(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116723506 A
(43)申请公布日 2023.09.08

(21)申请号 202211342483.4

(22)申请日 2022.10.31

(71)申请人 中电信数智科技有限公司
地址 100036 北京市海淀区复兴路33号

(72)发明人 王斌 杨戈 盛振明 夏建明
颜凤辉 王欣

(74)专利代理机构 南京钟山专利代理有限公司 32252
专利代理师 上官凤栖

(51)Int.Cl.
*H04W 12/06*(2021.01)
*H04L 67/02*(2022.01)

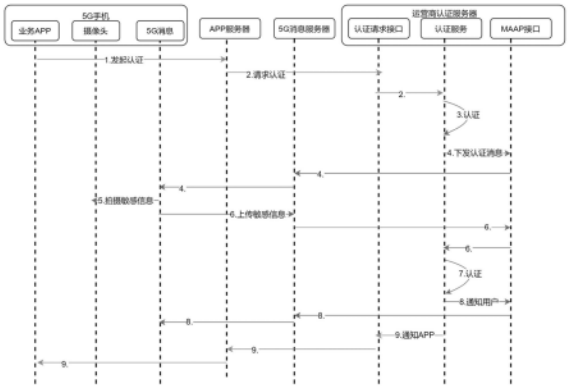
权利要求书2页 说明书6页 附图8页

(54)发明名称

一种通过5G消息进行敏感信息认证的方法、系统和存储介质

(57)摘要

本发明公开了一种通过5G消息进行敏感信息认证的方法，本方法利用5G消息进行敏感信息的传输，在运营商认证服务器和第三方认证服务器中对敏感信息进行认证，认证方法包括静态信息认证、动态信息认证和远端认证；敏感信息不流入发起认证的业务APP，业务APP只接收认证结果。本发明还公开了一种通过5G消息进行敏感信息认证的系统，包括5G手机、APP服务器、运营商认证服务器、5G消息服务器和第三方认证服务器；在运营商认证服务器中进行静态信息认证和动态信息认证，在第三方认证服务器中进行远端认证。认证过程很安全，避免业务APP窃取和监听敏感信息；当业务APP涉及贷款等经济行为时，本发明可通过动态信息认证判定用户是否被绑架，保证用户人身安全。




CN 116723506 A

1.一种通过5G消息进行敏感信息认证的方法,其特征在于,所述方法包括以下步骤:

S1:APP服务器将用户上传的基本认证信息转发给运营商认证服务器的认证请求接口,认证请求接口检查APP厂商和运营商是否有合约,如果有合约则将基本认证信息转发给运营商认证服务器的认证服务模块,如果没有合约则给APP服务器返回提示错误的信息;

S2:认证服务模块对基本认证信息进行认证,如果认证成功,认证服务模块构建一条5G MAAP卡片消息,通过运营商认证服务器的MAAP接口向5G消息服务器发送认证请求,5G消息服务器将认证请求转发给用户手机的5G消息模块,提示用户上传用于进一步认证的敏感信息;如果认证失败,认证服务模块通过认证请求接口通知APP服务器认证失败;

S3:用户将用于进一步认证的敏感信息通过手机的5G消息模块上传给5G消息服务器,5G消息服务器通过运营商认证服务器的MAAP接口将敏感信息转发给认证服务模块;

S4:认证服务模块根据认证业务的类型判断是否需要远端认证,如果不需要则在运营商认证服务器进行本地认证,认证服务模块将认证结果通知给用户和业务APP;如果需要,认证服务模块将敏感信息转发给第三方认证服务器进行远端认证。

2.根据权利要求1所述的通过5G消息进行敏感信息认证的方法,其特征在于:步骤S2中,所述基本认证信息包括手机号、姓名和不完整身份证号,所述认证服务模块对基本认证信息进行认证具体为:

认证服务模块根据用户的手机号,从运营商认证服务器的用户信息数据库中调取用户信息,结合姓名和不完整身份证号进行比对。

3.根据权利要求1所述的通过5G消息进行敏感信息认证的方法,其特征在于:步骤S2中,所述敏感信息包括照片、视频、身份证、银行卡和活体检验媒体。

4.根据权利要求1所述的通过5G消息进行敏感信息认证的方法,其特征在于,步骤S4中,所述本地认证包括以下步骤:

S4.1:认证服务模块根据认证业务的类型判断进行静态信息认证还是进行动态信息认证;如果进行静态信息认证,进入步骤S4.2,如果进行动态信息认证,进入步骤S4.3;

S4.2:认证服务模块通过图像和视频检验,确认用户身份,认证服务模块形成一条包含认证结果的5G消息,通过MAAP接口发送到5G消息服务器,5G消息服务器将包含认证结果的5G消息转发给用户手机上的5G消息模块;同时,认证服务模块通过认证请求接口将认证结果反馈给APP服务器,APP服务器通知用户手机上的业务APP;

S4.3:认证服务模块生成一条5G MAAP卡片消息,通过MAAP接口发送给5G消息服务器,5G消息服务器转发给手机的5G消息模块,询问用户是否允许运营商获取用户动态信息进行安全检查,用户将选择结果通过5G消息发送给认证服务模块;如果用户允许运营商获取用户动态信息进行安全检查,则进入步骤S4.4;如果用户不允许运营商获取用户动态信息进行安全检查,则进行静态信息认证;

S4.4:认证服务模块从用户信息数据库中获取用户动态数据,判断用户行为是否异常,并将结果通过认证请求接口发送给APP服务器,APP服务器将结果反馈给业务APP。

5.根据权利要求1所述的通过5G消息进行敏感信息认证的方法,其特征在于,步骤S4中,所述远端认证具体为:

认证服务模块将敏感信息通过运营商认证服务器的远端认证接口转发给第三方认证服务器,第三方认证服务器对敏感信息进行认证,并将结果通过远端认证接口反馈给认证

服务模块，认证服务模块将认证结果通过认证请求接口反馈给APP服务器，APP服务器通知用户手机上的业务APP。

6.一种通过5G消息进行敏感信息认证的系统，其特征在于，包括：5G手机、APP服务器、运营商认证服务器、5G消息服务器和第三方认证服务器；

所述5G手机包括业务APP和5G消息模块，业务APP和5G消息模块完全隔离；业务APP用于采集用户姓名、手机号和非完整身份证号，向运营商认证服务器发起认证请求；5G消息模块用于接收运营商认证服务器下发的采集敏感信息的请求，将用户上传的敏感信息发送给5G消息服务器，解析认证结果展示给5G手机终端用户；

所述5G消息服务器包括数据转发模块和MAAP模块；对于上行5G消息，数据转发模块将5G手机中的5G消息模块发送的5G消息转发给MAAP模块，MAAP模块将5G消息发送给运营商认证服务器；对于下行5G消息，运营商认证服务器将下行消息发送给MAAP模块，MAAP模块将其发送给5G手机中的5G消息模块；

所述运营商认证服务器包括认证请求接口、认证服务模块、MAAP接口、用户信息数据库和远端认证接口；认证请求接口接收APP服务器发送的认证请求和基本认证信息，并检查APP厂商和运营商是否有合约，通知认证服务器进行基本信息认证，并接收认证结果返回给APP服务器；MAAP接口和5G消息服务器的MAAP模块交互，收发5G消息；

所述远端认证接口向第三方认证服务器发送远端认证请求，接收远端认证的结果，并反馈给认证服务模块。

7.根据权利要求6所述的通过5G消息进行敏感信息认证的系统，其特征在于，所述用户信息数据库包括入网登记信息和动态数据；所述入网登记信息包括姓名、性别、身份证号和身份证照片；所述动态数据包括是否长期关机后在异地突然开机、用户历史位置轨迹、用户手机当前注册基站位置。

8.根据权利要求6所述的通过5G消息进行敏感信息认证的系统，其特征在于，所述认证服务模块根据认证业务类型判断需要进行静态信息认证、动态信息认证还是远端认证；如果需要进行静态信息认证，认证服务模块根据用户的手机号从用户信息数据库调取入网登记信息，与用户在APP输入的姓名和不完整身份证号进行比对，如果不符合则认证失败，如果符合则要求用户通过5G消息上传身份证照片和活体检验媒体并进行检验；如果需要进行动态信息认证，认证服务模块在征得用户允许的情况下，根据用户信息数据库中的动态数据，判断用户行为是否异常，将结果反馈给APP服务器；如果需要远端认证，认证服务模块通过远端认证接口调用第三方认证服务器进行远端认证。

9.一种计算机可读存储介质，其特征在于：存储有计算机程序，所述计算机程序使计算机执行如权利要求1-5任一项所述的通过5G消息进行敏感信息认证的方法。

# 一种通过5G消息进行敏感信息认证的方法、系统和存储介质

## 技术领域

[0001] 本发明涉及移动通信和信息认证领域，具体涉及一种通过5G消息进行敏感信息认证的方法、系统和存储介质。

## 背景技术

[0002] 敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹以及不满十四周岁未成年人的个人信息，敏感个人信息一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。当前手机APP在大量业务场景下，都需要进行敏感个人信息认证，如要求用户拍摄身份证，银行卡正反面信息上传，并采集视频信息进行活体检查，这些信息都会通过APP传到云端APP服务器上，然后转交给第三方认证服务器进行认证。但是部分APP可能出于各种目的，保存用户敏感个人信息甚至原始图像、视频等信息。外部黑客可能利用系统漏洞盗取数据库，内部员工可能会利用管理漏洞盗取数据库，并售卖用户个人信息，导致用户信息被泄露，甚至引发诈骗或者银行卡非法开户等恶性问题。

## 发明内容

[0003] 本发明针对现有技术中的不足，提供一种通过5G消息进行敏感信息认证的方法、系统和存储介质；保证所有敏感信息都不流入APP，而是通过5G消息直接进入高度可信的运营商认证服务器，并在征得用户的允许下，根据用户的动态数据判断用户行为是否异常，作为进一步认证的依据。最终APP只需获取认证结果，保证后续业务正常进行。

[0004] 为实现上述目的，本发明采用以下技术方案：

一种通过5G消息进行敏感信息认证的方法，所述方法包括以下步骤：

S1：APP服务器将用户上传的基本认证信息转发给运营商认证服务器的认证请求接口，认证请求接口检查APP厂商和运营商是否有合约，如果有合约则将基本认证信息转发给运营商认证服务器的认证服务模块，如果没有合约则给APP服务器返回提示错误的信息；

S2：认证服务模块对基本认证信息进行认证，如果认证成功，认证服务模块构建一条5G MAAP卡片消息，通过运营商认证服务器的MAAP接口向5G消息服务器发送认证请求，5G消息服务器将认证请求转发给用户手机的5G消息模块，提示用户上传用于进一步认证的敏感信息；如果认证失败，认证服务模块通过认证请求接口通知APP服务器认证失败；

S3：用户将用于进一步认证的敏感信息通过手机的5G消息模块上传给5G消息服务器，5G消息服务器通过运营商认证服务器的MAAP接口将敏感信息转发给认证服务模块；

S4：认证服务模块根据认证业务的类型判断是否需要远端认证，如果不需要则在运营商认证服务器进行本地认证，认证服务模块将认证结果通知给用户和业务APP；如果需要，认证服务模块将敏感信息转发给第三方认证服务器进行远端认证。

[0005] 为优化上述技术方案，采取的具体措施还包括：

进一步地，步骤S2中，所述基本认证信息包括手机号、姓名和不完整身份证号，所

述认证服务模块对基本认证信息进行认证具体为：

认证服务模块根据用户的手机号，从运营商认证服务器的用户信息数据库中调取用户信息，结合姓名和不完整身份证号进行比对。

[0006] 进一步地，步骤S2中，所述敏感信息包括照片、视频、身份证、银行卡和活体检验媒体。

[0007] 进一步地，步骤S4中，所述本地认证包括以下步骤：

S4.1：认证服务模块根据认证业务的类型判断进行静态信息认证还是进行动态信息认证；如果进行静态信息认证，进入步骤S4.2，如果进行动态信息认证，进入步骤S4.3；

S4.2：认证服务模块通过图像和视频检验，确认用户身份，认证服务模块形成一条包含认证结果的5G消息，通过MAAP接口发送到5G消息服务器，5G消息服务器将包含认证结果的5G消息转发给用户手机上的5G消息模块；同时，认证服务模块通过认证请求接口将认证结果反馈给APP服务器，APP服务器通知用户手机上的业务APP；

S4.3：认证服务模块生成一条5G MAAP卡片消息，通过MAAP接口发送给5G消息服务器，5G消息服务器转发给手机的5G消息模块，询问用户是否允许运营商获取用户动态信息进行安全检查，用户将选择结果通过5G消息发送给认证服务模块；如果用户允许运营商获取用户动态信息进行安全检查，则进入步骤S4.4；如果用户不允许运营商获取用户动态信息进行安全检查，则进行静态信息认证；

S4.4：认证服务模块从用户信息数据库中获取用户动态数据，判断用户行为是否异常，并将结果通过认证请求接口发送给APP服务器，APP服务器将结果反馈给业务APP。

[0008] 进一步地，步骤S4中，所述远端认证具体为：

认证服务模块将敏感信息通过运营商认证服务器的远端认证接口转发给第三方认证服务器，第三方认证服务器对敏感信息进行认证，并将结果通过远端认证接口反馈给认证服务模块，认证服务模块将认证结果通过认证请求接口反馈给APP服务器，APP服务器通知用户手机上的业务APP。

[0009] 本发明还提出了一种通过5G消息进行敏感信息认证的系统，包括：5G手机、APP服务器、运营商认证服务器、5G消息服务器和第三方认证服务器；

所述5G手机包括业务APP和5G消息模块，业务APP和5G消息模块完全隔离；业务APP用于采集用户姓名、手机号和非完整身份证号，向运营商认证服务器发起认证请求；5G消息模块用于接收运营商认证服务器下发的采集敏感信息的请求，将用户上传的敏感信息发送给5G消息服务器，解析认证结果展示给5G手机终端用户；

所述5G消息服务器包括数据转发模块和MAAP模块；对于上行5G消息，数据转发模块将5G手机中的5G消息模块发送的5G消息转发给MAAP模块，MAAP模块将5G消息发送给运营商认证服务器；对于下行5G消息，运营商认证服务器将下行消息发送给MAAP模块，MAAP模块将其发送给5G手机中的5G消息模块；

所述运营商认证服务器包括认证请求接口、认证服务模块、MAAP接口、用户信息数据库和远端认证接口；认证请求接口接收APP服务器发送的认证请求和基本认证信息，并检查APP厂商和运营商是否有合约，通知认证服务器进行基本信息认证，并接收认证结果返回给APP服务器；MAAP接口和5G消息服务器的MAAP模块交互，收发5G消息；

所述远端认证接口向第三方认证服务器发送远端认证请求，接收远端认证的结

果,并反馈给认证服务模块。

[0010] 为优化上述技术方案,采取的具体措施还包括:

进一步地,所述用户信息数据库包括入网登记信息和动态数据;所述入网登记信息包括姓名、性别、身份证号和身份证照片;所述动态数据包括是否长期关机后在异地突然开机、用户历史位置轨迹、用户手机当前注册基站位置。

[0011] 进一步地,所述认证服务模块根据认证业务类型判断需要进行静态信息认证、动态信息认证还是远端认证;如果需要进行静态信息认证,认证服务模块根据用户的手机号从用户信息数据库调取入网登记信息,与用户在APP输入的姓名和不完整身份证号进行比对,如果不符合则认证失败,如果符合则要求用户通过5G消息上传身份证照片和活体检验媒体并进行检验;如果需要进行动态信息认证,认证服务模块在征得用户允许的情况下,根据用户信息数据库中的动态数据,判断用户行为是否异常,将结果反馈给APP服务器;如果需要远端认证,认证服务模块通过远端认证接口调用第三方认证服务器进行远端认证。

[0012] 本发明还提出了一种计算机可读存储介质,存储有计算机程序,所述计算机程序使计算机执行如上所述的通过5G消息进行敏感信息认证的方法。

[0013] 本发明的有益效果是:

(1)发起认证的APP需要事先与运营商签合约,且用于认证的敏感信息只经过运营商5G网络,APP无法获取用户的敏感信息,敏感信息难以被攻击和窃取;

(2)对于APP开发厂商而言,开发成本更低;在APP服务器侧,无需对接多家银行或者公安等系统,也无需采购第三方接口,不需要进行集成,只需要和运营商通过一个简单的HTTP接口就可以获得认证结果;对于APP侧,无需集成图像和视频采集功能;

(3)对于贷款等经济行为的认证,通过结合运营商存储的动态信息,判断用户是否可能存在被绑架到偏僻位置强迫进行认证的风险,或者诱骗到传销组织的可能,可以一定程度上评判用户行为是否异常。

## 附图说明

[0014] 图1为本认证方法的整体流程图;

图2为典型的5G MAAP卡片消息示意图;

图3a为向用户发起认证时的用户交互界面图;

图3b为展示认证结果的用户交互界面图;

图4为远端认证流程图;

图5为动态信息认证流程图;

图6为本认证系统结构示意图;

图7为业务APP和5G消息模块关系示意图;

图8为攻击者窃取信息示意图;

图9为5G消息服务器结构图;

图10为运营商认证服务器结构图。

## 具体实施方式

[0015] 现在结合附图对本发明作进一步详细的说明。

[0016] 在一实施例中，本发明提出了一种通过5G消息进行敏感信息认证的方法，该方法的整体流程图如图1所示，具体包括以下步骤：

步骤1：业务APP对用户发起认证，要求用户输入基本认证信息，如姓名，手机号，非完整身份证号，例如前三位加后四位，再把基本认证信息上传到APP服务器。

[0017] 步骤2：APP服务器将基本认证信息转发给运营商认证服务器的认证请求接口，认证请求接口检查APP厂商和运营商是否有合约，如果有则转发给认证服务模块，如果没有则给APP服务器直接返回错误的提示。

[0018] 步骤3：认证服务模块根据用户手机号获取用户静态信息，和用户输入信息进行比对，如果符合则认证成功，进入步骤4；如果认证失败，则通过认证请求接口通知APP服务器认证失败。

[0019] 步骤4：认证服务模块构建一条5G MAAP卡片消息，包含发起认证的APP信息，需要用户上传的信息，如身份证，银行卡正反面照片，活体检验媒体(转头、点头和读出某串数字等)，通过MAAP接口，5G消息服务器，到达用户手机的5G消息模块。

[0020] 一个典型的5G MAAP卡片消息如图2所示。5G消息支持文字、图像、语音、视频、地理位置等信息的下行上传，为敏感信息认证提供了足够的技术手段；5G消息的MAAP系统类似于企业公众号或者行业短信，但是审批更加严格，提供了一个高度安全的号码识别保障，每一个号码由一个企业的chatbot提供具体业务，如10000代表中国电信，10086代表中国移动，这些号码无法被仿冒，用户向这些号码发送的5G消息无法轻易被拦截窃听；使用5G消息不需要额外安装APP，保证了用户使用的便捷性；用户在运营商都有高度可信的基础认证信息可以作为参考，因此可以为各类外部APP提供实名认证服务；此外，一些用户动态信息，如号码使用时间，使用该号码的手机是否长时间没有开机，使用该号码的手机是否长期没有移动，用户当前位置等，都可以作为进一步的可信度参考，在征得用户同意的情况下，为更敏感的认证如金融贷款类服务提供进一步诚信和安全依据。

[0021] 在本实施例中，用户使用中国电信的号码，选择中国电信作为实名认证的实施方。

[0022] 中国电信向用户发送5G消息，提示Example APP委托中国电信进行实名认证，让用户选择是否接受，如图3a所示。

[0023] 步骤5：用户阅读这条5G MAAP卡片消息后，按照规定拍摄用于进一步认证的敏感信息。

[0024] 步骤6：敏感信息经过5G消息服务器，MAAP接口，最终被送到认证服务模块。

[0025] 步骤7：认证服务模块通过图像、视频检验，确认用户身份。

[0026] 步骤8：认证服务模块形成一条包含认证结果的5G消息，通过MAAP接口发送到5G消息服务器，5G消息服务器转发到用户手机5G消息模块，5G消息模块通过手机展示认证结果给用户，如图3b所示。

[0027] 步骤9：认证服务模块通过认证请求接口将认证结果发送到APP服务器，APP服务器将认证结果送到用户手机上的APP。

[0028] 当认证业务涉及到银行或公安的数据库，需要用到第三方认证服务器进行远端认证；远端认证的流程图如图4所示。

[0029] 在本实施例中以银行服务器作为第三方认证服务器为例，远端认证的具体步骤如下：

步骤1:认证服务模块识别银行卡上的银行名称和卡号;

步骤2:认证服务模块将用户姓名、身份证号、银行名称和银行卡号发送给远端认证接口;

步骤3:远端认证接口根据银行名称,将相关信息发送给对应银行的认证服务器,即图4中的第三方认证服务器进行认证;

步骤4:第三方认证服务器将认证结果返回给远端认证接口;

步骤5:远端认证接口将认证结果返回给认证服务模块;

后续流程同静态信息认证流程。

[0030] 当涉及到贷款等金融业务,还需要结合动态信息认证;动态信息认证的流程图如图5所示,具体步骤如下:

步骤1:认证服务模块生成一条5G MAAP卡片消息,询问用户是否允许运营商获取用户动态信息进行安全检查,之后通过MAAP接口和5G消息服务器到达5G手机上的5G消息模块;

步骤2:用户选择允许或者拒绝,生成一条包含选择结果的5G消息,通过5G消息服务器,MAAP接口到达认证服务模块;如果用户不同意,则动态信息认证失败,跳过步骤3和步骤4;

步骤3:如果用户同意,则从用户信息数据库获取用户动态信息;

步骤4:认证服务模块将返回的用户动态信息进行数据分析,判断用户行为是否异常。

[0031] 后续流程同静态信息认证流程。

[0032] 在另一实施例中,本发明提出了一种与通过5G消息进行敏感信息认证的方法相应的系统,该系统的整体结构如图6所示,上述系统包括:5G手机、APP服务器、运营商认证服务器、5G消息服务器和第三方认证服务器。

[0033] 5G手机包括业务APP和5G消息模块,业务APP和5G消息模块完全隔离,如图7所示;业务APP用于采集用户姓名、手机号和非完整身份证号,向运营商认证服务器发起认证请求;5G消息模块用于接收运营商认证服务器下发的采集敏感信息的请求,将用户上传的敏感信息发送给5G消息服务器,解析认证结果展示给5G手机终端用户;

传统的认证方式中,敏感信息会流入APP数据库中,外部攻击者很容易窃取这部分敏感信息,如图8所示;而本认证方法中,用户的敏感信息没有流入APP服务器,不存在信息泄密问题。

[0034] 5G消息服务器的结构如图9所示,包括数据转发模块和MAAP模块;数据转发模块将5G消息模块发送的5G消息转发给MAAP模块,MAAP模块将5G消息发送给运营商认证服务器。

[0035] 运营商认证服务器的结构如图10所示,包括认证请求接口、认证服务模块、MAAP接口、用户信息数据库和远端认证接口;

认证请求接口接收APP服务器发送的认证请求和基本认证信息,并检查APP厂商和运营商是否有合约,通知认证服务器进行基本信息认证,并接收认证结果返回给APP服务器;MAAP接口和5G消息服务器的MAAP模块交互,收发5G消息;

认证服务模块根据认证业务类型判断需要进行静态信息认证、动态信息认证还是远端认证;如果需要进行静态信息认证,认证服务模块根据用户的手机号从用户信息数据

库调取入网登记信息,与用户在APP输入的姓名和不完整身份证号进行比对,如果不符合则认证失败,如果符合则要求用户通过5G消息上传身份证照片和活体检验媒体并进行检验;如果需要进行动态信息认证,认证服务模块在征得用户允许的情况下,根据用户信息数据库中的动态数据,判断用户行为是否异常,将结果反馈给APP服务器;如果需要远端认证,认证服务模块通过远端认证接口调用第三方认证服务器进行远端认证;

用户信息数据库包括入网登记信息和动态数据;所述入网登记信息包括姓名、性别、身份证号和身份证照片;所述动态数据包括是否长期关机后在异地突然开机、用户历史位置轨迹、用户手机当前注册基站位置;

远端认证接口向第三方认证服务器发送远端认证请求,接收远端认证的结果,并反馈给认证服务模块。

[0036] 在另一实施例中,本发明提出了一种计算机可读存储介质,存储有计算机程序,所述计算机程序使计算机执行如上所述的通过5G消息进行敏感信息认证的方法。

[0037] 在本申请所公开的实施例中,计算机存储介质可以是有形的介质,其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合使用的程序。计算机存储介质可以包括但不限于电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备,或者上述内容的任何合适组合。计算机存储介质的更具体示例会包括基于一个或多个线的电气连接、便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或快闪存储器)、光纤、便捷式紧凑盘只读存储器(CD-ROM)、光学储存设备、磁储存设备或上述内容的任何合适组合。

[0038] 本领域普通技术人员可以意识到,结合本申请所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以根据每个特定的应用使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。

[0039] 以上仅是本发明的优选实施方式,本发明的保护范围并不仅局限于上述实施例,凡属于本发明思路下的技术方案均属于本发明的保护范围。应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理前提下的若干改进和润饰,应视为本发明的保护范围。

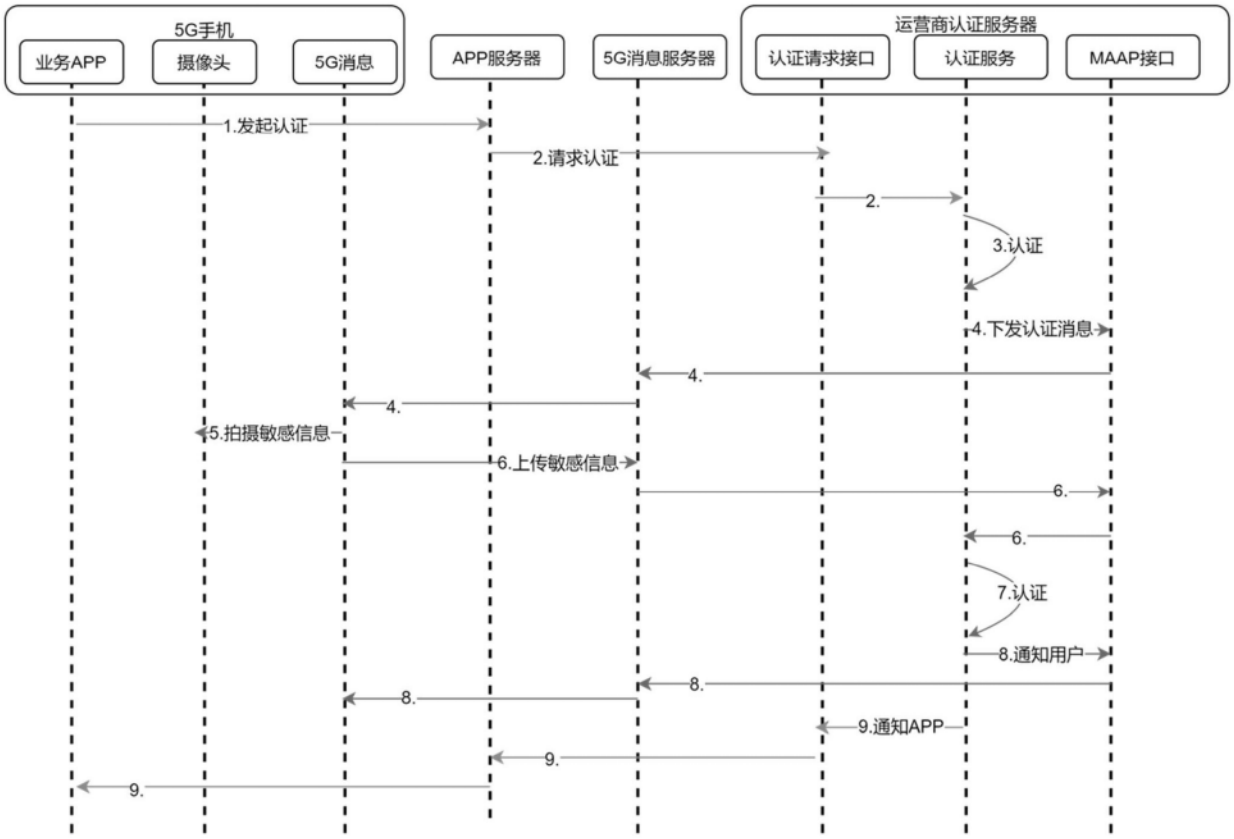

5G手机
业务APP
摄像头
5G消息
APP服务器
5G消息服务器
运营商认证服务器
认证请求接口
认证服务
MAAP接口
1.发起认证
2.请求认证
2.
3.认证
4.下发认证消息
4.
4.
5.拍摄敏感信息
6.上传敏感信息
6.
6.
7.认证
8.通知用户
8.
8.
9.通知APP
9.
9.

图1


17:22
行政服务中心
今天 15:57
你好
5G消息"赋能数智政务，创造信息服务新价值!图、文、声并茂，信息快、准、全! 南山区推出政务服务版"5G消息"，推动政务数字化转型，打造智能的政务服务窗口!欢迎您免费体验集政务服务申报、预约、取号、查询、咨询等服务为一体的南山政务服务"5G消息。
我要办事
我要取号
排队查询
进度查询
我要办事
政务地图
企业信息查询
咨询和反馈
≡ 阳光办事
≡ 亲清政企
≡ 我的主页
■ 统一显示实名认证logo、名称、服务号
■ 多媒体卡片式呈现效果
■ 内置按钮/悬浮按钮，与Chatbot对接，点击直接触发对应业务流程
■ 固定菜单可包含多个建议回复或建议操作按钮

图2


中国电信10000
星级服务
温馨提示
Example APP于2022年7月26日15时30分，委托中国电信对您名下的user账号进行实名认证，您是否接受
接受
拒绝
拨打110报警
07-26 11:23
您已接受Example APP于2022年7月26日15时30分，委托中国电信对您名下的user账号进行实名认证，请上传身份证正反面照片。
07-26 11:26
输入内容

图3a


中国电信10000
07-26 11:31
5G办理
信息确认
Example APP于2022年7月26日15时30分，委托中国电信对您名下的user账号进行实名认证，认证结果为姓名：XXX，性别X，身份证号XXX，是否正确
正确
不正确
拨打110报警
07-26 11:28
输入内容

图3b

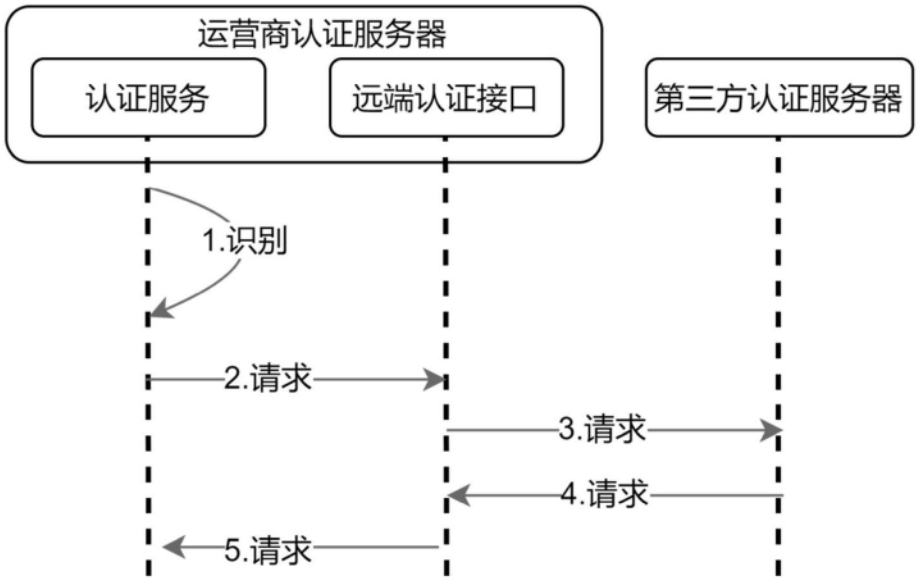

运营商认证服务器
认证服务
远端认证接口
第三方认证服务器
1.识别
2.请求
3.请求
4.请求
5.请求

图4

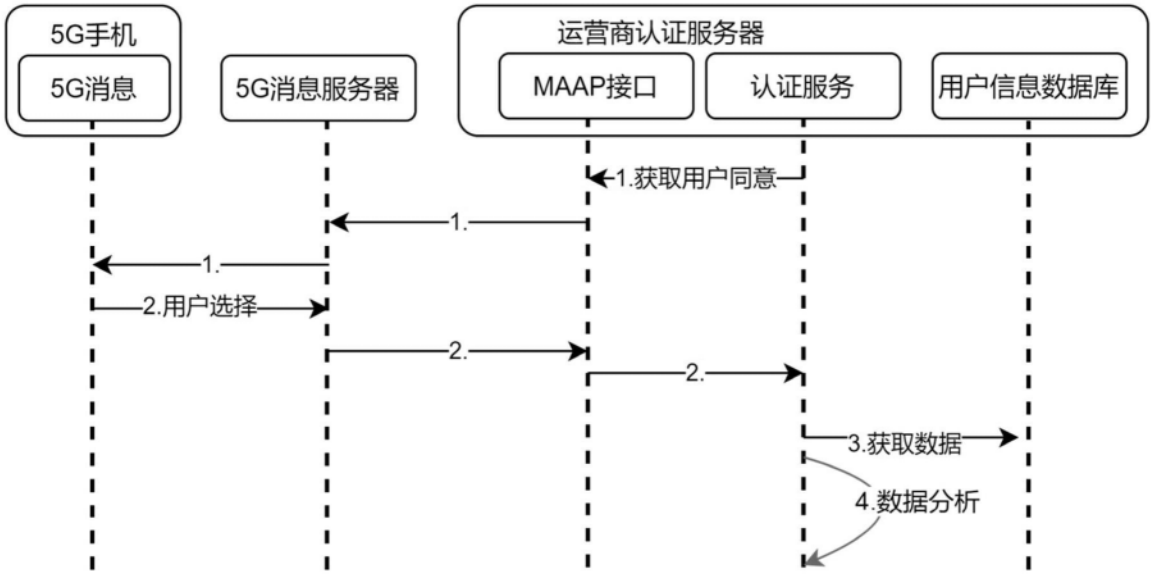

5G手机
5G消息
5G消息服务器
运营商认证服务器
MAAP接口
认证服务
用户信息数据库
1.获取用户同意
1.
1.
2.用户选择
2.
2.
3.获取数据
4.数据分析

图5

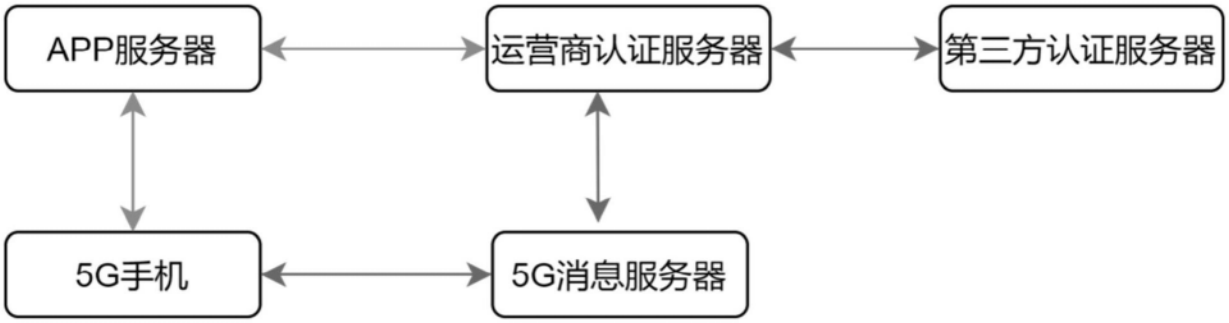

APP服务器
运营商认证服务器
第三方认证服务器
5G手机
5G消息服务器

图6

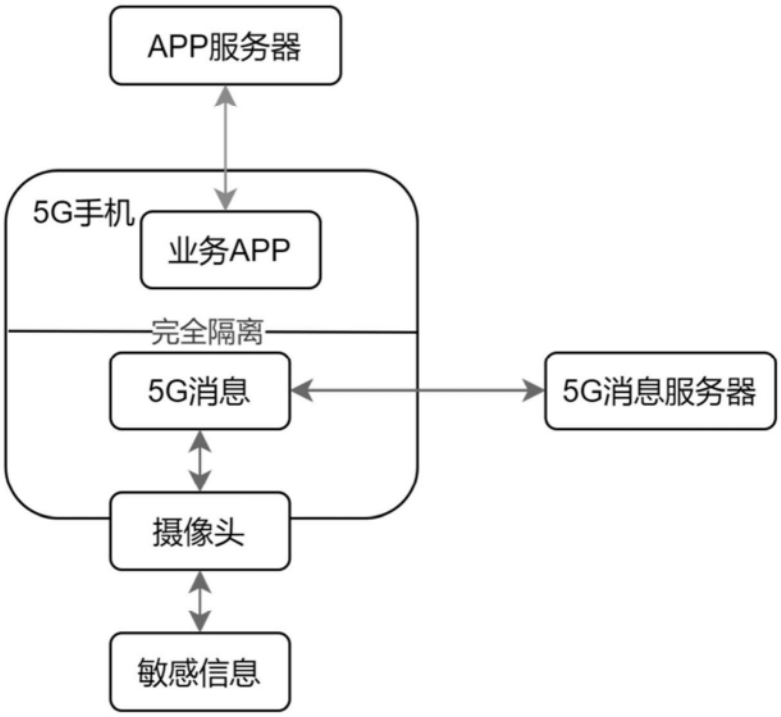

APP服务器
5G手机
业务APP
完全隔离
5G消息
5G消息服务器
摄像头
敏感信息

图7

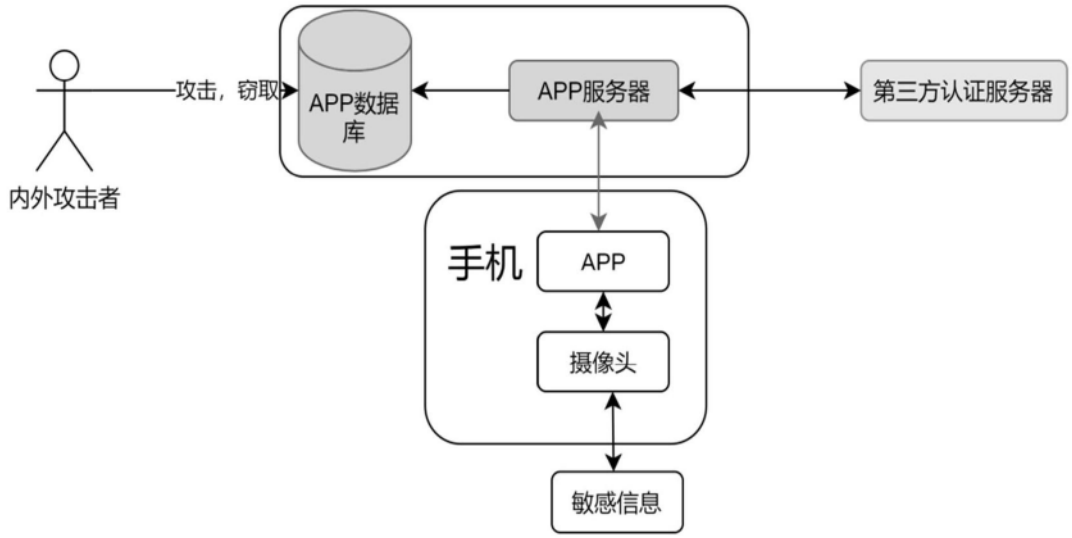

攻击，窃取
APP数据库
APP服务器
第三方认证服务器
内外攻击者
手机
APP
摄像头
敏感信息

图8

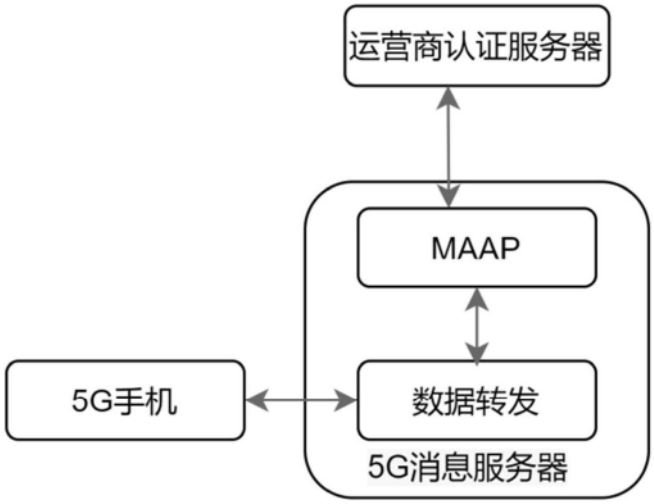

运营商认证服务器
MAAP
5G手机
数据转发
5G消息服务器

图9

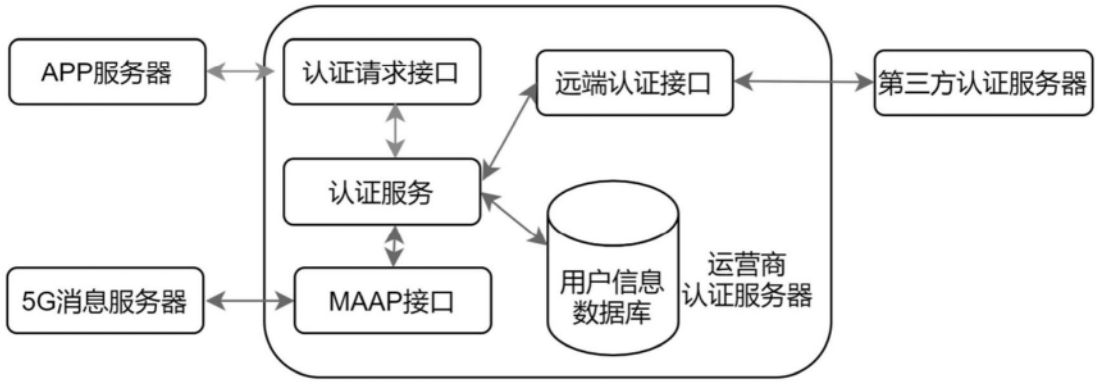

APP服务器
认证请求接口
远端认证接口
第三方认证服务器
认证服务
5G消息服务器
MAAP接口
用户信息
数据库
运营商
认证服务器

图10