设备
20:第二通信设备
21:代理
30:安全中继服务器
40:网页服务器
50:位置检查服务器
60:认证信息存储服务器
70:网络

CN 105027131 A

1. 一种用于允许访问网站的通信设备的安全登录的安全登录方法，所述方法包括：

认证数据提供设备确定所述认证数据提供设备与所述通信设备是否位于同一地点；

当所述确定的结果为所述认证数据提供设备与所述通信设备位于同一地点时，所述认证数据提供设备获取所述通信设备的认证相关数据；以及

所述认证数据提供设备将获取的认证相关数据提供给所述通信设备或所述网站。

2. 根据权利要求 1 所述的安全登录方法，其中，所述获取认证相关数据包括：

向所述通信设备请求解密密钥，并从所述通信设备接收所述解密密钥；以及

提取加密的登录认证信息，并通过使用所述解密密钥对提取的登录认证信息进行解密，

其中，所述提供认证相关数据包括将解密的登录认证信息提供给所述网站或所述通信设备。

3. 根据权利要求 2 所述的安全登录方法，还包括：

所述认证数据提供设备检查所述通信设备的访问令牌，

其中，所述提供认证相关数据包括将所述访问令牌连同所述登录认证信息一起提供给所述网站。

4. 根据权利要求 1 所述的安全登录方法，

其中，所述获取认证相关数据包括提取加密的登录认证信息，

其中，所述提供认证相关数据包括将提取的加密的登录认证信息提供给所述通信设备，

其中，所述方法还包括：

所述通信设备通过使用已经存储的解密密钥来对从所述认证数据提供设备接收的所述加密的登录认证信息进行解密；以及

所述通信设备通过使用解密的登录认证信息来对所述网站进行认证。

5. 根据权利要求 1 所述的安全登录方法，

其中，所述获取认证相关数据包括提取解密密钥，

其中，所述提供认证相关数据包括将提取的解密密钥提供给所述通信设备，

其中，所述方法还包括：

所述通信设备通过使用所述解密密钥来对已经存储的加密的登录认证信息进行解密；以及

所述通信设备通过使用解密的登录认证信息来对所述网站进行认证。

6. 根据权利要求 1 所述的安全登录方法，

其中，所述获取认证相关数据包括提取认证信息存储地址，

其中，所述提供认证相关数据包括将提取的认证信息存储地址提供给所述通信设备，

其中，所述方法还包括：

所述通信设备从认证信息存储服务器接收存储在所述认证信息存储地址处的认证信息；以及

所述通信设备通过使用接收到的认证信息来对所述网站进行认证。

7. 根据权利要求 6 所述的安全登录方法，还包括：

所述通信设备对从所述认证数据提供设备接收的所述认证信息存储地址进行解密。

8. 根据权利要求 1 所述的安全登录方法，还包括 ：

所述认证数据提供设备检查所述网站的安全等级，

其中，所述获取认证相关数据包括 ：

当所述确定的结果为所述认证数据提供设备与所述通信设备位于同一地点时，应用检查出的安全等级 ；以及

基于所应用的安全等级来获取所述认证相关数据。

9. 根据权利要求 8 所述的安全登录方法，

其中，所述获取认证相关数据包括 ：

当所述确定的结果为所述认证数据提供设备与所述通信设备不位于同一地点时，应用比所述检查出的安全等级高的加强的安全等级 ；以及

基于所应用的加强的安全等级来获取所述认证相关数据。

10. 根据权利要求 9 所述的安全登录方法，

其中，所述获取认证相关数据包括 ：当所应用的安全等级高于阈值等级时，获取加强的认证信息 ；以及

其中，所述提供认证相关数据包括将所述加强的认证信息提供给所述网站或所述通信设备。

11. 根据权利要求 9 所述的安全登录方法，

其中，所述获取认证相关数据包括 ：在所应用的安全等级高于阈值等级的情况下，当用户成功进行用户认证时，获取所述认证相关数据。

12. 根据权利要求 9 所述的安全登录方法，

其中，所述获取认证相关数据包括 ：

当所应用的安全等级为预设的特定安全等级时，输出用于请求所述通信设备允许登录的通知窗口 ；以及

当通过所述通知窗口输入批准信号时，获取所述认证相关数据。

13. 根据权利要求 1 所述的安全登录方法，在所述提供认证相关数据之后，还包括 ：

所述认证数据提供设备监测所述认证数据提供设备与所述通信设备是否一直位于同一地点 ；以及

当所述监测的结果为所述认证数据提供设备与所述通信设备不位于同一地点时，所述认证数据提供设备执行所述通信设备的登出。

14. 根据权利要求 1 所述的安全登录方法，还包括 ：

当所述确定的结果为确定所述认证数据提供设备与所述通信设备位于同一地点时，所述认证数据提供设备将安全登录激活消息提供给所述通信设备。

15. 一种认证数据提供设备，包括 ：

至少一个处理器 ；

存储器 ；以及

至少一个程序，其被存储在所述存储器中并被配置为由所述至少一个处理器执行，

其中，所述程序包括 ：

位置检查模块，其被配置为确定注册了安全登录服务的通信设备与所述认证数据提供设备是否位于同一地点 ；

认证数据获取模块，其被配置为当所述位置检查模块确定所述通信设备与所述认证数据提供设备位于同一地点时，获取所述通信设备所访问的网站的认证相关数据；以及

认证数据提供模块，其被配置为将获取的认证相关数据提供给所述网站或所述通信设备。

16. 根据权利要求 15 所述的认证数据提供设备，还包括：

数据存储模块，其被配置为存储加密的登录认证信息，

其中，所述认证数据获取模块向所述通信设备请求解密密钥，并从所述通信设备接收所述解密密钥，然后提取存储在所述数据存储模块中的加密的登录认证信息，并通过使用所述解密密钥来对提取的登录认证信息进行解密；以及

其中，所述认证数据提供模块将解密的登录认证信息提供给所述网站或所述通信设备。

17. 根据权利要求 16 所述的认证数据提供设备，

其中，所述认证数据提供模块检查所述通信设备的访问令牌，并将所述访问令牌连同所述登录认证信息一起提供给所述网站。

18. 根据权利要求 15 所述的认证数据提供设备，还包括：

数据存储模块，其被配置为存储加密的登录认证信息，

其中，所述认证数据获取模块提取存储在所述数据存储模块中的加密的登录认证信息；以及

其中，所述认证数据提供模块将提取的加密的登录认证信息提供给所述通信设备。

19. 根据权利要求 15 所述的认证数据提供设备，还包括：

数据存储模块，其被配置为存储解密密钥，该解密密钥用于对存储在所述通信设备中的加密的登录认证信息进行解密，

其中，所述认证数据获取模块从所述数据存储模块中提取解密密钥；以及

其中，所述认证数据提供模块将提取的解密密钥提供给所述通信设备。

20. 根据权利要求 15 所述的认证数据提供设备，还包括：

数据存储模块，其被配置为存储认证信息存储地址，登录认证信息被存储在该认证信息存储地址处，

其中，所述认证数据获取模块从所述数据存储模块中提取所述网站的认证信息存储地址；以及

其中，所述认证数据提供模块将提取的认证信息存储地址提供给所述通信设备。

21. 根据权利要求 15 所述的认证数据提供设备，还包括：

安全策略应用模块，其被配置为检查所述网站的安全策略，并且当所述位置检查模块确定所述通信设备与所述认证数据提供设备位于同一地点时，应用检查出的安全等级，

其中，所述认证数据获取模块基于所述安全策略应用模块所应用的安全等级来获取所述认证相关数据。

22. 根据权利要求 21 所述的认证数据提供设备，

其中，当所述通信设备与所述认证数据提供设备不位于同一地点时，所述安全策略应用模块应用比所述检查出的安全等级高的加强的安全等级。

23. 根据权利要求 22 所述的认证数据提供设备，

其中，当所述安全策略应用模块所应用的安全等级高于阈值等级时，所述认证数据获取模块获取加强的认证信息；以及

其中，所述认证数据提供模块将所述加强的认证信息提供给所述网站或所述通信设备。

24. 根据权利要求 22 所述的认证数据提供设备，

其中，在所述安全策略应用模块所应用的安全等级高于阈值等级的情况下，当用户成功进行用户认证时，所述认证数据获取模块获取所述认证相关数据。

25. 根据权利要求 22 所述的认证数据提供设备，

其中，在所述安全策略应用模块所应用的安全等级为预设的特定安全等级的情况下，所述认证数据获取模块输出用于请求所述通信设备允许登录的通知窗口，并且当通过所述通知窗口输入批准信号时，获取所述认证相关数据。

26. 根据权利要求 15 所述的认证数据提供设备，

其中，在通信设备成功登录所述网站的情况下，所述位置检查模块监测所述通信设备与所述认证数据提供设备是否一直位于同一地点，并且当所述通信设备与所述认证数据提供设备不位于同一地点时，执行所述通信设备的登出。

27. 根据权利要求 15 所述的认证数据提供设备，

其中，当确定所述通信设备与所述认证数据提供设备位于同一地点时，所述位置检查模块将安全登录激活消息发送所述通信设备，以激活所述通信设备的安全登录菜单。

28. 一种安全登录系统，包括：

第二通信设备；

第一通信设备，其被配置为确定所述第一通信设备与所述第二通信设备是否位于同一地点，并且当所述第一通信设备与所述第二通信设备位于同一地点时，获取所述第二通信设备所访问的网站的认证相关数据，并将所述认证相关数据提供给所述第二通信设备或网页服务器；以及

网页服务器，其被配置为从所述第一通信设备或所述第二通信设备接收认证相关数据，并对所述第二通信设备进行登录认证。

29. 根据权利要求 28 所述的安全登录系统，

其中，所述第一通信设备向所述第二通信设备请求解密密钥，并从所述第二通信设备接收所述解密密钥，然后提取加密的登录认证信息，并通过使用所述解密密钥来对提取的登录认证信息进行解密；以及

其中，所述网页服务器基于从所述第一通信设备提供的所述登录认证信息来执行对所述第二通信设备的登录认证。

30. 根据权利要求 29 所述的安全登录系统，

其中，所述第一通信设备检查所述通信设备的访问令牌，并将所述访问令牌连同所述登录认证信息一起提供给所述网页服务器；以及

其中，所述网页服务器基于所述访问令牌识别所述第二通信设备并执行登录认证。

31. 根据权利要求 28 所述的安全登录系统，

其中，所述第一通信设备提取加密的登录认证信息，并将加密的登录认证信息提供给所述第二通信设备；以及

其中，所述第二通信设备通过使用已经存储的解密密钥来对从所述第一通信设备接收的所述加密的登录认证信息进行解密，并将解密的登录认证信息发送至所述网页服务器以执行登录认证。

32. 根据权利要求 28 所述的安全登录系统，

其中，所述第一通信设备提取解密密钥，并将提取的解密密钥提供给所述第二通信设备；

其中，所述第二通信设备通过使用从所述第一通信设备接收的所述解密密钥来对已经存储的加密的登录认证信息进行解密，并将解密的登录认证信息发送至所述网页服务器；以及

其中，所述网页服务器基于从所述第二通信设备接收的所述认证信息来执行对所述第二通信设备的登录认证。

33. 根据权利要求 28 所述的安全登录系统，

其中，所述第一通信设备提取认证信息存储地址并将所述认证信息存储地址发送至所述第二通信设备，认证信息被存储在所述认证信息存储地址处；

其中，所述第二通信设备从认证信息存储服务器接收存储在所述认证信息存储地址处的所述认证信息；以及

其中，所述网页服务器从所述第二通信设备接收所述认证信息，并执行对所述第二通信设备的登录认证。

34. 根据权利要求 33 所述的安全登录系统，

其中，所述第二通信设备对从所述第一通信设备接收的所述认证信息存储地址进行解密，然后从所述认证信息存储服务器接收存储在所述认证信息存储地址处的所述认证信息。

35. 根据权利要求 28 所述的安全登录系统，

其中，所述第一通信设备检查所述网站的安全等级，并且当所述第一通信设备与所述第二通信设备位于同一地点时，所述第一通信设备应用检查出的安全等级以基于所应用的安全等级来获取所述认证相关数据。

36. 根据权利要求 35 所述的安全登录系统，

其中，当所述第一通信设备与所述第二通信设备不位于同一地点时，所述第一通信设备应用比所述检查出的安全等级高的加强的安全等级，并基于所应用的加强的安全等级来获取所述认证相关数据。

37. 根据权利要求 36 所述的安全登录系统，

其中，当所应用的安全等级高于阈值等级时，所述第一通信设备获取加强的认证信息，并将所述加强的认证信息提供给所述网页服务器或所述第二通信设备；以及

其中，所述网页服务器基于从所述第一通信设备或所述第二通信设备接收的所述加强的认证信息来执行对所述第二通信设备的登录认证。

38. 根据权利要求 36 所述的安全登录系统，

其中，当所应用的安全等级高于阈值等级时，所述第一通信设备执行对用户的用户认证，并且当所述用户认证成功时，获取所述认证相关数据。

39. 根据权利要求 36 所述的安全登录系统，

其中，在所应用的安全等级为预设的特定安全等级的情况下，所述第一通信设备输出用于请求所述第二通信设备允许登录的通知窗口，并且当通过所述通知窗口输入批准信号时，获取所述认证相关数据。

40. 根据权利要求 28 所述的安全登录系统，

其中，在所述第二通信设备成功登录的情况下，所述第一通信设备监测所述第一通信设备与所述第二通信设备是否一直位于同一地点，并且当所述第一通信设备与所述第二通信设备不位于同一地点时，执行所述第二通信设备的登出。

41. 根据权利要求 28 所述的安全登录系统，

其中，当确定所述第一通信设备与所述第二通信设备位于同一地点时，所述第一通信设备将安全登录激活消息发送至所述第二通信设备；以及

其中，当接收到所述安全登录激活消息时，所述第二通信设备激活安全登录菜单。

用于安全登录的系统、方法及其设备

技术领域

[0001] 本发明涉及登录处理技术，并且更具体地，涉及一种用于允许与多个设备相关联的用户进行登录的安全登录系统、方法及其设备。

[0002] 本申请要求于2012年12月27日递交到韩国知识产权局的韩国专利申请No.10-2012-0155630以及于2013年6月27日递交到韩国知识产权局的韩国专利申请No.10-2013-0074461的权益，故通过引用的方式将这些申请的全部内容整体合并到本申请中。

背景技术

[0003] 密码认证被用作进行用户认证的通用方法。在密码认证中，用户访问网页服务器并设定其ID和密码，然后通过在终端上输入所设定的ID和密码来登录网页服务器。此外，作为现有密码认证的改进，提出了一种通过使用由用户设定的触摸图案来认证该用户的技术。韩国未审查专利公布No.10-2009-0013432公开了一种用于通过使用图案来认证用户的便携式终端及其锁定和释放方法。

[0004] 然而，如果使用该方法，则用户的认证信息（即用户的密码和ID）可能被其它人借助于肩窥其它所获取。此外，如果特定用户的ID和密码被他人获取，则该用户的个人数据可能持续地暴露于他人，直到该特定用户改变ID和密码或者取消会员身份为止。

发明内容

[0005] 技术问题

[0006] 本发明被设计用于解决相关技术的问题，因此本发明旨在提供一种用于保护用户的认证信息免受外界所入侵（比如肩窥）以及加强认证信息的安全性的安全登录系统、方法及其设备。

[0007] 通过以下描述将理解本发明的其它目的和优点，并且应当理解的是，这些目的和优点可通过权利要求书中所限定的装置、方法及其组合来实现。

[0008] 技术方案

[0009] 在本发明的一个方面，提供了一种用于允许访问网站的通信设备的安全登录的安全登录方法，该方法包括：认证数据提供设备确定所述认证数据提供设备与所述通信设备是否位于同一地点；当所述确定的结果为所述认证数据提供设备与所述通信设备位于同一地点时，所述认证数据提供设备获取所述通信设备的认证相关数据；以及所述认证数据提供设备将获取的认证相关数据提供给所述通信设备或所述网站。

[0010] 所述获取认证相关数据可包括：向所述通信设备请求解密密钥，并从所述通信设备接收所述解密密钥；以及提取加密的登录认证信息并通过使用所述解密密钥对提取的登录认证信息进行解密，其中，所述提供认证相关数据包括将解密的登录认证信息提供给所述网站或所述通信设备。

[0011] 所述方法还可包括：所述认证数据提供设备检查所述通信设备的访问令牌，其中，

所述提供认证相关数据包括将所述访问令牌连同所述登录认证信息一起提供给所述网站。

[0012] 此外，所述获取认证相关数据可包括提取加密的登录认证信息，所述提供认证相关数据可包括将提取的加密的登录认证信息提供给所述通信设备，以及所述方法还可包括：所述通信设备通过使用已经存储的解密密钥来对从所述认证数据提供设备接收的所述加密的登录认证信息进行解密；以及所述通信设备通过使用解密的登录认证信息来对所述网站进行认证。

[0013] 此外，所述获取认证相关数据可包括提取解密密钥，所述提供认证相关数据可包括将提取的解密密钥提供给所述通信设备，以及所述方法还可包括：所述通信设备通过使用所述解密密钥来对已经存储的加密的登录认证信息进行解密；以及所述通信设备使用解密的登录认证信息来对所述网站进行认证。

[0014] 此外，所述获取认证相关数据可包括提取认证信息存储地址，所述提供认证相关数据可包括将提取的认证信息存储地址提供给所述通信设备，以及所述方法还可包括：所述通信设备从认证信息存储服务器接收存储在所述认证信息存储地址处的认证信息；以及所述通信设备使用接收的认证信息来对所述网站进行认证。在这一情况下，所述方法还可包括：所述通信设备对从所述认证数据提供设备接收的所述认证信息存储地址进行解密。

[0015] 所述方法还可包括：所述认证数据提供设备检查所述网站的安全等级，以及所述获取认证相关数据可包括：当确定的结果为所述认证数据提供设备与所述通信设备位于同一地点时，应用检查出的安全等级；以及基于所应用的安全等级来获取所述认证相关数据。

[0016] 所述获取认证相关数据可包括：当确定的结果为所述认证数据提供设备与所述通信设备不位于同一地点时，应用比所述检查出的安全等级高的加强的安全等级；以及基于所应用的加强的安全等级来获取所述认证相关数据。

[0017] 进一步地，所述获取认证相关数据可包括：当所应用的安全等级高于阈值等级时，获取加强的认证信息；以及所述提供认证相关数据可包括将所述加强的认证信息提供给所述网站或所述通信设备。

[0018] 此外，所述获取认证相关数据可包括：在所应用的安全等级高于阈值等级的情况下，当用户成功进行用户认证时，获取所述认证相关数据。

[0019] 同时，所述获取认证相关数据可包括：当所应用的安全等级为预设的特定安全等级时，输出用于请求所述通信设备允许登录的通知窗口；以及当通过所述通知窗口输入批准信号时，获取所述认证相关数据。

[0020] 所述方法还可包括：所述认证数据提供设备监测所述认证数据提供设备与所述通信设备是否一直位于同一地点；以及当监测的结果为所述认证数据提供设备与所述通信设备不位于同一地点时，所述认证数据提供设备执行所述通信设备的登出。

[0021] 此外，所述方法还可包括：当确定的结果为确定出所述认证数据提供设备与所述通信设备位于同一地点时，所述认证数据提供设备将安全登录激活消息提供给所述通信设备。

[0022] 在本发明的第二方面，还提供了一种认证数据提供设备，包括：至少一个处理器；存储器；以及至少一个程序，其被存储在所述存储器中并被配置为由所述至少一个处理器执行，其中，所述程序包括：位置检查模块，其被配置为确定注册了安全登录服务的通信设备与所述认证数据提供设备是否位于同一地点；认证数据获取模块，其被配置为当所述位

置检查模块确定所述通信设备与所述认证数据提供设备位于同一地点时，获取所述通信设备所访问的网站的认证相关数据；以及认证数据提供模块，其被配置为将获取的认证相关数据提供给所述网站或所述通信设备。

[0023] 在本发明的第三方面，还提供了一种安全登录系统，包括：第二通信设备；第一通信设备，其被配置为确定所述第一通信设备与所述第二通信设备是否位于同一地点，以及在所述第一通信设备与所述第二通信设备位于同一地点时，获取所述第二通信设备所访问的网站的认证相关数据并将所述认证相关数据提供给所述第二通信设备或网页服务器；以及网页服务器，其被配置为从所述第一通信设备或所述第二通信设备接收认证相关数据并执行对所述第二通信设备的登录认证。

[0024] 有益效果

[0025] 在本发明中，由于第一通信设备和第二通信设备被关联以向网页服务器提供登录认证信息，所以能够保护用户的 ID 和密码免受肩窥，并且加强了用户的认证信息的安全性。

[0026] 此外，在本发明中，由于基于多个通信设备的位置信息对登录认证信息的安全等级进行了加强或者登录认证信息被选择性地提供到网页服务器，所以能够进一步加强用户的认证信息的安全性。

[0027] 此外，在本发明中，由于解密密钥从特定的设备获得，然后对加密的登录认证信息进行解密，所以即使加密的登录认证信息被他人获取，该加密的登录认证信息也无法被他人解密，因此，用户的认证信息可受到保护而不被外界所入侵。

[0028] 此外，在本发明中，如果成功登录之后多个指定的通信设备离开了同一地点，则成功登录的通信设备被强制登出，以防止非法用户使用网页服务。

附图说明

[0029] 附图示出了本发明的优选实施例，并且与上文公开的内容一起用于提供对本发明的技术特征的进一步理解。然而，本发明不被解读为限于附图。

[0030] 图 1 为示出根据本发明实施例的安全登录系统的图。

[0031] 图 2 为示出了根据本发明一实施例的一种用于在安全登录系统中进行登录认证的方法的流程图。

[0032] 图 3 为示出了显示根据本发明实施例的安全登录菜单的网页的图。

[0033] 图 4 为用于示出根据本发明另一实施例的一种用于在安全登录系统中进行登录认证的方法的流程图。

[0034] 图 5 为用于示出根据本发明另一实施例的一种用于在安全登录系统中进行登录认证的方法的流程图。

[0035] 图 6 为用于示出根据本发明另一实施例的一种用于在安全登录系统中进行登录认证的方法的流程图。

[0036] 图 7 为用于示出根据本发明实施例的一种用于将已经登录安全登录系统的通信设备强制登出的方法的流程图。

[0037] 图 8 为示出根据本发明实施例的认证数据提供设备的图。

[0038] 图 9 为示出根据本发明实施例的安全登录程序的图。

[0039] 图 10 为用于示出根据本发明实施例的一种用于在认证数据提供设备中提供认证相关数据的方法的流程图。

[0040] 图 11 为用于示出根据本发明实施例的一种用于在认证数据提供设备中强制登出通信设备的方法的流程图。

具体实施方式

[0041] 下文中，将参照附图对本发明的优选实施例进行详细描述。在描述之前，应当理解的是，说明书和所附权利要求书中所使用的术语不应当被解读为限于通常或字典中的含义，而应当基于本发明的技术方面所对应的含义和概念在发明人为了最好地解释而被允许适当地限定这些术语的原则下进行理解。因此，此处给出的描述仅是出于示例目的的优选示例，而不意在限制本发明的范围，所以应当理解的是，可在不超出本发明范围的情况下，进行等同替换和修改。

[0042] 图 1 为示出根据本发明实施例的安全登录系统的图。

[0043] 如图 1 所示，根据本发明实施例的安全登录系统包括第一通信设备 10、第二通信设备 20、安全中继服务器 30、网页服务器 40、位置检查服务器 50 以及认证信息存储服务器 60。

[0044] 第一通信设备 10、第二通信设备 20、安全中继服务器 30、网页服务器 40、位置检查服务器 50 以及认证信息存储服务器 60 通过网络 70 相互通信。在本文中，网络 70 包括移动通信网络、有线互联网网络、本地无线通信网络等，这在现有技术中是周知的因而在此不再详述。

[0045] 网页服务器 40 是用于向用户提供在线服务的服务器，所述服务例如为门户服务 (portal service)、金融服务、在线购物服务、电子商务服务等，并且网页服务器 40 存储每个用户的 ID 和密码。此外，网页服务器 40 可以存储每个用户的加强的认证信息，比如一次性密码 (OTP)、生物信息等。特别地，当第二通信设备 20 试图登录时，网页服务器 40 从第一通信设备 10 或第二通信设备 20 接收第二通信设备 20 的登录认证信息 (即 ID 和密码)，并且基于登录认证信息对第二通信设备 20 进行登录认证。此外，网页服务器 40 可从第一通信设备 10 或第二通信设备 20 接收加强的认证信息，并且基于加强的认证信息进行用户认证。

[0046] 安全中继服务器 30 存储一个表，在该表中，至少一个用户标识信息与第一通信设备 10 的标识信息相映射。此时，安全中继服务器 30 可将以下各项中的任一项存储为第一通信设备 10 的标识信息 :第一通信设备 10 的电话号码、IP 地址、MAC 地址、以及安装在第一通信设备 10 中的安全登录应用的标识信息 ;并且还可将安全登录服务 ID、居民登记号码、互联网个人标识号 (I-PIN)、移动通信电话号码等存储为用户标识信息。

[0047] 特别地，如果第二通信设备 20 开始浏览网页，则安全中继服务器 30 从第二通信设备 20 接收包含用户标识信息的服务通知消息，对与用户标识信息相映射的第一通信设备 10 的标识信息进行检查，然后将服务通知消息发送至具有该标识信息的第一通信设备 10。

[0048] 此外，如果从第二通信设备 20 接收到登录通知消息，则安全中继服务器 30 对与第二通信设备 20 的用户标识信息相映射的第一通信设备 10 的标识信息进行检查，并且将登录通知消息发送至具有该标识信息的第一通信设备 10。安全中继服务器 30 可将服务通知

消息或登录通知消息作为推送消息进行发送。

[0049] 位置检查服务器 50 对第二通信设备 20 或第一通信设备 10 所处的地点进行检查。特别地，位置检查服务器 50 存储与无线电基站的标识信息相映射的位置信息，并且如果从第二通信设备 20 或第一通信设备 10 接收到无线电基站的标识信息，则位置检查服务器 50 对与无线电基站的标识信息相映射的位置信息进行检查，并且将该位置信息发送至第二通信设备 20 或第一通信设备 10。

[0050] 认证信息存储服务器 60 针对每个用户存储每个站点的加密的登录认证信息。此时，认证信息存储服务器 60 指定登录认证信息的存储地址，并将加密的登录认证信息分别存储在所指定的存储地址处。此外，认证信息存储服务器 60 可存储每个用户的加强的认证信息。

[0051] 第二通信设备 20 试图登录到网页服务器 40，并且用于安全登录服务的代理 21 被装载到第二通信设备 20 中。如果第二通信设备 20 开始浏览网页，则代理 21 将包含用户标识信息的服务通知消息发送至安全中继服务器 30。代理 21 可检查第二通信设备 20 的位置信息，并将该位置信息包括在服务通知消息中。此外，代理 21 监测第二通信设备 20 是否对特定的站点进行登录，并且如果第二通信设备 20 对特定的站点进行登录，则代理 21 生成登录通知消息并将该登录通知消息发送至安全中继服务器 30，所述登录通知消息包含试图登录的网站的标识信息、登录用户的标识信息和第二通信设备 20 的标识信息。

[0052] 此外，代理 21 在网页中输出显示安全登录服务的昵称或 ID 的安全登录菜单（参见图 3），并且如果有对安全登录菜单的输入，则代理 21 可生成登录通知消息并将该登录通知消息发送至安全中继服务器 30。选择性地，如果第二通信设备 20 从网页服务器 40 接收到具有登录菜单的网页，则代理 21 可立即生成登录通知消息，并将该登录通知消息发送至安全中继服务器 30。此外，如果从第一通信设备 10 接收到安全登录菜单激活消息，则代理 21 将去激活的安全登录菜单激活，以使得用户可认识到第一通信设备 10 和第二通信设备 20 位于同一地点。此时，代理 21 可通过将安全登录菜单的深色改变为亮色、使安全登录菜单闪烁、或者向安全登录菜单输出激活图形标记，来激活安全登录菜单。

[0053] 在一个实施例中，代理 21 可存储解密密钥并将该解密密钥提供给指定的第一通信设备 10。代理 21 自动生成并存储用于用户的固有解密密钥。存储在第二通信设备 20 中的解密密钥用于解密登录认证信息，根据下述的第一等级和第二等级的安全策略对登录认证信息进行分类。

[0054] 在另一实施例中，代理 21 可从第一通信设备 10 接收加密的认证信息，通过使用代理中存储的解密密钥来解密该认证信息，然后通过使用解密的认证信息来向网页服务器 40 进行登录认证。

[0055] 在另一实施例中，代理 21 可存储每个网站的加密的认证信息，从第一通信设备 10 接收用于解密相应的认证信息的解密密钥，通过使用解密密钥来解密认证信息，以及将解密的认证信息提供给网页服务器 40。

[0056] 此外，在另一实施例中，代理 21 可从第一通信设备 10 接收认证信息存储地址，以及可从认证信息存储服务器 60 接收存储在该认证信息存储地址处的认证信息。

[0057] 在没有具体限制的情况下，第二通信设备 20 可使用能够经由网络 70 访问网页服务器 40 的任何通信设备，例如台式计算机、平板计算机、笔记本电脑、移动通信终端等。此

外，当安全登录应用或插件被安装时，代理 21 可被装载在第二通信设备 20 中。此外，如果包括在网页中的安全登录脚本被执行，则代理 21 可被装载在第二通信设备 20 中。此外，代理 21 还可执行其它脚本、网页存储 (web storage) 或者其它程序或指令，例如 cookies。

[0058] 第一通信设备 10 将认证相关数据提供给第二通信设备 20 或网页服务器 40。认证相关数据包括以下各项至少之一 :解密密钥、登录认证信息 (即 ID 和密码)、加强的认证信息以及认证信息存储地址。第一通信设备 10 基于第二通信设备 20 的位置信息来应用安全等级。为此，第一通信设备 10 可存储安全策略表并且存储第二通信设备 20 的位置信息，在所述安全策略表中网站标识信息与安全等级相映射。

[0059] 此外，如果从安全中继服务器 30 接收到通知第二通信设备 20 的安全登录服务的发起的服务通知消息，则第一通信设备 10 将自身的位置信息与第二通信设备 20 的位置信息相比较，并确定第一通信设备 10 和第二通信设备 20 是否位于同一地点。如果确定第一通信设备 10 和第二通信设备 20 位于同一地点，则第一通信设备 10 将安全登录激活消息发送至第二通信设备 20。

[0060] 此外，如果从安全中继服务器 30 接收到登录通知消息，则第一通信设备 10 从登录通知消息中提取网站标识信息，并检查安全策略表中与该网站标识信息对应的安全等级。此外，基于所确定的结果，第一通信设备 10 原封不动地应用检查到的安全等级、或者应用加强的安全等级作为用户的登录安全等级。同时，如果所确定的结果为确定第一通信设备 10 和第二通信设备 20 不位于同一地点，则第一通信设备 10 不向网页服务器 40 或第二通信设备 20 提供认证相关数据，而是可发送向第二通信设备 20 通知无法进行登录的消息。

[0061] 在一实施例中，第一通信设备 10 可对安全数据进行分类和存储，该安全数据针对每个通信设备的标识信息记录了每个网站的登录认证信息。此外，在从第二通信设备 20 获取解密密钥后，第一通信设备 10 可通过使用该解密密钥来对第二通信设备 20 所访问的网站的登录认证消息进行解密，并将解密的登录认证信息发送至网页服务器 40 或第二通信设备 20。

[0062] 在另一实施例中，第一通信设备 10 还可对安全数据 (该安全数据针对每个通信设备的标识信息记录了每个网站的登录认证信息) 进行分类和存储并将第二通信设备 20 所访问的网站的加密的认证信息发送至第二通信设备 20。

[0063] 在另一实施例中，第一通信设备 10 可存储每个通信设备的解密密钥，并将用于对加密的认证信息进行解密的解密密钥发送到第二通信设备 20。

[0064] 在另一实施例中，第一通信设备 10 可以对针对每个通信设备的标识信息的每个网站的认证信息存储地址进行分类和存储。此外，第一通信设备 10 可对要被第二通信设备 20 的用户所访问的网站进行检查，然后将存储该网站的认证信息的认证信息存储地址提供给第二通信设备 20。

[0065] 同时，如果所应用的安全等级高于阈值等级，则第一通信设备 10 可将加强的认证信息发送至网页服务器 40 或第二通信设备 20。

[0066] 第一通信设备 10 为平板计算机、笔记本电脑、移动通信终端、服务器等，并且优选地为智能电话。

[0067] 图 2 为示出了根据本发明一实施例的一种用于在安全登录系统中进行登录认证的方法的流程图。

[0068] 参考图 2，第二通信设备 20 访问被赋予用户所输入的网站地址的网页服务器 40，以及网页服务器 40 将具有登录菜单（其允许输入 ID 和密码）的网页发送至第二通信设备 20(S201)。此时，网页服务器 40 生成访问令牌，并将访问令牌和网站标识信息（例如，网页服务器的站点地址）与网页一起发送至第二通信设备 20。访问令牌是一种其中记录有第二通信设备 20 进行登录所需的安全信息的对象，并且访问令牌具有固有标识信息（例如，安全标识信息）。

[0069] 接下来，第二通信设备 20 将从网页服务器 40 接收的网页显示在屏幕上。此外，第二通信设备 20 的代理 21 在网页的登录菜单的下方输出去激活的安全登录菜单。此时，代理 21 可以通过控制安全登录菜单在网页上以深色或半透明色显示来使安全登录菜单去激活。如果安全登录服务的昵称或 ID 被存储在诸如 cookies 之类的存储区域中，则第二通信设备 20 的代理 21 可将该昵称或 ID 与安全登录菜单一起显示在网页上。

[0070] 图 3 为示出根据本发明实施例，显示安全登录菜单的网页的图。

[0071] 如图 3 所示，除网页中基本提供的登录菜单 31 之外，代理 21 还可将根据本发明的安全登录菜单 32 显示在该网页上。此时，如果 cookies 中保留有安全登录服务的使用记录，则代理 21 可以从 cookies 中检查安全登录服务中所使用的用户的 ID 或昵称，并在安全登录菜单 32 的某个区域中显示该用户的 ID 或昵称。图 3 示出了针对安全登录服务在网页中显示“Nick”作为该用户的昵称连同安全登录菜单 32，并且安全登录菜单 32 以深色显示（即，处于去激活状态）。选择性地，代理 21 可以以工具栏的形式在网页浏览器的菜单树中包括有安全登录菜单 32。

[0072] 接下来，第二通信设备 20 的代理 21 检查出第二通信设备 20 开始浏览网页，通知安全登录服务的发起，并将包含有第二通信设备 20 的用户标识信息和第二通信设备的标识信息的服务通知消息发送至安全中继服务器 30(S203)。此时，代理 21 可将以下各项中任一项记录在服务通知消息中作为用户标识信息：安全登录服务 ID、用户的居民登记号码、互联网个人标识号 (I-PIN)、移动通信电话号码等。此外，代理 21 可以将自身的标识信息（即代理标识信息）、第二通信设备 20 的 IP 地址、MAC 地址等中的任一项记录在服务通知消息中作为所述第二通信设备 20 的标识信息。此外，代理 21 可检查第二通信设备 20 的位置信息并将该位置信息包括在服务通知消息中。例如，代理 21 可通过使用装载在第二通信设备 20 中的 GPS 接收器来获取 GPS 坐标，并将 GPS 坐标或与 GPS 坐标对应的管理地址信息包括在服务通知消息中作为位置信息。此外，如果第二通信设备 20 是其中装载有本地无线通信模块（例如 WiFi 模块）的终端，则代理 21 可以获取可通过该本地无线通信模块访问的邻近的小型无线电基站（例如，接入点）的标识信息，将该小型无线电基站的标识信息发送至位置检查服务器 50，从位置检查服务器 50 接收位置信息，然后将该位置信息包括在服务通知消息中。该代理检查第二通信设备 20 是可用于移动通信的终端还是固定终端，如果第二通信设备 20 是可用于移动通信的终端，则该代理获取位置信息并将该位置信息包括在服务通知消息中。

[0073] 如果这样，安全中继服务器 30 检查服务通知消息中包含的用户标识信息，并且检查与该用户标识信息相映射的第一通信设备 10 的标识信息。此外，安全中继服务器 30 将服务通知消息发送至具有检查到的标识信息的第一通信设备 10(S205)。

[0074] 随后，第一通信设备 10 检查访问网页服务器 40 的第二通信设备 20 的位置信息，

并且还检查第一通信设备 10 的位置信息 (S207)。此时，第一通信设备 10 可从服务通知消息中提取第二通信设备的标识信息，并从存储了与标识信息相映射的位置信息的数据中检查第二通信设备 20 的位置信息。此外，如果服务通知消息包含第二通信设备 20 的位置信息，则第一通信设备 10 可通过从服务通知消息中提取位置信息来检查第二通信设备 20 的位置信息。进一步地，第一通信设备 10 可通过使用装载在其中的 GPS 接收器来获取 GPS 坐标，并基于 GPS 坐标来检查自身的位置。此外，第一通信设备 10 可识别出借助于本地无线通信可用于无线通信的小型无线电基站（例如接入点），将该小型无线电基站的标识信息发送至位置检查服务器 50，并且从位置检查服务器 50 接收位置信息，从而检查第一通信设备 10 的位置信息。

[0075] 接下来，第一通信设备 10 将自身的位置信息与第二通信设备 20 的位置信息相比较，以确定第一通信设备 10 与第二通信设备 20 是否位于同一地点 (S209)。此时，第一通信设备 10 可通过检查第一通信设备 10 与第二通信设备 20 是否位于同一管理区内或第一通信设备 10 与第二通信设备 20 之间的距离是否小于阈值距离（例如，100 米）来确定第一通信设备 10 与第二通信设备 20 是否位于同一地点。进一步地，如果第二通信设备 20 和第一通信设备 10 分别访问小型无线电基站，则第二通信设备 20 可通过检查第一通信设备 10 与第二通信设备是否访问同一小型无线电基站，来确定第一通信设备 10 与第二通信设备 20 是否位于同一地点。

[0076] 如果确定第一通信设备 10 和第二通信设备 20 位于同一地点，则第一通信设备 10 将安全登录激活消息发送至第二通信设备 20(S211)。此时，第一通信设备 10 基于包含在服务通知消息中的第二通信设备的标识信息来识别第二通信设备 20，并将安全登录激活消息发送至第二通信设备 20。

[0077] 如果这样，第二通信设备 20 的代理 21 对去激活的安全登录菜单进行激活，以使得用户认识到第一通信设备 10 与第二通信设备 20 位于同一地点。此时，代理 21 可通过将安全登录菜单的深色改变为亮色、使安全登录菜单闪烁或者向安全登录菜单输出激活图形标记来激活安全登录菜单。

[0078] 接下来，第二通信设备 20 的代理 21 监测安全登录菜单是否被点击，如果安全登录菜单被点击，则第二通信设备 20 的代理 21 生成登录通知消息并将登录通知消息发送至安全中继服务器 (S213,S215)，所述登录通知消息包含待登录的网站的标识信息、用于访问网页服务器 40 的访问令牌、用户标识信息、以及第二通信设备 20 的标识信息。

[0079] 然后，安全中继服务器 30 检查登录通知消息中包含的用户标识信息，以及检查与该用户标识信息相映射的第一通信设备 10 的标识信息。此外，安全中继服务器 30 将登录通知消息发送至具有检查到的标识信息的第一通信设备 10(S217)。

[0080] 接下来，第一通信设备 10 从接收自安全中继服务器 30 的登录通知消息中提取用户标识信息、网站标识信息、访问令牌以及第二通信设备 20 的标识信息。随后，第一通信设备 10 从安全策略表中检查与提取的网站标识信息相映射的安全等级 (S219)。

[0081] 接下来，第一通信设备 10 检查步骤 S209 中所进行的确定的结果，并且基于确定结果来应用检查到的安全等级或加强的安全等级 (S211)。换言之，如果确定第一通信设备 10 与第二通信设备 20 位于同一地点，则第一通信设备 10 原封不动地应用检查到的安全等级。同时，如果检查出第一通信设备 10 与第二通信设备 20 不位于同一地点，则第一通信设备

10 不原封不动地应用检查到的安全等级，而是应用高于检查到的安全等级的加强的安全等级。此时，如果步骤 S219 中检查到的安全等级为最高等级（即，第三等级），则第一通信设备 10 可原封不动地应用该安全等级，即第三等级。

[0082] 随后，第一通信设备 10 基于所应用的安全等级来获取为认证相关数据之一的登录认证信息（即，ID 和密码）(S223)。详细地，如果安全等级为第一等级（最低等级），则第一通信设备 10 通过向第二通信设备 20 请求解密密钥并且从第二通信设备 20 接收解密密钥来得到该安全等级中所用的解密密钥。此外，第一通信设备 10 基于第二通信设备的标识信息，在针对每个通信设备进行分类的安全数据中检查专用于第二通信设备的安全数据，并且从包含在检查到的安全数据中的登录认证消息中提取与网站标识信息相映射的加密的登录认证信息（即，ID 和密码）。随后，第一通信设备 10 通过使用解密密钥来解密提取的登录认证信息，从而获取登录认证信息。

[0083] 此外，如果安全等级为第二等级，则第一通信设备 10 通知第二通信设备 20 试图登录网站，并输出通知窗口以询问是否批准登录。此处，仅当用户通过通知窗口输入批准信号时，第一通信设备 10 才向第二通信设备 20 请求解密密钥，并从第二通信设备 20 接收解密密钥，然后通过使用解密密钥从专用于第二通信设备的安全数据中提取并解密与网站标识信息相映射的加密的登录认证信息。

[0084] 同时，如果安全等级为第三等级（最高等级），则第一通信设备 10 通过从用户处接收诸如生物信息（例如指纹信息、虹膜信息等）或 OTP 之类的加强的认证信息来获取认证信息。此时，与安全等级为第一等级的情况类似，第一通信设备 10 从第二通信设备 20 获取解密密钥，通过使用解密密钥来解密网站的登录认证信息，并且从用户处获取所有的解密的登录认证信息和加强的登录认证信息。

[0085] 在其它情况下，如果安全等级为第三等级，则第一通信设备 10 可输出用于输入其认证信息的输入窗口，并且通过该输入窗口从用户接收用户认证信息，比如密码、生物信息（例如，指纹信息、虹膜信息等）、居民登记号码等。在这一情况下，如果用户所输入的用户认证信息与第一通信设备 10 中存储的用户认证信息相同，则第一通信设备 10 可通过从用户接收加强的认证信息或从第二通信设备 20 接收解密密钥来解密网站的登录认证信息，或者可接收加强的认证信息并且也解密登录认证信息。换言之，如果安全等级为第三等级，则第一通信设备 10 进行用户认证，如果用户认证成功，则第一通信设备 10 获取认证相关数据。

[0086] 接下来，第一通信设备 10 检查从登录通知消息中提取的网站标识信息和访问令牌，并将获取的登录认证信息和加强的登录认证信息至少之一发送至被赋予网站认证信息的网页服务器 40(S225)。此时，第一通信设备 10 将访问令牌连同相应的认证信息一起发送至网页服务器 40。

[0087] 然后，网页服务器 40 基于从第一通信设备 10 接收的访问令牌识别出试图登录的第二通信设备 20，并检查认证信息是否准确，从而进行对第二通信设备 20 的登录认证(S227)。此时，如果 ID 和密码被记录在认证信息中，则网页服务器 40 通过检查 ID 和密码是否准确来对第二通信设备 20 进行登录认证。此外，如果诸如用户的生物信息或 OTP 等之类的加强的认证信息被包括在认证信息中，则网页服务器 40 通过检查认证信息是否与已经存储在其中的用户的加强的认证信息相同来附加地对第二通信设备 20 进行登录认证。换

言之，在从第一通信设备 10 接收到登录认证信息和加强的认证信息的情况下，网页服务器 40 首先基于包含在认证信息中的 ID 和密码来认证第二通信设备 20 的用户，然后基于加强的认证信息来认证第二通信设备 20 的用户。

[0088] 接下来，如果登录认证失败，则网页服务器 40 将此视为第二通信设备 20 的登录失败，但是如果登录认证成功，则网页服务器 40 将认证成功消息发送到第二通信设备 20(S229)，然后提供第二通信设备 20 所请求的在线服务。如果登录认证成功，则网页服务器 40 向第一通信设备 10 通知第二通信设备 20 成功地进行了登录。

[0089] 同时，如果安全等级被应用为第三等级，则第一通信设备 10 可仅将加强的认证信息发送至网页服务器 40，而不发送登录认证信息。在这一情况下，网页服务器 40 基于加强的认证信息来认证第二通信设备 20。

[0090] 此外，第一通信设备 10 可将解密的登录认证信息和加强的认证信息至少之一发送至第二通信设备 20。在这一情况下，第二通信设备 20 通过将从第一通信设备 10 接收的认证信息发送至网页服务器 40 来进行登录认证。

[0091] 下文中，在参考图 4 至图 6 的描述中，以与图 2 中的附图标记相同的附图标记表示的每个步骤 (S201 至 S221) 与图 2 中的步骤基本相同，因此在此不再详述。

[0092] 图 4 为示出了根据本发明另一实施例的一种用于在安全登录系统中进行登录认证的方法的流程图。

[0093] 参考图 4，第一通信设备 10 应用安全等级，然后基于该安全等级获得用户的登录认证信息 (S423)。详细地，如果安全等级为第一等级（最低等级），则第一通信设备 10 基于第二通信设备的标识信息从针对每个通信设备进行分类的安全数据中检查专用于第二通信设备的安全数据，并且从包含在检查到的安全数据中的登录认证消息中提取与网站标识信息相映射的加密的登录认证信息。此外，如果安全等级为第二等级，则第一通信设备 10 通知第二通信设备 20 试图登录网站，并输出通知窗口以询问是否批准登录。此处，仅当用户通过通知窗口输入批准信号时，第一通信设备 10 才从专用于第二通信设备的安全数据中提取与网站相映射的加密的登录认证信息。

[0094] 同时，如果安全等级为第三等级（最高等级），则第一通信设备 10 从用户处接收诸如生物信息、OTP 等之类的加强的认证信息，从而获取加强的认证信息。此时，与安全等级为第一等级的情况类似，第一通信设备 10 从专用于第二通信设备的安全数据中附加地提取与网站相映射的加密的登录认证信息。

[0095] 在其它情况下，如果安全等级为第三等级，则第一通信设备 10 可输出用于输入用户认证信息的输入窗口，并且通过该输入窗口从用户接收用户认证信息，比如密码、生物信息（例如，指纹信息、虹膜信息等）、居民登记号码等。此外，如果用户所输入的用户认证信息与第一通信设备 10 中存储的用户认证信息相同，则第一通信设备 10 可接收用户所输入的加强的认证信息或者提取加密的登录认证信息，或者获取两者（即，加强的认证信息和加密的登录认证信息）。换言之，如果安全等级为第三等级，则第一通信设备 10 进行用户认证，如果用户认证成功，则第一通信设备 10 获取认证相关数据。

[0096] 接下来，第一通信设备 10 可将获取的加密的登录认证信息和加强的认证信息至少之一发送至第二通信设备 20(S425)。第一通信设备 10 通过使用预定的加密密钥来加密加强的认证信息，并将加密的加强认证信息发送至第二通信设备 20，以使得可使用第二通

信设备 20 中存储的解密密钥对加密的加强认证信息正常地进行解密。

[0097] 然后，第二通信设备 20 通过使用其中存储的解密密钥来对从第一通信设备 10 接收的加密的登录认证信息进行解密 (S427)，并将解密的登录认证信息发送至网页服务器 40 以请求登录认证 (S429)。此时，在从第一通信设备 10 接收到加强的认证信息的情况下，第二通信设备 20 通过使用其中存储的解密密钥来解密加强的认证信息，并附加地将解密的加强认证信息发送至网页服务器 40。

[0098] 接下来，网页服务器 40 通过检查从第二通信设备 20 接收的认证信息是否准确来对第二通信设备 20 进行登录认证 (S431)。此时，如果 ID 和密码被记录在认证信息中，则网页服务器 40 检查 ID 和密码是否准确以对第二通信设备 20 进行登录认证。此外，如果诸如生物信息或 OTP 等之类的加强的认证信息被包括在认证信息中，则网页服务器 40 可通过检查认证信息是否与已经存储在其中的用户的加强的认证信息相同，来附加地对第二通信设备 20 进行登录认证。

[0099] 接下来，如果登录认证失败，则网页服务器 40 将此视为第二通信设备 20 的登录失败，但是如果登录认证成功，则网页服务器 40 将认证成功消息发送到第二通信设备 20(S433)，然后提供第二通信设备 20 所请求的在线服务。

[0100] 同时，如果安全等级被应用为第三等级，则第一通信设备 10 可仅将加强的认证信息发送至第二通信设备 20，而不发送登录认证信息。在这一情况下，第二通信设备 20 解密加强的认证信息，并将加强的认证信息而不是登录认证信息发送至网页服务器 40 以进行针对网页服务的认证。

[0101] 图 5 为示出了根据本发明另一实施例的一种用于在安全登录系统中进行登录认证的方法的流程图。

[0102] 在图 5 所描绘的实施例中，第一通信设备 10 存储针对每个通信设备进行分类的解密密钥，并且第二通信设备 20 存储每个网站的加密的登录认证信息。

[0103] 参考图 5，如果应用了安全等级，则第一通信设备 10 基于所应用的安全等级进行提取解密密钥（其为认证相关数据之一）的处理 (S523)。详细地，如果安全等级为第一等级（最低等级），则第一通信设备 10 从针对每个用户进行分类的解密密钥中提取与包含在登录通知消息中的第二通信设备的标识信息对应的解密密钥。此外，如果安全等级为第二等级，则第一通信设备 10 通知第二通信设备 20 试图登录网站，并输出通知窗口以询问是否批准登录。此处，仅当用户通过通知窗口输入批准信号时，第一通信设备 10 才提取与第二通信设备的标识信息对应的解密密钥。

[0104] 同时，如果安全等级为第三等级（最高等级），则第一通信设备 10 提取与第二通信设备的标识信息对应的解密密钥，并从用户处接收诸如生物信息、OTP 等之类的加强的认证信息，从而获取加强的认证信息 (S525)。在其它情况下，如果安全等级为第三等级，则第一通信设备 10 输出用于输入用户认证信息的输入窗口，并通过输入窗口从用户接收用户的用户认证信息。此处，在认证用户认证信息是否准确之后，第一通信设备 10 可选择性地得到认证相关数据。换言之，如果安全等级为第三等级，则第一通信设备 10 认证用户所输入的用户认证信息是否准确，然后如果认证成功，则第一通信设备 10 可从用户接收加强的认证信息或提取解密密钥，或者获取两者（即，加强的认证信息和解密密钥）。在参考图 5 的描述中，要解释的是，第一通信设备 10 应用第三等级作为安全等级并附加地获取加强的认

证信息。

[0105] 接下来，第一通信设备 10 将提取的解密密钥和加强的认证信息发送至第二通信设备 20(S527)。第一通信设备 10 通过使用预定的加密密钥来加密加强的认证信息，并将加密的加强认证信息发送至第二通信设备 20，以使得可使用第二通信设备 20 中存储的解密密钥对加强的认证信息正常地进行解密。

[0106] 随后，第二通信设备 20 从其中存储的每个站点的加密的登录认证信息中提取与当前访问的网站的标识信息相映射的解密的登录认证信息 (S529)。随后，第二通信设备 20 通过使用从第一通信设备 10 接收的解密密钥来解密提取的登录认证信息。此外，第二通信设备 20 通过使用其中存储的解密密钥来对从第一通信设备 10 接收的加强的认证信息进行解密。

[0107] 接下来，第二通信设备 20 将解密的登录认证信息和加强的认证信息发送至网页服务器 40 以请求登录认证 (S533)。

[0108] 接下来，网页服务器 40 通过检查从第二通信设备 20 接收的登录认证信息和加强的认证信息两者是否准确来对第二通信设备 20 进行登录认证 (S535)。接下来，如果登录认证失败，则网页服务器 40 将此视为第二通信设备 20 的登录失败，但是如果登录认证成功，则网页服务器 40 将认证成功消息发送到第二通信设备 20(S537)，然后提供第二通信设备 20 所请求的在线服务。

[0109] 同时，如果安全等级被应用为第一等级或第三等级，则第一通信设备 10 可仅将解密密钥发送至第二通信设备 20 而不发送加强的认证信息，并且第二通信设备 20 通过使用解密密钥来对步骤 S529 中提取的登录认证信息进行解密并将解密的登录认证信息发送至网页服务器 40。换言之，如果在第一通信设备 10 中安全等级被应用为第一等级或第二等级，则第二通信设备 20 仅将登录认证信息发送至网页服务器 40 而不发送加强的认证信息，并且网页服务器 40 基于登录认证信息对第二通信设备 20 进行登录认证。

[0110] 此外，如果安全等级被应用为第三等级，则第一通信设备 10 可仅将加强的认证信息发送至第二通信设备 20。在这一情况下，第二通信设备 20 解密加强的认证信息，并将加强的认证信息而不是登录认证信息发送至网页服务器 40。如果这样，网页服务器 40 基于加强的认证信息来对第二通信设备 20 进行登录认证。

[0111] 图 6 为示出了根据本发明另一实施例的一种用于在安全登录系统中进行登录认证的方法的流程图。

[0112] 在图 6 所描绘的实施例中，第一通信设备 10 针对每个通信设备的标识信息对每个网站的加密的认证信息存储地址进行分类和存储。

[0113] 参考图 6，如果应用了安全等级，则第一通信设备 10 基于所应用的安全等级执行提取认证信息存储地址（其为认证相关数据之一）的过程 (S623)。详细地，如果安全等级为第一等级（最低等级），则第一通信设备 10 基于包括在登录通知消息中的第二通信设备的标识信息来检查专用于试图登录的第二通信设备的存储地址数据，并从存储地址数据中提取与包含在登录通知消息中的站点标识信息相映射的加密的认证信息存储地址。此外，如果安全等级为第二等级，则第一通信设备 10 通知第二通信设备 20 试图登录网站，并输出通知窗口以询问是否批准登录。此处，仅当用户通过通知窗口输入批准信号时，第一通信设备 10 才从专用于第二通信设备的存储地址数据中提取与网站标识信息相映射的加密的认

证信息存储地址。

[0114] 同时，如果安全等级为第三等级（最高等级），则第一通信设备 10 从专用于第二通信设备的存储地址数据中提取与站点标识信息相映射的加密的认证信息存储地址，并从用户处接收诸如生物信息、OTP 等之类的加强的登录认证信息，从而获取加强的认证信息 (S625)。

[0115] 在其它情况下，如果安全等级为第三等级，则第一通信设备 10 可输出用于输入用户认证信息的输入窗口，并通过输入窗口从用户接收用户认证信息。此外，在认证用户认证信息准确之后，第一通信设备 10 可选择性地接收认证相关数据。换言之，如果安全等级为第三等级，则第一通信设备 10 认证用户认证信息是否准确，如果认证成功，则第一通信设备 10 可从用户接收加强的认证信息或提取认证信息存储地址，或者获取两者（即，加强的认证信息和认证信息存储地址）。在图 6 中，示出了第一通信设备 10 应用第三等级作为安全等级并附加地获取加强的认证信息。

[0116] 接下来，第一通信设备 10 将提取的加密的认证信息存储地址和加强的认证信息发送至第二通信设备 20(S627)。此时，第一通信设备 10 通过使用预定的加密密钥来加密加强的认证信息，并将加密的加强认证信息发送至第二通信设备 20，以使得可通过第二通信设备 20 中存储的解密密钥对加密的加强认证信息正常地进行解密。

[0117] 随后，第二通信设备 20 通过使用其中存储的解密密钥来解密加密的认证信息存储地址。此外，第二通信设备 20 将包含存储地址的认证信息请求消息发送至认证信息存储服务器 60(S629)。

[0118] 如果这样，认证信息存储服务器 60 检查认证信息请求消息中的认证信息存储地址，提取存储地址处存储的加密的认证信息，并且将加密的认证信息发送至第二通信设备 20(S631)。

[0119] 随后，第二通信设备 20 通过使用其中存储的解密密钥来解密加密的认证信息，并且还对从第一通信设备 10 接收的加强的认证信息进行解密 (S633)。接下来，第二通信设备 20 将解密的登录认证信息和加强的认证信息发送至网页服务器 40 以请求登录认证 (S635)。

[0120] 如果这样，网页服务器 40 通过检查从第二通信设备 20 接收的登录认证信息和加强的认证信息两者是否准确，来对第二通信设备 20 进行登录认证 (S637)。接下来，如果登录认证失败，则网页服务器 40 将此视为第二通信设备 20 的登录失败，但是如果登录认证成功，则网页服务器 40 将认证成功消息发送到第二通信设备 20(S639)，然后提供第二通信设备 20 所请求的在线服务。

[0121] 同时，如果安全等级被应用为第一等级或第二等级，则第一通信设备 10 仅将认证信息存储地址发送至第二通信设备 20，并且第二通信设备 20 通过基于认证信息存储地址从认证信息存储服务器 60 接收登录认证信息并解密该登录认证信息来对网页服务器 40 进行登录认证。换言之，如果安全等级被应用为第一等级或第二等级，则第二通信设备 20 通过仅使用登录认证信息而不使用加强的认证信息来进行登录认证。

[0122] 此外，如果安全等级被应用为第三等级，则第一通信设备 10 可仅将加强的认证信息发送至第二通信设备 20。在这一情况下，第二通信设备 20 解密加强的认证信息，并将加强的认证信息而不是登录认证信息发送至网页服务器 40。如果这样，网页服务器 40 基于加

强的认证信息来对第二通信设备 20 进行登录认证。

[0123] 在另一实施例中，如果安全等级被应用为第三等级，则第一通信设备 10 可提取加强的认证信息的存储地址，并将存储地址发送至第二通信设备 20。在这一情况下，第二通信设备 20 将记录加强的认证信息的存储地址的认证信息请求消息发送至认证信息存储服务器 60，并且认证信息存储服务器 60 提取记录存储地址的加强的认证信息，并将加强的认证信息发送至第二通信设备 20。此外，第二通信设备 20 对接收的加强的认证信息进行解密，然后对网页服务器 40 进行登录认证。

[0124] 同时，在以上实施例中，如果确定第一通信设备 10 与第二通信设备 20 不位于同一地点，则第一通信设备 10 可能无法将与认证有关的任何数据（例如，登录认证信息、解密密钥、认证信息存储地址、加强的认证信息等）提供给网页服务器 40 或第二通信设备 20，并且提供，通知对第二通信设备 20 而言登陆不可用的消息。详细地，如果确定第一通信设备 10 和第二通信设备 20 位于同一地点，则第一通信设备 10 检查安全登录通知消息中包含的站点标识信息，并原封不动地应用与站点标识信息相映射的安全等级。此外，第一通信设备 10 根据所应用的安全等级来执行获取认证相关数据的过程，并将获得的认证相关数据（即，登录认证信息、解密密钥、认证信息存储地址以及加强的认证信息）提供给第二通信设备 20 或网页服务器 40。同时，如果确定出第一通信设备 10 和第二通信设备 20 不位于同一地点，则第一通信设备 10 不提供认证相关数据而是发送通知对第二通信设备 20 而言登陆不可用的消息。

[0125] 图 7 为示出了根据本发明实施例的一种用于将已经登录安全登录系统的通信设备强制登出的方法的流程图。

[0126] 参考图 7，如果第二通信设备 20 成功登录到网站，则第一通信设备 10 持续地监测第二通信设备 20 的位置信息 (S701)。换言之，如果从网页服务器 40 通知了第二通信设备 20 的登录成功，则第一通信设备 10 持续地监测第二通信设备 20 的位置信息。如果第二通信设备 20 是允许移动通信的通信终端，则第一通信设备 10 可持续地从第二通信设备 20 接收位置信息，并监测第二通信设备 20 的位置信息。

[0127] 接下来，第一通信设备 10 基于监测到的位置信息来确定第一通信设备 10 与第二通信设备 20 是否位于同一地点 (S703)，然后如果确定第一通信设备 10 与第二通信设备 20 位于同一地点，则第一通信设备 10 再次执行步骤 S701。此时，第一通信设备 10 可通过检查第一通信设备 10 与第二通信设备 20 是否位于同一管理区内或第一通信设备 10 与第二通信设备 20 之间的距离是否小于阈值距离（例如，100 米）来确定第一通信设备 10 与第二通信设备 20 是否位于同一地点。

[0128] 同时，如果步骤 S703 的确定结果为确定第一通信设备 10 与第二通信设备 20 不位于同一地点，则第一通信设备 10 将登出请求消息发送至网页服务器 40(S705)。此时，第一通信设备 10 将从登录通知消息中提取的访问令牌包括在登出请求消息中。

[0129] 如果这样，网页服务器基于包含在登出请求消息中的访问令牌来识别出成功登录的第二通信设备 20，并对第二通信设备 20 进行强制登出 (S707)。随后，网页服务器 40 将通知登出的消息发送至第二通信设备 20(S709)，并且还向第一通信设备 10 通知第二通信设备 20 已登出。

[0130] 图 8 是示出根据本发明实施例的认证数据提供设备的图。

[0131] 图 8 中所描绘的认证数据提供设备 100 执行图 1 至图 7 中示出的第一通信设备 10 的操作。

[0132] 如图 8 所示，根据本发明实施例的认证数据提供设备 100 包括存储器 110、存储器控制器 121、至少一个处理器 (CPU)122、外围接口 123、输入 / 输出 (I/O) 子系统 130、显示设备 141、输入设备 142、通信电路 150 以及 GPS 接收器 160。这些部件通过至少一根通信总线或信号线进行通信。图 8 中所描绘的各个部件可被实施为硬件、软件、硬件和软件的结合，包括至少一个信号处理和 / 或专用集成电路。

[0133] 存储器 110 可包括高速随机访问存储器并且还可包括至少一个磁盘储存设备、诸如闪存之类的非易失性存储器或者另一非易失性半导体存储设备。在某些实施例中，存储器 110 还可包括位置与至少一个存储器 122 相距较远的存储器，例如通过通信网络接入通信电路 150 的网络附着存储设备，所述通信网络选自以下各项组成的组 :互联网、内联网、局域网 (LAN)、无线局域网 (WLAN)、存储区域网络 (SAN) 或者其结合。认证信息提供设备 100 的其它部件 (比如处理器 122 和外围接口 123) 对存储器 110 的访问可受到存储器控制器 121 的控制。

[0134] 外围接口 123 将输入 / 输出外围设备连接至处理器 122 和存储器 110。至少一个处理器 122 执行存储器 110 中存储的软件程序和 / 或一组指令以实现认证数据提供设备 100 的各种功能并处理数据。

[0135] 在某些实施例中，外围接口 123、处理器 122 以及存储器控制器 121 可在诸如芯片 120 的单个芯片上实施。在某些其它实施例中，他们可被是实施为单独的芯片。

[0136] I/O 子系统 130 给出了外围接口 123 与认证数据提供设备 100 的外围输入 / 输出设备 (比如显示设备 141 和输入设备 142) 之间的接口。

[0137] 显示设备 141 可使用液晶显示器 (LCD) 或发光聚合物显示器 (LPD)，并且这一显示设备 141 可以是电容型、电阻型或红外型的触摸显示器。触摸显示器在输入接口与设备和用户之间提供输出界面。触摸显示器向用户显示可视输出。可视输出可包括文字、图形、视频及其组合。可视输出可部分或全部对应于用户界面目标。触摸显示器形成了用于接收用户输入的触摸感测表面。

[0138] 输入设备 142 是诸如按键、键盘等的输入装置并且接收用户的输入信号。

[0139] 处理器 122 被配置为执行与认证数据提供设备 100 相关联的操作和指令。例如，处理器 122 可通过使用从存储器 110 搜索到的指令来对认证数据提供设备 100 的部件之间的输入和输出数据的接收和操控加以控制。

[0140] 通信电路 150 通过天线发送或接收无线电波或者通过电缆发送或接收数据。通信电路 150 将电信号转换为电波或者将电波转化为电信号，并可借助于电波与通信网络、另一移动网关或通信设备进行通信。通信电路 150 包括例如天线系统、RF 收发器、至少一个放大器、调谐器、至少一个振荡器、数字信号处理器、CODEC 芯片组、用户识别模块 (SIM) 卡、存储器等，但是也可包括用于执行这些功能的任何已知电路，而不限于以上所述。通信电路 150 可借助于被称为万维网 (WWW) 的互联网、内两网、和 / 或移动通信网络、无线 LAN、城域网 (MAN) 和 / 或本地无线通信来与其它设备通信。无线通信包括全球移动通信系统 (GSM)、增强型数据 GSM 环境 (EDGE)、宽带码分多址 (WCDMA)、码分多址 (CDMA)、时分多址 (TDMA)、网络电话 (VoIP)、蓝牙、zigbee、近场通信 (NFC) 或其它合适的通信协议，包括在本申请的

递交日尚未开发出的通信协议，并且可在不限于以上所述的情况下使用各种通信标准、协议和技术。

[0141] GPS（全球定位系统）接收器 160 接收多个人造卫星发射的卫星信号。GPS 接收器 160 可采用 C/A 码伪距离 (C/A-code pseudo-range) 接收器、C/A 码载波接收器、P 码接收器、Y 码接收器等。

[0142] 诸如操作系统 111、图形模块（一组指令）112 和安全登录程序（一组指令）113 的软件部件被装载（安装）在存储器 110 中。

[0143] 操作系统 111 可以是内置操作系统，比如 Darwin、RTXC、LINUX、UNIX、OS X、WINDOWS、VxWorks、Tizen、IOS 或 Android。操作系统 111 包括各种软件部件和 / 或用于控制和管理一般系统任务（例如，存储器管理、存储设备控制、电源管理等）的设备，并促进各个硬件和软件部件之间的通信。

[0144] 图形模块 112 包括用于在显示设备 141 上提供和显示图形的各种已知软件部件。在不进行限制的情况下，术语“图形”包括文字、网页、图标、数字图像、视频、动画等，并且还包括可显示给用户的所有对象。

[0145] 如果第二通信设备 20 试图登录网页服务器 40，则安全登录程序 113 获取认证相关数据并将认证相关数据提供给网页服务器 40 或第二通信设备 20。如果安全登录应用被安装，则安全登录程序 113 被装载到存储器 110 中。

[0146] 图 9 是示出根据本发明实施例的安全登录程序的图。

[0147] 如图 9 所示，根据本发明实施例的安全登录程序 113 包括数据存储模块 91、安全策略应用模块 92、位置检查模块 93、认证数据获取模块 94 以及认证数据提供模块 95。

[0148] 数据存储模块 91 存储其中记录有每个网站的安全等级的安全策略表，即安全策略表，在该表中，网站标识信息与安全等级相映射。在另一实施例中，数据存储模块 91 可对安全数据进行分类和存储，安全数据针对每个通信设备的标识信息记录了每个网站的登录认证信息（即 ID 和密码）。登录认证信息被加密并存储在数据存储模块 91 中，并基于存储在第二通信设备 20 中的解密密钥被正常解密。在另一实施例中，数据存储模块 91 可针对每个通信设备的标识信息对至少一个解密密钥进行分类和存储。在另一实施例中，数据存储模块 91 可针对每个通信设备的标识信息对安全地址数据进行分类和存储，安全地址数据记录了每个网站的认证信息存储地址。同时，数据存储模块 91 可存储每个第二通信设备 20 的位置信息并且还可包括诸如密码、生物信息、居民注册号码等之类的用户认证信息。

[0149] 如果第二通信设备 20 试图登录网页服务器 40，则安全策略应用模块 92 运作以针对提供给网页服务器 40 的第二通信设备 20 的登录认证信息确定并应用安全等级。详细地，如果安全策略应用模块 92 通过通信电路 150 从安全中继服务器 30 接收到登录通知消息，则安全策略应用模块 92 从登录通知消息中提取第二通信设备的标识信息、网站标识信息和访问令牌，并检查安全测量表中与网站标识信息相映射的安全等级。

[0150] 此外，安全策略应用模块 92 通过使用位置检查模块 93 来检查认证数据提供设备 100 和第二通信设备 20 的位置。此处，如果认证数据提供设备 100 与第二通信设备 20 位于同一地点，则检查到的安全等级可被原封不动地应用，而如果认证数据提供设备 100 与第二通信设备 20 不位于同一地点，则可以应用比检查到的安全等级高的加强的安全等级作为登录认证信息的安全等级。

[0151] 位置检查模块93确定认证数据提供设备100与第二通信设备20是否位于同一地点。此时，位置检查模块93可通过检查第二通信设备20与认证数据提供设备100是否位于同一管理区内或认证数据提供设备100与第二通信设备20之间的距离是否小于阈值距离（例如，100米），来确定第二通信设备20与认证数据提供设备100是否位于同一地点。此外，位置检查模块93还可通过检查认证数据提供设备100是否能够借助于通信电路150与第二通信设备20进行本地无线通信（例如，蓝牙通信），来确定第二通信设备20与认证数据提供设备100是否位于同一地点。

[0152] 位置检查模块93可通过从接收自安全中继服务器30的服务通知消息中提取第二通信设备的标识信息，并检查数据存储模块91中与第二通信设备的标识信息相映射的位置信息来检查第二通信设备20的位置信息。此外，如果从安全中继服务器30接收的服务通知消息包含第二通信设备20的位置信息，则位置检查模块93可通过从服务通知消息中提取位置信息来检查第二通信设备20的位置信息。进一步地，位置检查模块93通过使用GPS接收器160来获取GPS坐标，并基于GPS坐标来检查认证数据提供设备100的位置。此外，位置检查模块93可通过经由通信电路150识别允许本地无线通信的小型无线电基站、将小型无线电基站的标识信息发送至位置检查服务器50、然后从位置检查服务器50接收映射有小型无线电基站的标识信息的位置信息，来检查认证数据提供设备100的位置信息。

[0153] 如果确定第二通信设备20和认证数据提供设备100位于同一地点，则位置检查模块93将安全登录激活消息发送至第二通信设备20。

[0154] 同时，如果第二通信设备20成功登录到网页服务器40，则位置检查模块93持续地监测第二通信设备20和认证数据提供设备100的位置，并且如果认证数据提供设备100与第二通信设备20不位于同一地点，则位置检查模块93将登出请求消息发送至网页服务器40。

[0155] 认证数据获取模块94检查安全策略应用模块92所应用的安全等级，然后根据安全等级来执行用于获取认证相关数据的过程。

[0156] 认证数据获取模块94可通过基于包括在登录通知消息中的第二通信设备的标识信息，从数据存储模块91中的多个安全数据中检查出专用于第二通信设备的安全数据，并从安全数据中提取与网站标识信息相映射的加密的登录认证信息（即ID和密码）来获取认证相关数据。此时，认证数据获取模块94可通过使用从第二通信设备20接收的解密密钥来解密提取的登录认证信息。

[0157] 在另一实施例中，认证数据获取模块94可通过基于包含在登录通知消息中的第二通信设备的标识信息，从数据存储模块91中提取与第二通信设备20的标识信息对应的解密密钥，来获取认证相关数据。

[0158] 在另一实施例中，认证数据获取模块94可通过基于包括在登录通知消息中的第二通信设备的标识信息，从数据存储模块91中检查出专用于第二通信设备的存储地址数据，并从存储地址数据中提取与网站标识信息相映射的加密的认证信息存储地址来获取认证相关数据。

[0159] 认证数据获取模块94基于安全中继应用模块92所应用的安全等级来执行获取认证相关数据的过程。换言之，如果安全中继应用模块92所应用的安全等级为第一等级，则认证数据获取模块94立即获取认证相关数据（即，登录认证信息、解密密钥或认证信息存

储地址）。如果安全策略应用模块 92 所应用的安全等级为第二等级，则认证数据获取模块 94 通知第二通信设备 20 正试图登录网站，并向显示设备 141 输出通知窗口以询问是否批准登录。此处，仅当用户输入批准信号时，认证数据获取模块 94 才执行获取认证相关数据的过程。

[0160] 同时，如果安全策略应用模块 92 所应用的安全等级为第三等级，则认证数据获取模块 94 向显示设备 141 输出输入窗口以请求输入加强的认证信息，并获取诸如通过输入窗口输入的生物信息或 OTP 之类的加强的认证信息作为认证相关数据。此外，如果安全策略应用模块 92 所应用的安全等级为第三等级，则认证数据获取模块 94 向显示器 141 输出输入窗口，以使得用户能够输入用户认证数据。此处，如果通过认证输入窗口输入的用户认证信息是准确的，则认证数据获取模块 94 执行获取认证相关数据的过程，而如果用户认证信息不准确，则认证数据获取模块 94 不执行获取认证相关数据的过程。换言之，如果安全等级为第三等级，则认证数据获取模块 9494 进行用户认证，并且如果用户认证成功，则可获取认证相关数据。

[0161] 认证数据提供模块 95 将认证数据获取模块 94 获取的认证相关数据提供给网页服务器 40 或第二通信设备 20。当认证数据提供模块 95 将认证相关数据提供给网页服务器 40 时，认证数据提供模块 95 检查登录通知消息中的网页标识信息和访问令牌，并将认证相关数据连同访问令牌一起发送至被赋予网站标识信息的网页服务器 40。

[0162] 图 10 为示出根据本发明实施例的一种用于在认证数据提供设备中提供认证相关数据的方法的流程图。

[0163] 参考图 10，当第二通信设备 20 试图登录网页服务器 40 时，通信电路 150 从安全中继服务器 30 接收通知第二通信设备 20 正试图登录网页服务器 40 的登录通知消息 (S1001)。

[0164] 如果这样，安全策略应用模块 92 通过从登录通知消息中提取第二通信设备的标识信息、网站标识信息和访问令牌，并从数据存储模块 91 的安全策略表中检查与网站标识信息相映射的安全等级，来检查第二通信设备 20 所访问的网站的安全等级 (S1003)。接下来，安全策略应用模块 92 请求确定认证数据提供设备 100 与第二通信设备 20 是否位于同一地点。

[0165] 如果这样，位置检查模块 93 通过分别检查认证数据提供设备 100 和第二通信设备 20 的位置信息，并将认证数据提供设备 100 和第二通信设备 20 的位置信息相比较，来确定第二通信设备 20 与认证数据提供设备 100 是否位于同一位置 (S1005)。此时，位置检查模块 93 可通过检查第二通信设备 20 与认证数据提供设备 100 是否位于同一管理区内或认证数据提供设备 100 与第二通信设备 20 之间的距离是否小于阈值距离（例如，100 米），来确定第二通信设备 20 与认证数据提供设备 100 是否位于同一地点。

[0166] 此外，位置检查模块 93 还可通过检查认证数据提供设备 100 是否能够借助于通信电路 150 与第二通信设备 20 进行本地无线通信（例如，蓝牙通信），来确定第二通信设备 20 与认证数据提供设备 100 是否位于同一地点。

[0167] 同时，位置检查模块 93 可通过从接收自安全中继服务器 30 的服务通知消息中提取第二通信设备的标识信息并检查数据存储模块 91 中与该标识信息相映射的位置信息，来预先检查第二通信设备 20 的位置信息。此外，如果服务通知消息包括第二通信设备 20

的位置信息，则位置检查模块 93 可通过从服务通知消息中提取位置信息来检查第二通信设备 20 的位置信息。进一步地，位置检查模块 93 通过使用 GPS 接收器 160 来获取 GPS 坐标，并基于 GPS 坐标来检查认证数据提供设备 100 的位置。此外，位置检查模块 93 可通过经由通信电路 150 识别允许本地无线通信的小型无线电基站，将小型无线电基站的标识信息发送至位置检查服务器 50，然后从位置检查服务器 50 接收与小型无线电基站的标识信息相映射的位置信息，来检查认证数据提供设备 100 的位置信息。

[0168] 如果安全策略应用模块 92 从位置检查模块 93 接收到确定结果，则安全策略应用模块 92 基于确定结果来检查认证数据提供设备 100 与第二通信设备 20 是否位于同一地点 (S1007)。

[0169] 然后，如果认证数据提供设备 100 与第二通信设备 20 位于同一地点，则安全策略应用模块 92 应用步骤 S1003 中检查出的站点安全等级作为登录认证信息的安全等级 (S1009)。

[0170] 同时，如果检查出第二通信设备 20 与认证数据提供设备 100 不位于同一地点，则安全策略应用模块 92 应用比步骤 S1003 中检查出的安全等级高一个等级的加强的安全等级，作为登录认证信息的安全等级 (S1011)。此时，如果步骤 S1003 中检查出的安全等级为最高等级（即，如果不存在更高的安全等级），则安全策略应用模块 92 可原封不动地应用步骤 S1003 的安全等级，或者通过通信电路 150 向第二通信设备 20 发送消息以通知无法进行登录而不再进行提供认证相关数据的过程。同时，如果检查出第二通信设备与认证数据提供设备 100 不位于同一地点，则安全策略应用模块 92 不再进行提供认证相关数据的过程，但是可通过通信电路 150 向第二通信设备 20 发送消息以通知无法进行登录。

[0171] 接下来，认证数据获取模块 94 检查安全策略应用模块 92 所应用的安全等级 (S1013)。

[0172] 随后，如果检查出安全等级为第一等级 (S1015)，则认证数据获取模块 94 进行获取认证相关数据的过程，从而获取以下各项中的任一项：加密的登录认证信息、解密的登录认证信息、解密密钥、认证信息存储地址以及加强的认证信息 (S1017)。

[0173] 此时，认证数据获取模块 94 可通过从第二通信设备 20 接收解密密钥，并使用解密密钥解密网站的加密登录认证信息来获取认证相关数据。在这一情况下，认证数据获取模块 94 通过从登录通知消息中提取第二通信设备的标识信息并通过通信电路 150 向 / 或从具有标识信息的第二通信设备 20 请求和接收解密密钥来获取解密密钥。此外，认证数据获取模块 94 基于第二通信设备的标识信息从数据存储模块 91 中为每个通信设备分类的安全数据检查专用于第二通信设备的安全数据。随后，认证数据获取模块 94 可通过从包含在专用于第二通信设备的安全数据中的登录认证信息中提取与网站标识信息相映射的加密的登录认证信息（即 ID 和密码）并且然后使用解密密钥对登录认证信息进行解密以得到登录认证信息，来获取认证相关数据。

[0174] 此外，认证数据获取模块 94 可通过基于通信设备的标识信息从针对每个通信设备进行分类的安全数据中检查出专用于第二通信设备的安全数据，并从包含在检查出的安全数据中的登录认证消息中提取与网站标识信息相映射的加密的登录认证信息（即 ID 和密码）来获取认证相关数据。

[0175] 在另一实施例中，认证数据获取模块 94 可通过从数据存储模块 91 中提取与第二

通信设备 20 的标识信息对应的解密密钥来获取认证相关数据。

[0176] 在另一实施例中，认证数据获取模块 94 可通过检查与第二通信设备的标识信息相映射的存储地址数据，并提取包含在检查出的存储地址数据的登录通知消息中的与网站标识信息相映射的加密的认证信息存储地址来获取认证相关数据。

[0177] 同时，如果检查出的安全等级为第二等级 (S1019)，则认证数据获取模块 94 通知第二通信设备 20 正试图登录网站，并且还向显示设备 141 输出通知窗口以询问是否批准登录 (S1021)。例如，认证数据获取模块 94 可向显示设备 141 输出通知窗口，比如“从远程点试图访问“www. ～～～～～～～ .com”。是否批准登录？”此外，仅当用户输入批准信号时 (S1023)，认证数据获取模块 94 才获取认证相关数据 (即，解密的登录认证信息、加密的登录认证信息、解密密钥或认证信息存储地址) (S1025)。

[0178] 同时，如果检查出的安全等级为第三等级，则认证数据获取模块 94 向显示设备 141 输出认证输入窗口以使得用户进行用户认证 (S1026)。例如，认证数据获取模块 94 可向显示设备 141 输出认证输入窗口“从远程点试图访问“www. ～～～～～～～ .com”。如果批准登录请输入密码。”接下来，如果通过认证输入窗口进行的用户认证信息输入与存储在数据存储模块 91 中的用户认证信息相同，则认证数据获取模块 94 如在第一等级中那样获取认证相关数据 (即，解密的登录认证信息、加密的登录认证信息、解密密钥或认证信息存储地址)。随后，认证数据获取模块 94 通过向显示设备 141 输出输入窗口以请求输入加强的认证信息 (S1029)，并经由输入窗口从用户处接收诸如生物信息、OTP 等之类的加强的认证信息 (S1031) 来附加地获取认证相关数据。认证数据获取模块 94 可借助于预定的加密算法对加强的认证信息进行加密。同时，如果安全等级为第三等级并且用户认证成功，则认证数据获取模块 94 可获取除加强的认证信息之外的认证相关数据中的至少一项，即解密的登录认证信息、加密的登录认证信息、解密密钥和认证信息存储地址中的至少一项，或者可仅获取加强的认证信息。

[0179] 接下来，认证数据提供模块 95 通过通信电路 150 将获取的认证相关数据提供给被赋予网站标识信息的网页服务器 40 或第二通信设备 20(S1033)。此时，如果认证数据提供模块 95 将认证相关数据发送至网页服务器 40，则认证数据提供模块 95 将从登录通知消息中提取的访问令牌一起发送，以使得在网页服务器 40 处对第二通信设备 20 进行登录认证。

[0180] 同时，如果安全等级为第三等级，则认证数据获取模块 95 可仅获取加强的认证信息作为认证相关数据。在这一情况下，认证数据提供模块 95 将加强的认证信息提供给网页服务器 40 或第二通信设备 20，而不发送登录认证信息、解密密钥、认证信息存储地址等。

[0181] 图 11 为示出了根据本发明实施例的一种用于在认证数据提供设备中强制登出通信设备的方法的流程图。

[0182] 参考图 11，如果第二通信设备 20 成功登录到网页服务器 40 以接收服务，则位置检查模块 93 通过使用 GPS 接收器 160 来持续地监测认证数据提供设备 100 的位置信息 (S1101)。换言之，如果从网页服务器 40 通知了第二通信设备 20 的成功登录，则位置检查模块 93 持续地监测认证数据提供设备 100 的位置信息。如果第二通信设备 20 是可用于移动通信的通信终端，则认证数据提供设备 100 持续地接收第二通信设备 20 的位置信息，以监测第二通信设备 20 的位置信息。

[0183] 接下来，基于监测到的位置信息，位置检查模块 93 确定认证数据提供设备 100 与

第二通信设备 20 是否一直位于同一地点 (S1103)。此时，位置检查模块 93 可通过检查第二通信设备 20 与认证数据提供设备 100 是否位于同一管理区内或认证数据提供设备 100 与第二通信设备 20 之间的距离是否小于阈值距离（例如，100 米），来确定第二通信设备 20 与认证数据提供设备 100 是否位于同一地点。此外，位置检查模块 93 还可通过检查认证数据提供设备 100 是否能够借助于通信电路 150 与第二通信设备 20 进行本地无线通信（例如，蓝牙通信），来确定第二通信设备 20 与认证数据提供设备 100 是否一直位于同一地点。

[0184] 如果检查出第二通信设备 20 和认证数据提供设备 100 位于同一地点，则位置检查模块 93 再次执行步骤 S1101。同时，如果检查出第二通信设备 20 和认证数据提供设备 100 不位于同一地点，则位置检查模块 93 从接收自安全中继服务器 30 的登录通知消息中检查访问令牌 (S1105)。此外，位置检查模块 93 将包括在访问令牌中的登出请求消息发送至网页服务器 40，以使得登录到网页服务器 40 的第二通信设备 20 被强制登出 (S1107)。

[0185] 尽管本说明书包含很多特征，但是这些特征不应被理解为对本发明的范围或所附权利要求进行限制。在不同示例性实施例的背景下描述的某些特征还可在单个示例性实施例中以组合的方式执行。相反地，在单个示例性实施例的背景下描述的各种特征可在多个示例性实施例中单独执行或者以任何合适的子组合方式执行。

[0186] 虽然附图以特定的顺序描述了操作，但是不应当理解为这些操作以附图中所示的特定顺序被执行或者以连续的顺序被依次执行，或者所有操作被执行以得到期望的结果。多任务或平行处理在特定环境下可能是有利的。此外，应当理解的是，所有示例性实施例不要求区分上述实施例中所给出的各种系统部件。程序部件和系统通常可被实施为单个软件产品或多个软件产品包。

[0187] 本发明的上述方法可被实施为程序指令并被记录在非瞬时计算机可读介质（比如，光盘只读存储器 (CD-ROM)、随机访问存储器 (RAM)、只读存储器 (ROM)、软盘、硬盘、磁光盘等）中。这些处理被可本发明所属技术领域的普通技术人员容易地执行，因而在此不再赘述。

[0188] 应当注意，本发明所属技术领域的普通技术人员可在不超出本发明的精神和范围的情况下对本发明作出各种替换、修改和改变，并且本发明不受上述实施例和附图的限制。

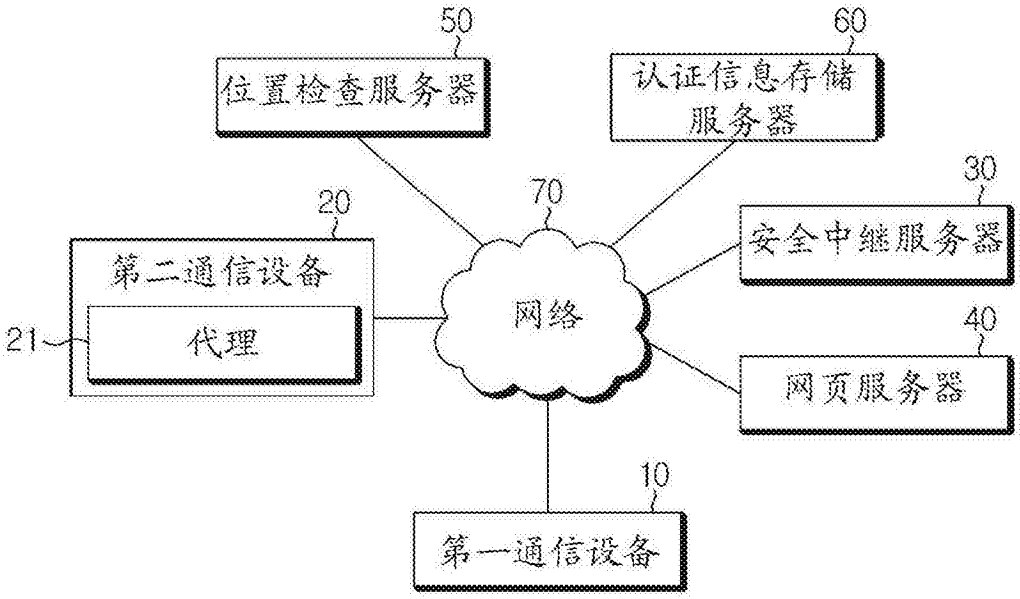

50
位置检查服务器
60
认证信息存储服务器
30
安全中继服务器
70
20
第二通信设备
21
代理
网络
40
网页服务器
10
第一通信设备

图 1

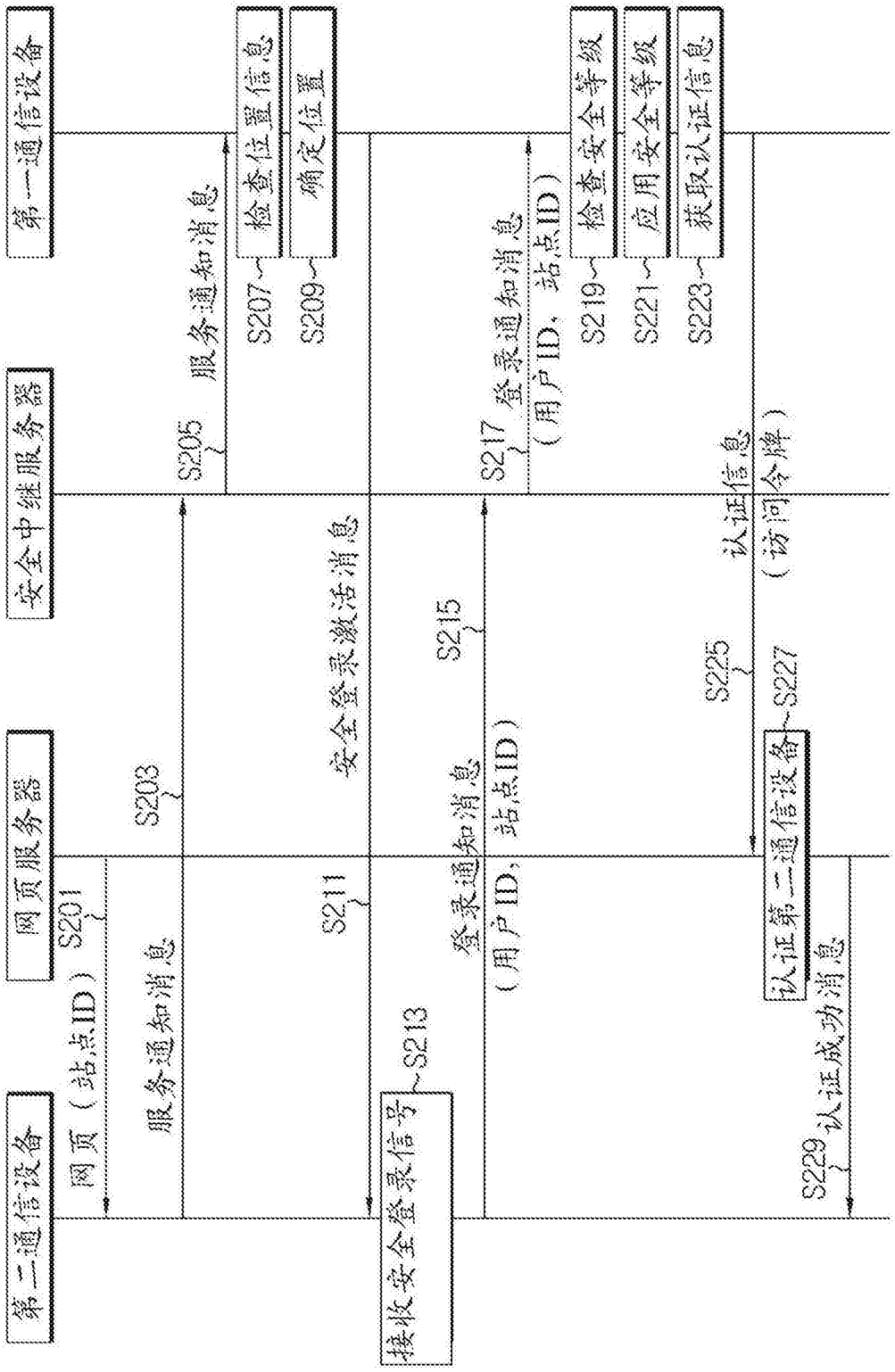

第二通信设备
网页服务器
安全中继服务器
第一通信设备
网页（站点ID）
S201
服务通知消息
S203
S205
服务通知消息
S207
检查位置信息
S209
确定位置
S211
安全登录激活消息
S213
接收安全登录信号
S215
登录通知消息
（用户ID，站点ID）
S217
登录通知消息
（用户ID，站点ID）
S219
检查安全等级
S221
应用安全等级
S223
获取认证信息
S225
认证信息
（访问令牌）
S227
认证第二通信设备
S229
认证成功消息

图 2

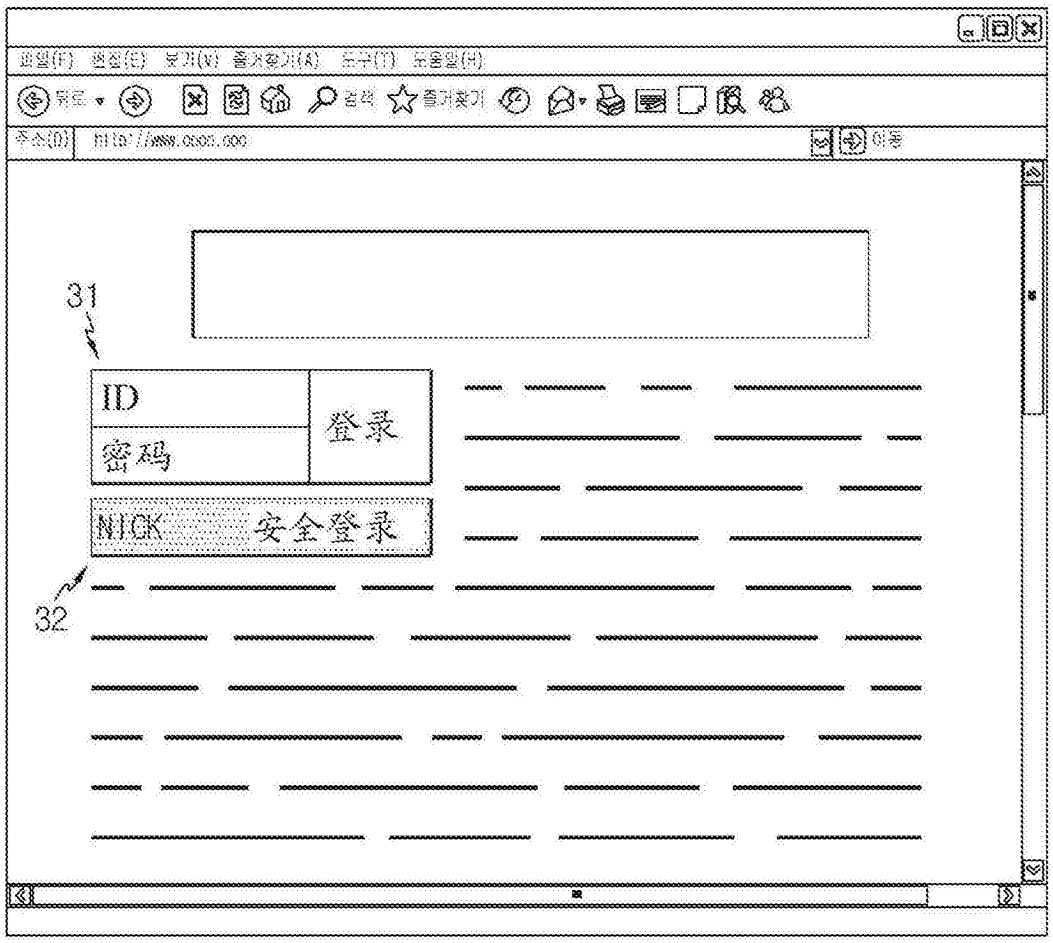


图 3

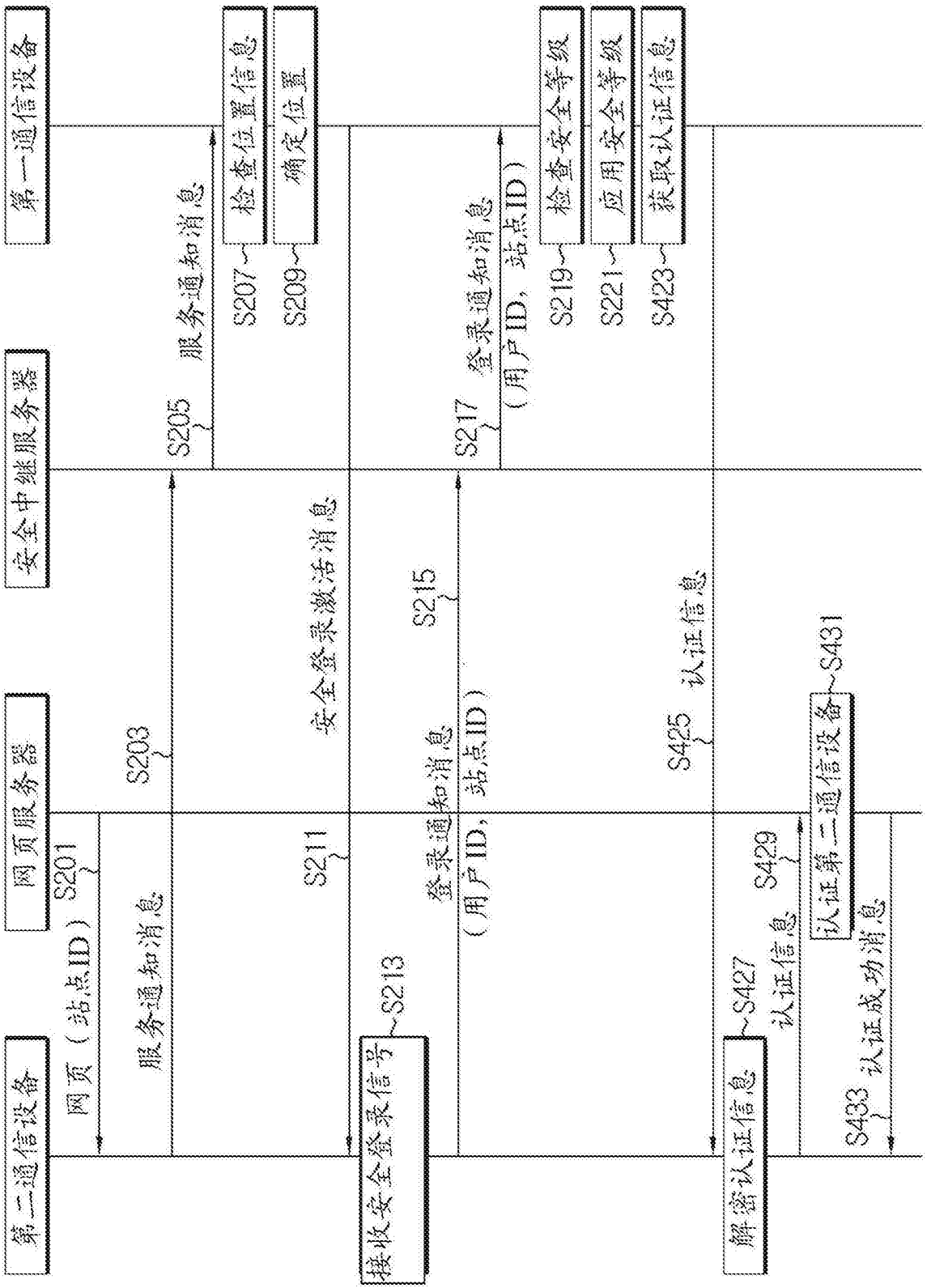

第二通信设备
网页服务器
安全中继服务器
第一通信设备
网页（站点ID）
S201
服务通知消息
S203
S205
服务通知消息
S207
检查位置信息
S209
确定位置
S211
安全登录激活消息
S213
接收安全登录信号
S215
登录通知消息
（用户ID，站点ID）
S217
登录通知消息
（用户ID，站点ID）
S219
检查安全等级
S221
应用安全等级
S423
获取认证信息
S425
认证信息
S427
解密认证信息
S429
认证信息
S431
认证第二通信设备
S433
认证成功消息

图 4

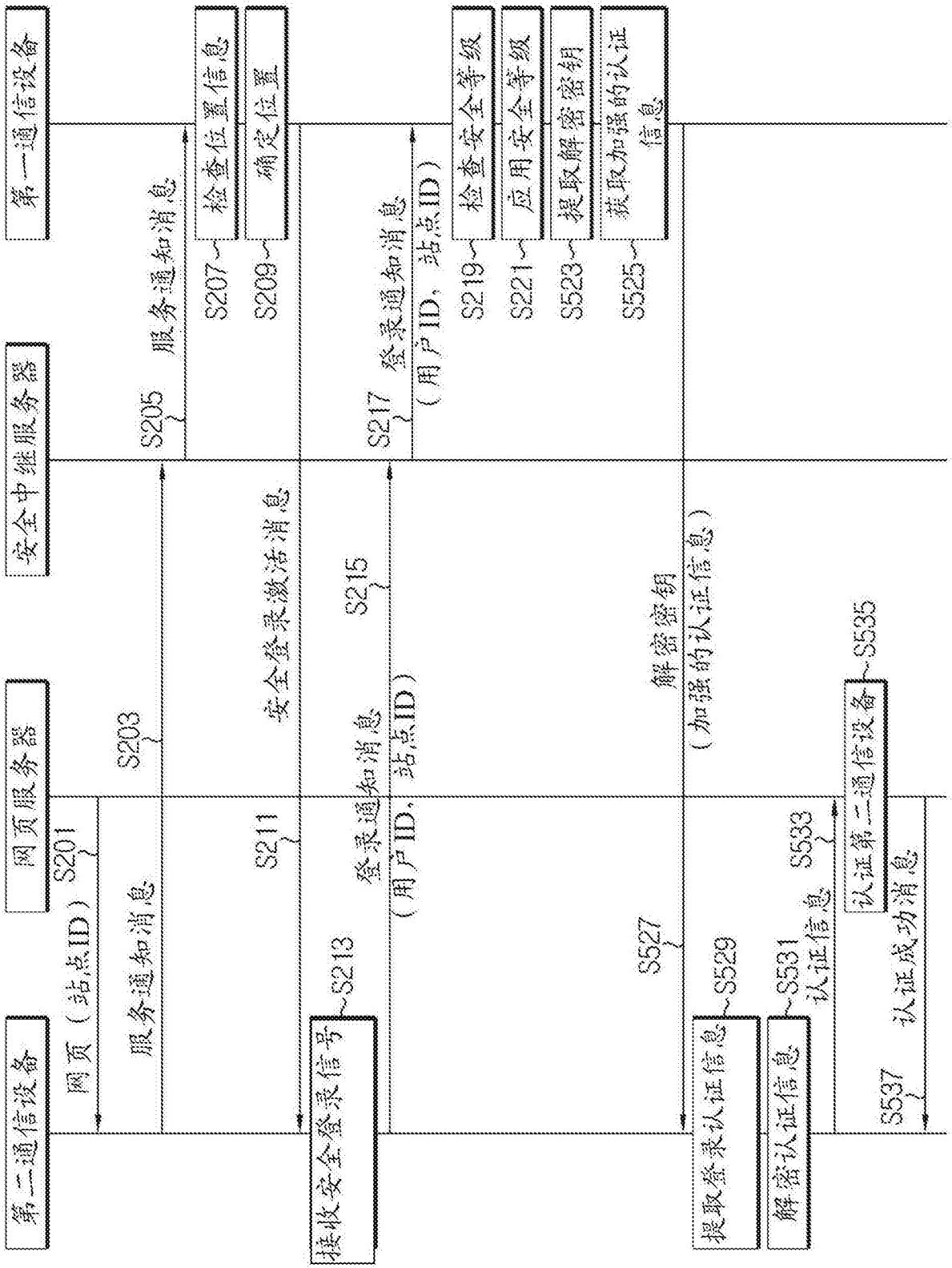

第一通信设备
安全中继服务器
网页服务器
第二通信设备
网页（站点ID）
S201
服务通知消息
S203
S205
服务通知消息
S207
检查位置信息
S209
确定位置
S211
安全登录激活消息
S213
接收安全登录信号
S215
登录通知消息
（用户ID，站点ID）
S217
登录通知消息
（用户ID，站点ID）
S219
检查安全等级
S221
应用安全等级
S523
提取解密密钥
S525
获取加强的认证信息
S527
解密密钥
（加强的认证信息）
S529
提取登录认证信息
S531
认证信息
S533
认证第二通信设备
S535
S537
认证成功消息
解密认证信息

图 5

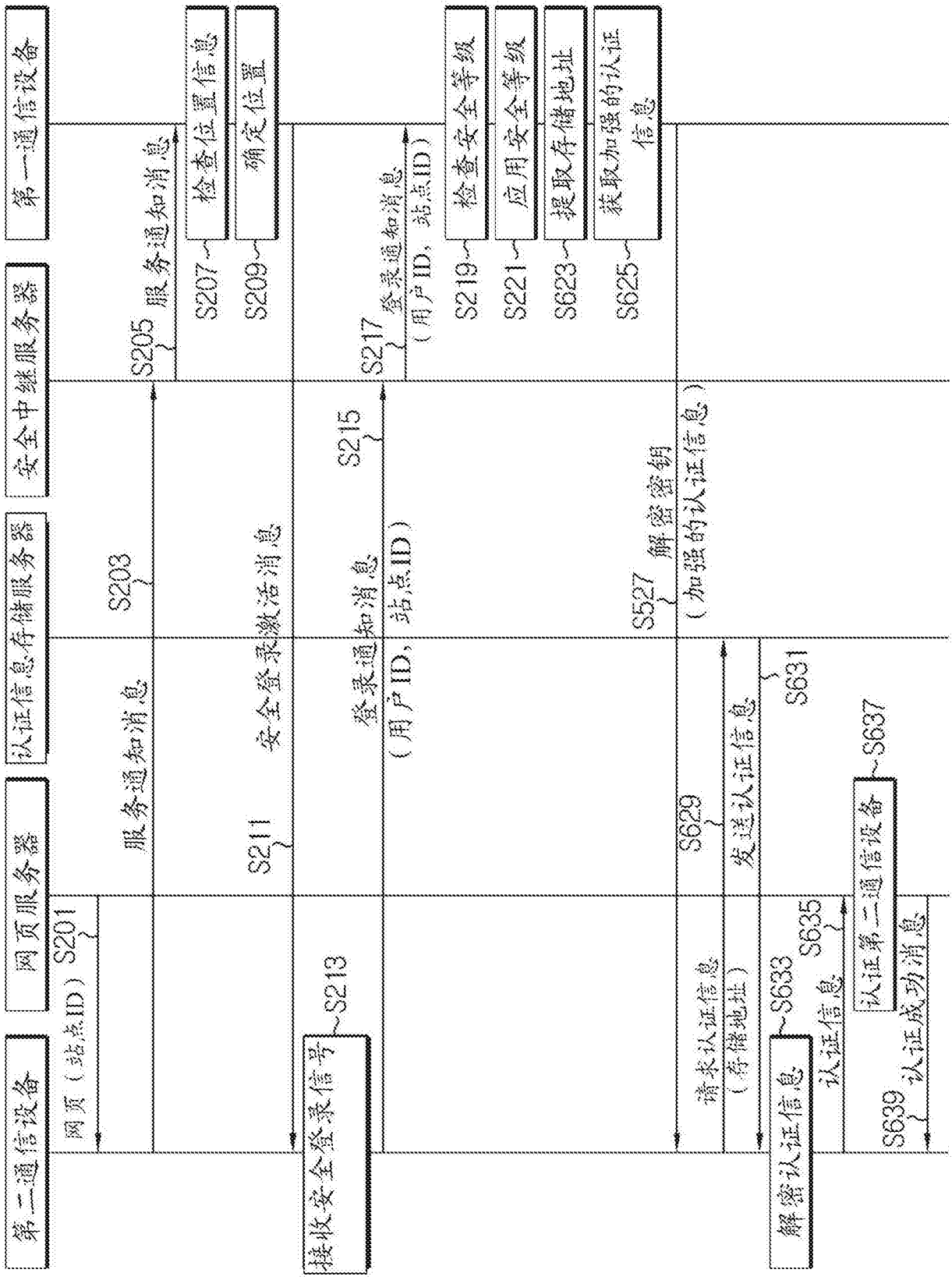

第一通信设备
安全中继服务器
认证信息存储服务器
网页服务器
第二通信设备
S201
网页（站点ID）
S203
服务通知消息
S205
服务通知消息
S207
检查位置信息
S209
确定位置
S211
安全登录激活消息
S213
接收安全登录信号
S215
登录通知消息
（用户ID，站点ID）
S217
登录通知消息
（用户ID，站点ID）
S219
检查安全等级
S221
应用安全等级
S623
提取存储地址
S625
获取加强的认证信息
S527
解密密钥
（加强的认证信息）
S629
请求认证信息
（存储地址）
S631
发送认证信息
S633
解密认证信息
S635
认证信息
S637
认证第二通信设备
S639
认证成功消息

图 6

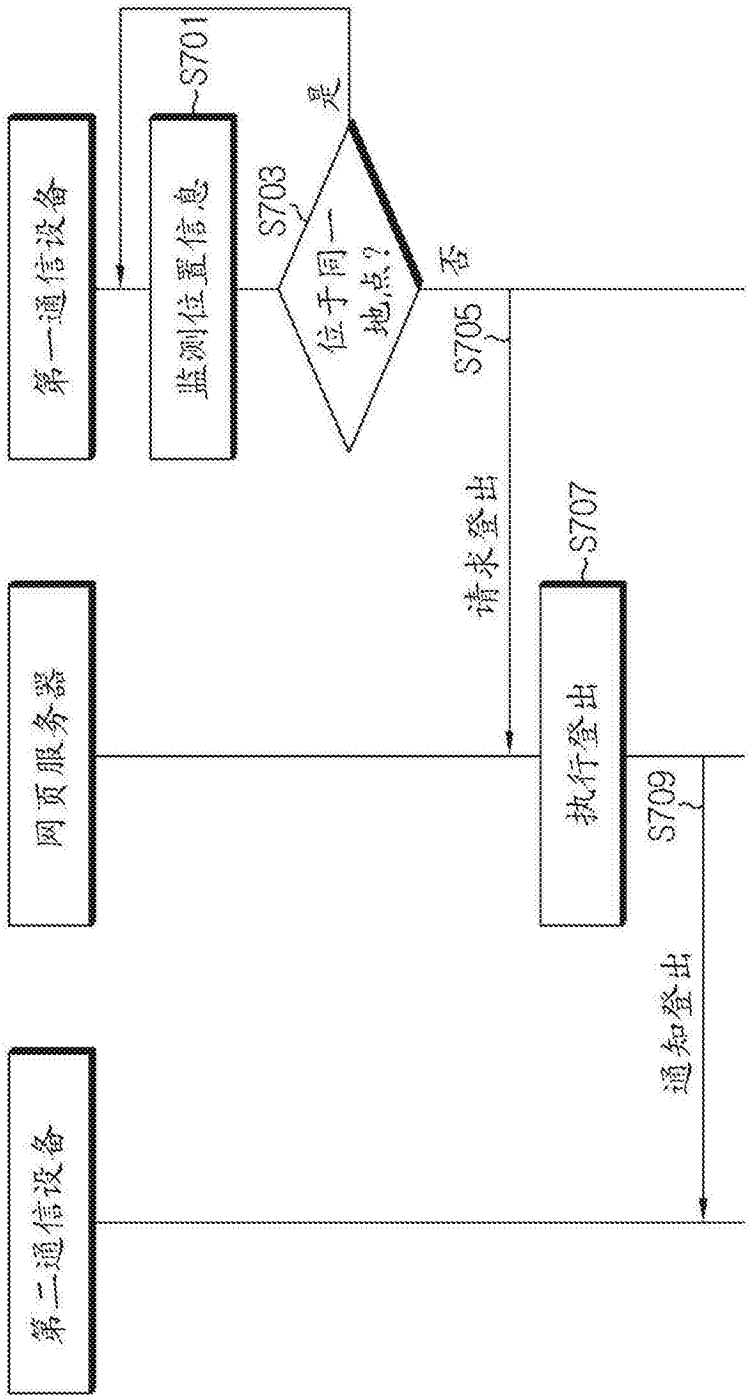

第一通信设备
监测位置信息
S701
S703
位于同一地点?
是
否
S705
请求登出
网页服务器
S707
执行登出
S709
通知登出
第二通信设备

图 7

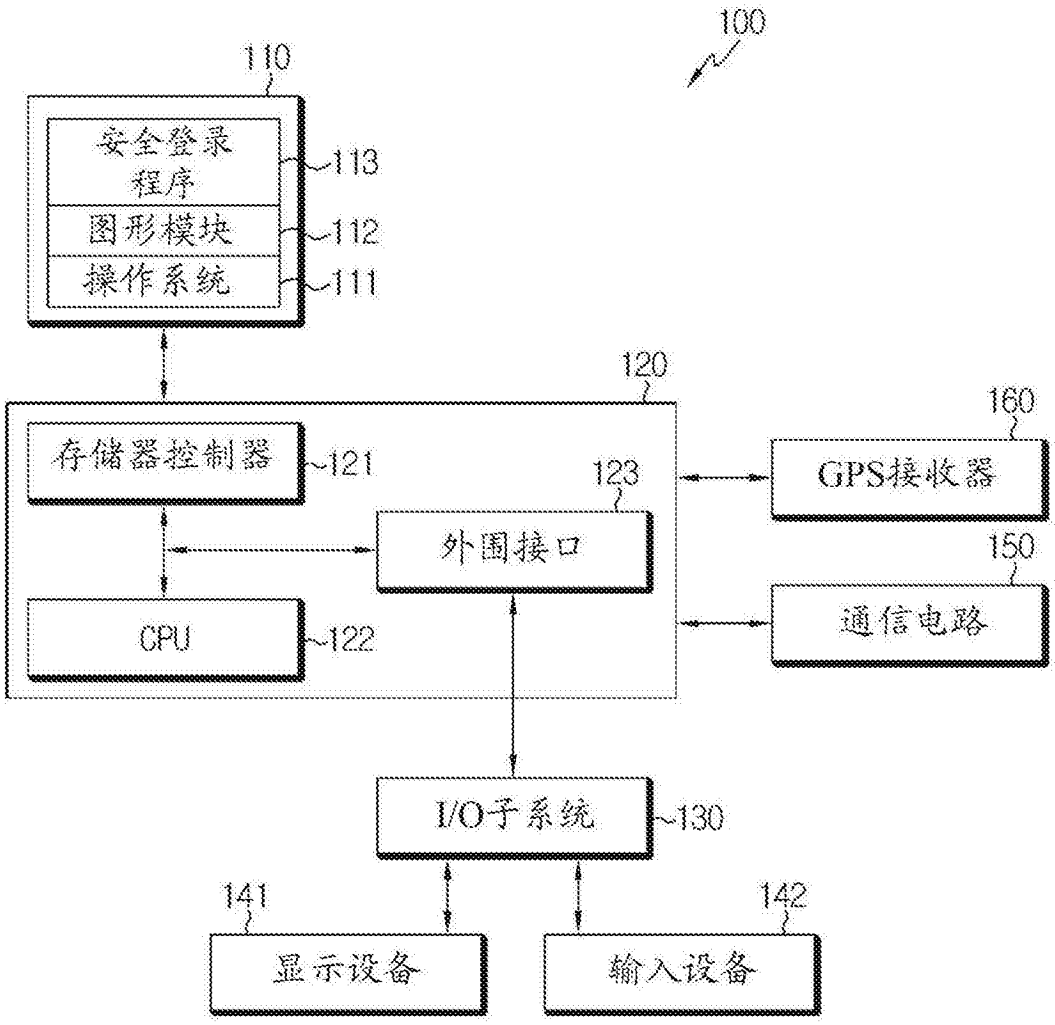

100
110
安全登录程序
113
图形模块
112
操作系统
111
120
存储器控制器
121
123
外围接口
CPU
122
160
GPS接收器
150
通信电路
I/O子系统
130
141
显示设备
142
输入设备

图 8

[Fig. 9]

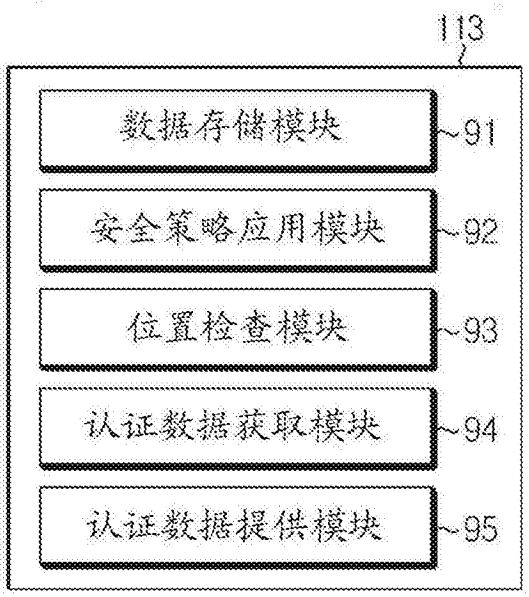


图 9

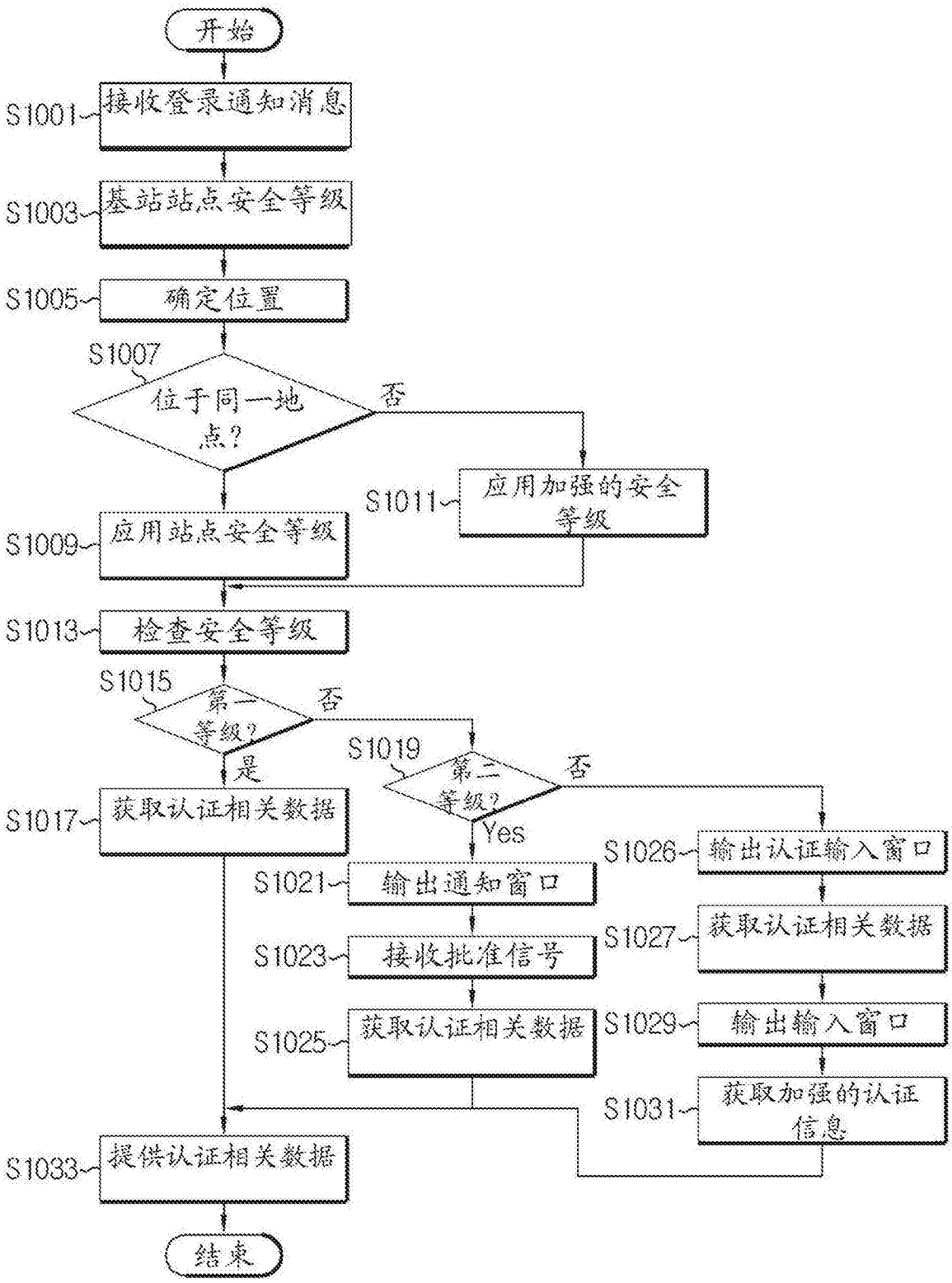

开始
S1001
接收登录通知消息
S1003
基站站点安全等级
S1005
确定位置
S1007
位于同一地点?
否
S1011
应用加强的安全等级
S1009
应用站点安全等级
S1013
检查安全等级
S1015
第一等级?
否
是
S1019
第二等级?
否
Yes
S1017
获取认证相关数据
S1021
输出通知窗口
S1023
接收批准信号
S1025
获取认证相关数据
S1026
输出认证输入窗口
S1027
获取认证相关数据
S1029
输出输入窗口
S1031
获取加强的认证信息
S1033
提供认证相关数据
结束

图 10

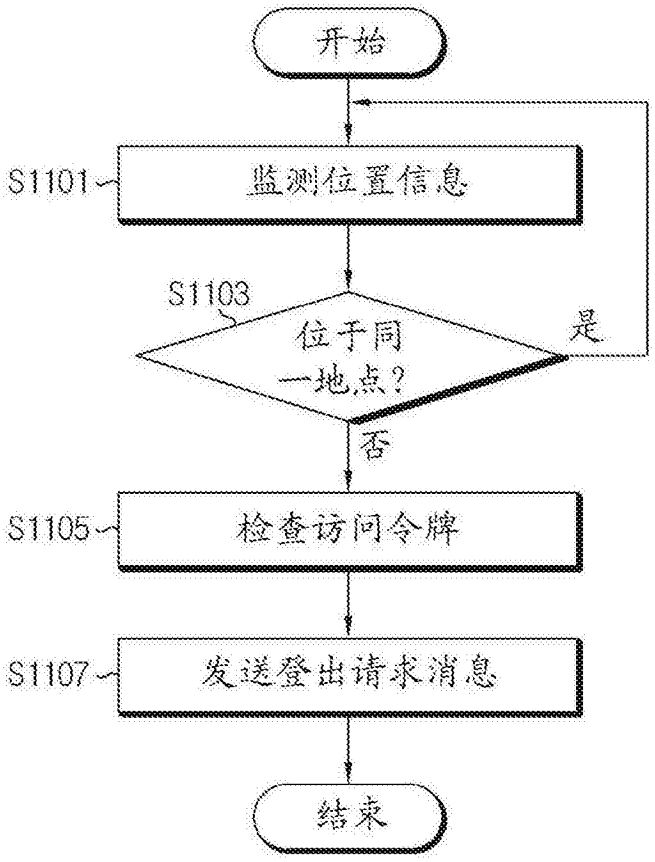

开始
S1101
监测位置信息
S1103
位于同一地点?
是
否
S1105
检查访问令牌
S1107
发送登出请求消息
结束

图 11