说 明 书 摘 要

本发明提供了一种电子设备的开机方法、装置、TPM设备及存储介质，先通过接收到所述电子设备产生的访问请求时获取电子设备的位置信息，接着，根据所述位置信息判断电子设备是否在预设范围内；在判断到所述电子设备在预设范围内，并在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥，解决了现有技术中可能存在开机秘钥被盗的风险。

摘 要 附 图


在接收到所述电子设备产生的访问请求时获取电子设备的位置信息
S101
根据所述位置信息判断电子设备是否在预设范围内
S102
若是，在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥
S103

权　利　要　求　书

1、一种电子设备的开机方法，其特征在于，包括：

在接收到所述电子设备产生的访问请求时获取电子设备的位置信息；

根据所述位置信息判断电子设备是否在预设范围内；

若是，在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥。

2、根据权利要求1所述的一种电子设备的开机方法，其特征在于，还包括：

在根据所述位置信息判断电子设备不在预设范围内，删除用于访问电子设备的秘钥。

3、根据权利要求2所述的一种电子设备的开机方法，其特征在于，所述在删除用于访问电子设备的秘钥之后，还包括：

监测所述电子设备重新处于预设范围内时，基于用户的操作获取秘钥，并向所述电子设备发送所述秘钥。

4、根据权利要求3所述的一种电子设备的开机方法，其特征在于，所述基于用户的操作获取秘钥包括：

获取由用户输入的秘钥，或基于用户的操作接收由服务器下发的秘钥。

5、一种电子设备的开机装置，其特征在于，包括：

位置信息获取单元，用于在接收到所述电子设备产生的访问请求时获

取电子设备的位置信息；

判断单元，用于根据所述位置信息判断电子设备是否在预设范围内；

发送单元，用于在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥。

6、根据权利要求5所述的一种电子设备的开机装置，其特征在于，还包括：

在根据所述位置信息判断电子设备不在预设范围内，删除用于访问电子设备的秘钥。

7、根据权利要求6所述的一种电子设备的开机装置，其特征在于，所述在删除用于访问电子设备的秘钥之后，还包括：

监测所述电子设备重新处于预设范围内时，基于用户的操作获取秘钥，并向所述电子设备发送所述秘钥。

8、根据权利要求7所述的一种电子设备的开机装置，其特征在于，所述基于用户的操作获取秘钥包括：

获取由用户输入的秘钥，或基于用户的操作接收由服务器下发的秘钥。

9、一种电子设备的TPM设备，其特征在于，包括存储器以及处理器，所述存储器内存储有计算机程序，所述计算机程序能够被所述处理器执行，以实现如权利要求1至4任意一项所述的一种电子设备的开机方法。

10、一种计算机可读存储介质，其特征在于，存储有计算机程序，所述计算机程序能够被所述计算机可读存储介质所在设备的处理器执行，以实现如权利要求1至4任意一项所述一种电子设备的开机方法。

说　　明　　书

一种电子设备的开机方法、装置、TPM设备及存储介质

技术领域

本发明涉及计算机领域，特别涉及一种电子设备的开机方法、装置、TPM设备及存储介质。

背景技术

在现有技术中，笔记本电脑的可以基于密码的输入、指纹识别、或者人脸识别来执行开机操作，然而，在一些情况下，在笔记本电脑的使用者离开笔记电脑之后，可能被人为以相同外观且具有相同开机界面的笔记本电脑替换，使用者在被替换后的笔记本电脑上输入相同的密码或者指纹时，可能导致秘钥信息被盗取。

有鉴于此，提出本申请。

发明内容

本发明公开了一种电子设备的开机方法、装置、TPM设备及存储介质，旨在解决现有技术中可能存在开机秘钥被盗的风险。

本发明第一实施例提供了一种电子设备的开机方法于，包括：

在接收到所述电子设备产生的访问请求时获取电子设备的位置信息；

根据所述位置信息判断电子设备是否在预设范围内；

若是，在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥；

优选地，还包括：

在根据所述位置信息判断电子设备不在预设范围内，删除用于访问电子设备的秘钥。

优选地，所述在删除用于访问电子设备的秘钥之后，还包括：

监测所述电子设备重新处于预设范围内时，基于用户的操作获取秘钥，并向所述电子设备发送所述秘钥。

优选地，所述基于用户的操作获取秘钥包括：

获取由用户输入的秘钥，或基于用户的操作接收由服务器下发的秘钥。

本发明第二实施例提供了一种电子设备的开机装置，包括：

位置信息获取单元，用于在接收到所述电子设备产生的访问请求时获取电子设备的位置信息；

判断单元，用于根据所述位置信息判断电子设备是否在预设范围内；

发送单元，用于在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥；

优选地，还包括：

在根据所述位置信息判断电子设备不在预设范围内，删除用于访问电子设备的秘钥。

优选地，所述在删除用于访问电子设备的秘钥之后，还包括：

监测所述电子设备重新处于预设范围内时，基于用户的操作获取秘钥，并向所述电子设备发送所述秘钥。

优选地，所述基于用户的操作获取秘钥包括：

获取由用户输入的秘钥，或基于用户的操作接收由服务器下发的秘钥。

本发明第三实施例提供了一种电子设备的TPM设备，包括存储器以及处理器，所述存储器内存储有计算机程序，所述计算机程序能够被所述处理器执行，以实现如上任意一项所述的一种电子设备的开机方法。

本发明第四实施例提供了一种计算机可读存储介质，其特征在于，存储有计算机程序，所述计算机程序能够被所述计算机可读存储介质所在设备的处理器执行，以实现如上任意一项所述一种电子设备的开机方法。

基于本发明提供的一种电子设备的开机方法、装置、TPM设备及存储介质，先通过接收到所述电子设备产生的访问请求时获取电子设备的位置信息，接着，根据所述位置信息判断电子设备是否在预设范围内；在判断到所述电子设备在预设范围内，并在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥，解决了现有技术中可能存在开机秘钥被盗的风险。

附图说明

图1是本发明第一实施例提供的一种电子设备的开机方法流程示意图；

图2是本发明第二实施例提供的一种电子设备的开机装置模块示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

为了更好的理解本发明的技术方案，下面结合附图对本发明实施例进行详细描述。

应当明确，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

在本发明实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本发明。在本发明实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。

应当理解，本文中使用的术语“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”或“响应于检测”。类似地，取决于语境，短语“如果确定”或“如果检测（陈述的条件或事件）”可以被解释成为“当确定时”或“响应于确定”或“当检测（陈述的条件或事件）时”或“响应于检测（陈述的条件或事件）”。

实施例中提及的“第一\第二”仅仅是是区别类似的对象，不代表针对对象的特定排序，可以理解地，“第一\第二”在允许的情况下可以互换特定的顺序或先后次序。应该理解“第一\第二”区分的对象在适当情况下可以互换，以使这里描述的实施例能够以除了在这里图示或描述的那些以外的顺序实施。

以下结合附图对本发明的具体实施例做详细说明。

本发明公开了一种电子设备的开机方法、装置、TPM设备及存储介质，旨在解决现有技术中可能存在开机秘钥被盗的风险。

请参阅图1，本发明第一实施例提供了一种电子设备的开机方法，其可由电子设备的TPM设备（以下简称TPM设备）来执行，特别的，由TPM设备内的一个或者多个处理器来执行，以至少实现如下步骤：

S101，在接收到所述电子设备产生的访问请求时获取电子设备的位置信息；

在本实施例中，所述TPM设备可以是手机、智能手表、智能项链等具有数据处理分析能力的终端，其中，所述控制设备内可安装有相应的操作系统以及应用软件，并通过操作系统以及应用软件的结合来实现本实施例所需的功能。

需要说明的是，TPM（可信平台模块）是一种硬件安全解决方案，旨在提供计算设备的安全功能和保护。它是一个集成电路芯片，通常嵌入在计算机、服务器、移动设备等硬件平台中。TPM的主要功能是提供安全存储、加密和认证功能。它可以生成和存储加密密钥、证书和其他敏感数据，并

用于进行加密操作、数字签名和认证过程。TPM 通过硬件级别的安全机制，提供对存储在其中的数据的保护，以防止未经授权的访问或篡改。TPM 还可以用于验证计算设备的完整性和认证设备的身份。它可以监测和记录设备的状态和配置，并与可信计算基础设施（TCB）进行安全交互，以确保系统的可信度。TPM 平台在数据安全、身份验证、数字版权保护、加密通信等领域发挥着重要作用。它提供了一种安全的基础，帮助保护计算设备和用户数据免受恶意攻击和未经授权的访问。

在本实施例中，TPM 设备内部可以配置有无线模块和定位模块，例如 4G 或 5G 模块（不仅限于此），其可以与所述电子设备进行通讯，其中，所述电子设备可以是笔记本电脑或者平板电脑等，所述电子设备能够与所述 TPM 设备内部的无线模块建立起通讯连接，进一步地，在本实施例中，所述电子设备在被进行输入密码验证或者指纹验证，当然也可以是人脸验证来发起访问请求时，配置在电子设备的定位模块（例如 GPS 模块）能够获取到电子设备的当前位置信息，并将其发送给 TPM 设备，TPM 设备能够基于内部的定位模块获取 TPM 设备的当前位置信息，并和电子设备的当前位置信息进行比较。

S102，根据所述位置信息判断电子设备是否在预设范围内；

S103，若是，在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥；

需要说明的是，以 TPM 设备为一个智能手表为例，其在接收到电子设备的访问请求后且判断电子设备在 TPM 设备的预设范围内（例如在 10 英尺范围内），其可以基于用户授权操作向所述电子设备提供用于访问的秘钥，具体地，在智能手表上可以弹出一个用于授权的界面，其中，所述界面配置有“登录”按钮，在监测到用户点击登录后发送秘钥。

在本发明一个可能的实施例中，还可以在用户点击登录按钮后，获取用户当前的身体参数，其中，身体参数可以包括心跳信息、呼吸信息、血氧信息等，将所述身体参数与历史数据进行匹配，在匹配成功后向电子设备发送秘钥。

在本发明一个可能的实施例中，还可以包括：

在根据所述位置信息判断电子设备不在预设范围内，删除用于访问电子设备的秘钥。

需要说明的是，在接收电子设备发起访问请求，然后电子设备却不在附近（即不在预设范围内），可以判断电子设备存在被盗的可能性，其可以删除秘钥，避免不法分子获取电子设备上的资料。

在本发明一个可能的实施例中，所述在删除用于访问电子设备的秘钥之后，还包括：

监测所述电子设备重新处于预设范围内时，基于用户的操作获取秘钥，并向所述电子设备发送所述秘钥。

需要说明的是，在秘钥被删除可能存在误删的情况，例如，电子设备被小孩子输入密码，此时在范围外的TPM设备接收到访问请求，但判断到电子设备在范围外，其会自动删除秘钥，而此时，佩戴有TPM设备的用户回到电子设备前（也就是电子设备处于TPM的范围内时），可以基于用户的操作重新生成秘钥，具体地，可以用户点击登录时，通过获取由在TPM设备输入的秘钥，当然，也可以接收由服务器下发的秘钥，在TPM设备上重新拥有秘钥后，下发给所述电子设备。

请参阅图2,本发明第二实施例提供了一种电子设备的开机装置,包括：

位置信息获取单201，用于在接收到所述电子设备产生的访问请求时获取电子设备的位置信息；

判断单元202，用于根据所述位置信息判断电子设备是否在预设范围内；

发送单元203，用于在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥；

优选地，还包括：

在根据所述位置信息判断电子设备不在预设范围内，删除用于访问电子设备的秘钥。

优选地，所述在删除用于访问电子设备的秘钥之后，还包括：

监测所述电子设备重新处于预设范围内时，基于用户的操作获取秘钥，并向所述电子设备发送所述秘钥。

优选地，所述基于用户的操作获取秘钥包括：

获取由用户输入的秘钥，或基于用户的操作接收由服务器下发的秘钥。

本发明第三实施例提供了一种电子设备的TPM设备，包括存储器以及处理器，所述存储器内存储有计算机程序，所述计算机程序能够被所述处理器执行，以实现如上任意一项所述的一种电子设备的开机方法。

本发明第四实施例提供了一种计算机可读存储介质，其特征在于，存储有计算机程序，所述计算机程序能够被所述计算机可读存储介质所在设备的处理器执行，以实现如上任意一项所述一种电子设备的开机方法。

基于本发明提供的一种电子设备的开机方法、装置、TPM设备及存储介质，先通过接收到所述电子设备产生的访问请求时获取电子设备的位置信

息，接着，根据所述位置信息判断电子设备是否在预设范围内；在判断到所述电子设备在预设范围内，并在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥，解决了现有技术中可能存在开机秘钥被盗的风险。

示例性地，本发明第三实施例和第四实施例中所述的计算机程序可以被分割成一个或多个模块，所述一个或者多个模块被存储在所述存储器中，并由所述处理器执行，以完成本发明。所述一个或多个模块可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序在所述实现一种电子设备的TPM设备中的执行过程。例如，本发明第二实施例中所述的装置。

所称处理器可以是中央处理单元(Central Processing Unit，CPU)，还可以是其他通用处理器、数字信号处理器 (Digital Signal Processor，DSP)、专用集成电路 (Application Specific Integrated Circuit，ASIC)、现成可编程门阵列 (Field-Programmable Gate Array，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等，所述处理器是所述一种电子设备的开机方法的控制中心，利用各种接口和线路连接整个所述实现一种电子设备的开机方法的各个部分。

所述存储器可用于存储所述计算机程序和/或模块，所述处理器通过运行或执行存储在所述存储器内的计算机程序和/或模块，以及调用存储在存储器内的数据，实现一种电子设备的开机方法的各种功能。所述存储器可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、

至少一个功能所需的应用程序（比如声音播放功能、文字转换功能等）等；存储数据区可存储根据手机的使用所创建的数据（比如音频数据、文字消息数据等）等。此外，存储器可以包括高速随机存取存储器，还可以包括非易失性存储器，例如硬盘、内存、插接式硬盘、智能存储卡（Smart Media Card，SMC）、安全数字（Secure Digital，SD）卡、闪存卡（Flash Card）、至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

其中，所述实现的模块如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实现上述实施例方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一个计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括电载波信号和电信信号。

需说明的是，以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。另外，本发明提供的装置实施例附图

中，模块之间的连接关系表示它们之间具有通信连接，具体可以实现为一条或多条通信总线或信号线。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

说　　明　　书　　附　　图


在接收到所述电子设备产生的访问请求时获取电子设备的位置信息
S101
根据所述位置信息判断电子设备是否在预设范围内
S102
若是，在监测到用户授权所述访问请求时，向所述电子设备提供用于访问的秘钥
S103

图 1

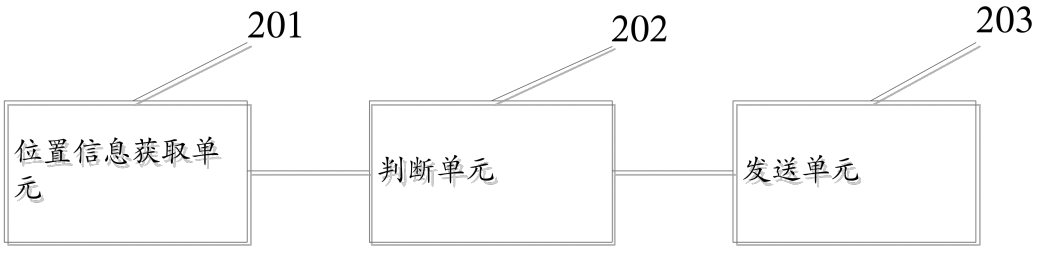
201
202
203
位置信息获取单元
判断单元
发送单元

图 2