(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110084064 B
(45)授权公告日 2020.05.19

(21)申请号 201910335491.8
(22)申请日 2019.04.24
(65)同一申请的已公布的文献号
申请公布号 CN 110084064 A
(43)申请公布日 2019.08.02
(73)专利权人 德萱(天津)科技发展有限公司
地址 300000 天津市西青区李七庄街凌奥创意产业园三期A栋515室
(72)发明人 不公告发明人
(51)Int.Cl.
*G06F 21/62*(2013.01)
(56)对比文件
CN 103368987 A,2013.10.23,
CN 104318153 A,2015.01.28,
CN 104850779 A,2015.08.19,
CN 103927476 A,2014.07.16,
审查员 王慧敏

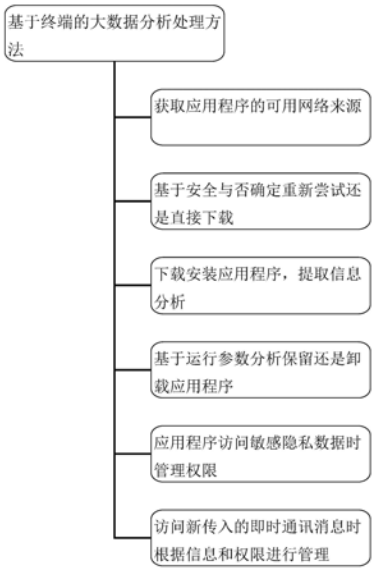
权利要求书4页 说明书17页 附图3页

(54)发明名称

基于终端的大数据分析处理方法及系统

(57)摘要

一种基于终端的大数据分析处理方法及系统,包括:查询应用程序并将标识可用网络来源的信息发送到判定服务器;基于判定结果,如果恶意则重新下载,安全则直接下载,待定则由用户选择:下载安装应用程序,提取信息并发送给判定服务器,基于分析结果确定保留还是卸载;执行应用程序时获取其运行参数分析,进一步确定保留还是卸载;再次确定保留该应用程序之后,在应用程序运行、访问终端上的敏感或隐私数据时进行权限管理以将其使能或禁止;接收新传入的即时通讯消息后当应用程序请求访问时,基于即时通讯消息包含的信息种类存储到不同数据库中,根据应用程序的读取权限和即时通讯消息的时间属性确定在规定时段内是否使能或禁止该应用程序的访问。




CN 110084064 B

1.一种基于终端的大数据分析处理方法,包括:

步骤S1,终端经由浏览器、通过无线网络搜索所需的应用程序,并获取含有可用应用程序的资源服务器的名称和/或IP信息,该名称和/或IP信息标识提供可用的应用程序下载的资源服务器;

步骤S2,终端将该资源服务器的名称和/或IP信息进行打包处理,发送给判定服务器进行恶意与否的确认;

步骤S3,判定服务器基于内置数据库中的涉及资源服务器的大数据进行判定和确认,并将结果通过无线链路返回给终端,终端根据判定服务器判定确认的恶意与否的结果执行对应操作:如果恶意则阻断与该资源服务器的通信链路并继续尝试步骤S1中获取的其它可用资源服务器且顺次执行步骤S2和S3,直到判定服务器确认非恶意或者尝试次数达到用户先前预设的次数;如果安全则直接下载该应用程序,如果待定则由用户选择是直接下载还是重新下载;

步骤S4,下载该应用程序后,终端直接安装或将开始安装按钮显示在显示器上由用户手动安装,安装该应用程序时赋予该应用程序最少的可用权限,完毕后提取该应用程序的信息,并对该应用程序进行签名处理,将提取的信息再次经由无线网络发送到判定服务器进行安全性认证;

步骤S5,终端根据判定服务器基于大数据的安全性认证结果,再次确定在终端中保留该应用程序还是卸载该应用程序;当保留该应用程序时,对该应用程序进行更新、并且添加或减少其对应的可用权限,而当卸载时将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库;

步骤S6,当该应用程序在终端上执行时,获取其运行参数并进行分析;

步骤S7,基于分析的结果再进一步确定在终端中保留该应用程序还是卸载该应用程序,并将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库;

步骤S8,当该应用程序请求访问终端上的用户隐私数据时,终端根据权限配置表确认其访问权限,并执行对应操作,其中该终端上的用户隐私数据在安装该应用程序之前进行了格式转换以增强其读取安全性;

步骤S9,当终端有新的即时通讯消息传入并且该应用程序请求访问时,终端基于新传入的即时通讯消息中包含时间属性而将新传入的即时通讯消息存储到不同数据库中,并确定该新传入的即时通讯消息中包含的信息的类别是否符合预设规则,同时基于应用程序的可用权限而在指定的时段内对该应用程序的访问进行使能或禁止;

其中:步骤S4进一步包括:在下载后终端安装该应用程序并提取其信息,对该应用程序进行签名处理,并将提取的信息发送到判定服务器进行安全性认证的步骤中,其中的终端在安装该应用程序的过程中,更改应用程序的文件后缀名以进行解压而得到其中包括的经过编译和工具打包形成的第一文件,获得变换工具以将包括类别名称的类别文件拷贝到第一目录位置,在第一目录位置处通过类别转换命令而生成应用程序中的分组数据;通过遍历分组数据的库函数而获取调取的函数,通过调取的函数的行为信息确定其行为属性,其中该行为信息包括访问行为信息、创建进程行为信息、操作进程行为信息、操作注册表行为信息、申请调取其它应用程序的标识符和权限的行为信息、安装行为信息、压缩打包行为信

息和移动数据传输行为信息，行为属性包括恶意与否；根据行为属性确定调取的函数的行为执行路径，将该执行路径进行记录，作为提取的信息的一部分，以在后续步骤中上传到判定服务器，通过将该执行路径的部分或全部与判定服务器中的基于字节码的路径大数据进行分析，进而进行安全性认证；其中终端对该应用程序进行签名处理的过程中，基于解压后的应用程序，获取应用程序中所有文件；将第一类型的文件用安全哈希算法计算摘要信息，并对该摘要信息进行编码，之后将编码值存入不同于第一类型的第二类型的第一文件中，以及将先前保存在第二类型的第一文件中的摘要信息和私钥信息生成一组签名信息并保存在第二类型的与第一文件不同的第二文件中的第一位置，将签名信息和公钥存入第二文件中的第二位置中，其中第一类型和第二类型涉及不同目录类型的文件；以及提取信息进一步包括：将应用程序的文件重命名为后缀名为压缩包形式的文件并进行解压，进而得到第一配置文件，使用第一开源软件将第一配置文件转换成可操作的文本格式；将使用第二开源软件反编译解压的结果中的二进制的源码文件；使用第三开源软件还原二进制的源码文件以获得该应用程序的文件的源码；基于应用程序的文件的源码，使用匹配算法将源码进行扫描，并对指定关键词进行统计，获取指定的各个关键词在类文件中的数量和对应位置并使用矩阵存储，基于距离算法计算每两个关键词之间的相似距离；基于相似距离对关键词分类，并将矩阵中的每个关键词作为根节点，把与各个节点之间相似度高的关键词聚合在一起，与存储对应位置的矩阵比对，去除不同类别的关键词，进而归类存储；将终端中的特征数据库中存储的安全应用程序的特征与归类存储的特征进行对比，去除该应用程序的特征中包含的安全特征以避免增加信息处理量并增加信息处理时间和功耗以及浪费终端有限的处理资源；将归类存储并去除特征的数据作为提取的信息的其它部分，与其它信息一起被发送到判定服务器进行安全性认证。

2.根据权利要求1所述的基于终端的大数据分析处理方法，其中：

步骤S5进一步包括：终端接收判定服务器基于大数据的安全性认证结果，并基于该结果进一步确定是否为恶意，当为恶意时卸载该应用程序，当为安全时在终端中保留该应用程序，而当待定时将风险提示信息在显示屏上展示给用户以供用户了解安全属性并选择卸载还是保留；当保留该应用程序时，对该应用程序赋予权限，该权限包括存储权限、拍照权限，麦克风使用的权限、录音权限、调用终端传感器的权限、读取和发送短消息权限、拨打电话权限、识别终端安装的SIM卡号码的权限、读取通信录的权限、读取用户运动数据的权限、开启移动运营商通信网络连接权限、开启无线保真连接权限、读取其它应用程序的权限、读取即时通讯软件的通信记录的权限，赋予权限包括赋予启用权限或者赋予禁用权限；当确定卸载时，将该应用程序的信息发送到判定服务器以更新判定服务器中用于大数据分析、判定和确认的数据库。

3.根据权利要求2所述的基于终端的大数据分析处理方法，其中：

步骤S6中，当该应用程序在终端上执行时，获取其运行参数并进行分析包括：执行应用程序，获取其运行过程中的行为参数，该行为参数包括系统API、文件权限的变化、进程和线程运行数据、网络访问请求数据、发送的网络数据，将该行为参数记录在日志文件中；监控应用程序中可移植的执行文件的创建操作，确定其创建主体，在终端存储器中建立可移植的执行文件与其创建主体间的对应关系；使用模拟工具自行运行和模拟终端用户的运行操作，以获得日志文件记录和网络数据分组文件记录；在模拟工具运行结束，并且在网络链路

开启接通和数据通信结束之后，将日志文件记录和网络数据分组文件记录存储在第一存储位置中；对日志文件记录和网络数据分组文件记录进行分析，其中使用特征提取对日志文件记录和网络数据分组文件记录的特征量化，将权限、API、URL和字符串转换成数值特征，使用基于均值和方差的特征选择算法选择特征的子集，结合分类和聚类以及标签构建规则对数值特征进行预测，基于该数值特征与预设配置文件中的参数的数值匹配而确定安装的该应用程序对于终端来说是否安全，并将其作为分析的结果的第一部分；当结果为安全或相反时，将应用程序中可移植的执行文件与其创建主体的对应关系作为分析的结果的第二部分，当为不安全即恶意时，另外将创建主体的相关信息进行标记以作为标识该应用程序会对终端造成影响的恶意标识信息并作为第二部分的补充部分，以供发送到判定服务器更新用于大数据分析、判定和确认的数据库，并且在终端进行记录并存储到安全信息数据库中以作为恶意的来源，在后续安装时可将该来源的应用程序作为来自恶意来源的应用程序而提供和显示给用户，供用户可选地对该来源进行彻底查杀并掐断该来源和来自其的所有应用程序的安装以及该来源对终端的任何访问请求；聚合结果的第一部分和分析的结果的第二部分以作为该应用程序的信息。

4.根据权利要求3所述的基于终端的大数据分析处理方法，其中：

步骤S6中，当该应用程序在终端上执行时，获取其运行参数并进行分析包括：当应用程序运行的同时移动网络也开启时，周期性地获取终端的流量数据，将应用程序收发的流量数据进行矢量化，提取其中的矢量片段，并存储到运行数据库中以供后续使用，同时截取某个时段内的多个矢量片段，将其与运行数据库中存储的历史矢量数据进行匹配，若与安全的历史矢量数据匹配则初步判定为非恶意应用程序行为，若与恶意的历史矢量数据匹配则初步判定为恶意应用程序行为，将得到的应用程序行为作为分析的结果。

5.根据权利要求3或4所述的基于终端的大数据分析处理方法，其中：

在步骤S7中，基于分析的结果进一步确定在终端中保留该应用程序还是卸载该应用程序，并将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库进一步包括：终端基于分析的结果的第一部分，当为安全的应用程序时保留该应用程序，而当为恶意时卸载该应用程序，并将包括分析的结果的第一部分和分析的结果的第二部分的应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库，其中为恶意时，分析的结果的第二部分还包括有将创建主体的相关信息进行标记以作为标识该应用程序会对终端造成影响的恶意标识信息的补充部分。

6.根据权利要求5所述的基于终端的大数据分析处理方法，其中：

在步骤S7中，在卸载应用程序之后，当终端启动网络通信时激活监控程序，进而使得该监控程序实时截取通过网络收发的数据，并将发送的数据宿和/或接收的数据源与之前确定的恶意的来源进行特征匹配，当符合匹配标准时将该结果显示给用户并分析待发送的数据所在的位置以及对该数据进行调用的实体的名称和位置，并将该调用的实体的名称和位置进行定点移除，之后显示移除成功与否的结果，如果不成功则重复上述移除操作并展示给用户移除进程，直到符合预设要求为止。

7.根据权利要求6所述的基于终端的大数据分析处理方法，其中：

分析待发送的数据所在的位置的同时还分析待发送的数据，以确定是否含有用户的账号、联系人、验证码、联系方式的信息，如果存在则将风险提示给用户。

8.一种基于终端的大数据分析处理系统,包括终端和判定服务器,其中终端包括:处理器,权限管理模块,解释引擎,消息分析模块,私密存储库,常规存储库;判定服务器内部设置有用于大数据分析、确认和判定的数据库;所述基于终端的大数据分析系统用于执行权利要求7所述的基于终端的大数据分析处理方法。

# 基于终端的大数据分析处理方法及系统

## 技术领域

[0001] 本发明涉及电数据处理领域，并且更具体而言，涉及一种基于终端的大数据分析处理方法及系统。

## 背景技术

[0002] 随着信息技术的快速发展，移动终端和高速移动网络为用户提供了丰富的信息和资源，用户在利用这些信息和资源工作、生活、娱乐的同时，也需要经由无线移动网络下载大量的应用程序到移动终端中。现今智能移动终端应用市场上有各种提高用户体验的应用程序，用户在享受便利的同时也带来了一系列安全问题。首先，网络逐步成为恶意应用程序传播的途径，从中下载、存储并安装到本地终端运行应用程序后，有些会恶意修改本地终端中的文件，造成系统瘫痪或者运行变慢，其次，还带来个人隐私泄露的风险，个人隐私包括用户的个人身份、银行账户、财务状况信息、行为偏好、健康情况，社会地位、社交记录等私人信息。应用程序及其关联的恶意网络资源或分析工具通过对单个用户的特定数据挖掘，大量而多样化的信息交集最终能够准确地描绘出该用户的轮廓，如个人年龄、经济状况、消费行为和等级、社会地位、社交圈等，进而催生出一些新的亟待解决的隐私风险及伦理安全问题。因此需要对安装的应用程序进行检测，如果存在恶意的企图则需要进行查杀，然而现有技术中的检测和查杀存在一系列问题。针对恶意应用程序的查杀，一般是检测出恶意程序后，删除恶意程序，以避免恶意程序执行恶意行为，但是无法追溯恶意程序的源头，因而无法对恶意程序的源头进行彻底查杀，断绝其源头。而且，对于恶意应用程序的分析包括静态分析和动态分析两种。静态分析简单快速，但是扫描前需要知道已知恶意应用程序的信息，如签名、行为模式、权限申请等。动态分析将应用程序运行在封闭环境中并监视，分析应用程序的行为特征，如文件权限改变、进程和线程运行情况、系统调用情况、网络访问情况等。但是无论是静态分析还是动态分析，其分析效率不够理想。另外，恶意的新安装的应用往往会试图访问终端的隐私信；尽管有的应用程序会有合法权限对用户的诸如传入的短消息服务之类的隐私信息的合法访问，但是现有技术缺少对机载已有用户隐私进行有效的文件保护，也缺乏对于隐私信息的访问的合理管理，从而导致安装的应用程序窃取用户的私密信息，进而导致用户的资产和隐私的泄漏，造成不可挽回的损失。

## 发明内容

[0003] 本发明的目的之一是提供一种基于终端的大数据分析处理方法及系统，其能够利用大数据和信息安全技术，在安装阶段对应用程序进行安全性检测，并且对终端有危害的应用程序进行拦截，并对其源头进行确认和阻断；并且针对应用程序对终端中用户隐私信息的合法或非法访问问题，对终端的隐私信息进行加密处理，对于合法访问，通过权限管理而进行隐私信息读取并且确保读取不超越预设权限，而对于非法访问，通过时间设置或者权限阻断设置而避免应用程序对隐私程序的不合理访问。本发明的基于终端的大数据分析处理方法及系统，可以基于大数据和权限管理实现系统的安全，并且最终保证应用程序在

终端上的下载、运行和数据访问的安全性。

[0004] 本发明为解决上述技术问题而采取的技术方案为:一种基于终端的大数据分析处理方法,包括:终端经由无线网络查询应用程序并将标识应用程序的可用网络来源的信息发送到判定服务器;终端基于判定服务器根据大数据获得的判定结果,如果恶意则确定重新尝试从其它可用资源下载,如果为安全则直接下载该应用程序,如果为待定则由用户确定风险等级后选择直接下载还是重新下载:终端下载并安装应用程序,提取该应用程序的信息并发送给判定服务器,基于判定服务器的分析结果,确定在终端保留还是卸载应用程序;终端执行应用程序时,获取其运行参数并进行分析,基于分析结果再进一步确定在终端中保留该应用程序还是卸载该应用程序;终端再次确定保留该应用程序之后,在应用程序运行、访问终端上的敏感或隐私数据时进行权限管理以将其使能或禁止;以及终端接收新传入的即时通讯消息之后并且当该应用程序请求访问该新传入的即时通讯消息时,基于新传入的新的即时通讯消息所包含的信息种类是否符合预设规定而存储到不同类别的数据库中,并且根据应用程序的读取权限和新传入的新的即时通讯消息的时间属性而确定在规定时段内是否使能或禁止该应用程序的访问。

[0005] 在一个实施例中,该方法进一步包括:步骤S1,终端经由浏览器、通过无线网络搜索所需的应用程序,并获取含有可用应用程序的资源服务器的名称和/或IP信息,该名称和/或IP信息标识提供可用的应用程序下载的资源服务器;步骤S2,终端将该资源服务器的名称和/或IP信息进行打包处理,发送给判定服务器进行恶意与否的确认;步骤S3,判定服务器基于内置数据库中的涉及资源服务器的大数据进行判定和确认,并将结果通过无线链路返回给终端,终端根据判定服务器判定确认的恶意与否的结果执行对应操作:如果恶意则阻断与该资源服务器的通信链路并继续尝试步骤S1中获取的其它可用资源服务器且顺次执行步骤S2和S3,直到判定服务器确认非恶意或者尝试次数达到用户先前预设的次数;如果安全则直接下载该应用程序,如果待定则由用户选择是直接下载还是重新下载;步骤S4,下载该应用程序后,终端直接安装或将开始安装按钮显示在显示器上由用户手动安装,安装该应用程序时赋予该应用程序最少的可用权限,完毕后提取该应用程序的信息,并对该应用程序进行签名处理,将提取的信息再次经由无线网络发送到判定服务器进行安全性认证;步骤S5,终端根据判定服务器基于大数据的安全性认证结果,再次确定在终端中保留该应用程序还是卸载该应用程序;当保留该应用程序时,对该应用程序更新并添加或减少其对应的可用权限,而当卸载时将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库;步骤S6,当该应用程序在终端上执行时,获取其运行参数并进行分析;步骤S7,基于分析的结果再进一步确定在终端中保留该应用程序还是卸载该应用程序,并将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库;步骤S8,当该应用程序请求访问终端上的用户隐私数据时,终端根据权限配置表确认其访问权限,并执行对应操作,其中该终端上的用户隐私数据在安装该应用程序之前进行了格式转换以增强其读取安全性;步骤S9,当终端有新的即时通讯消息传入并且该应用程序请求访问时,终端基于该新传入的即时通讯消息中包含时间属性而将新传入的即时通讯消息存储到不同数据库中,并确定该新传入的即时通讯消息中包含的信息的类别是否符合预设规则,同时基于应用程序的可用权限而在指定的时段内对该应用程序的访问进行使能或禁止。

[0006] 在一个实施例中，步骤S4进一步包括：在下载后终端安装该应用程序并提取其信息，对该应用程序进行签名处理，并将提取的信息发送到判定服务器进行安全性认证的步骤中，其中的终端在安装该应用程序的过程中，更改应用程序的文件后缀名以进行解压而得到其中包括的经过编译和工具打包形成的第一文件，获得变换工具以将包括类别名称的类别文件拷贝到第一目录位置，在第一目录位置处通过类别转换命令而生成应用程序中的分组数据；通过遍历分组数据的库函数而获取调取的函数，通过调取的函数的行为信息确定其行为属性，其中该行为信息包括访问行为信息、创建进程行为信息、操作进程行为信息、操作注册表行为信息、申请调取其它应用程序的标识符和权限的行为信息、安装行为信息、压缩打包行为信息和移动数据传输行为信息，而行为属性包括恶意与否；根据行为属性确定调取的函数的行为执行路径，将该执行路径进行记录，作为提取的信息的一部分，以在后续步骤中上传到判定服务器，通过将该执行路径的部分或全部与判定服务器中的基于字节码的路径大数据进行分析，进而进行安全性认证；其中终端对该应用程序进行签名处理的过程中，基于解压后的应用程序，获取应用程序中所有文件；将第一类型的文件用安全哈希算法计算摘要信息，并对该摘要信息进行编码，之后将编码值存入不同于第一类型的第二类型的第一文件中，以及将先前保存在第二类型的第一文件中的摘要信息和私钥信息生成一组签名信息并保存在第二类型的与第一文件不同的第二文件中的第一位置，将签名信息和公钥存入第二文件中的第二位置中，其中第一类型和第二类型涉及不同目录类型的文件；以及提取信息进一步包括提取信息的其它部分，即：将应用程序的文件重命名为后缀名为压缩包形式的文件并进行解压，进而得到第一配置文件，使用第一开源软件将第一配置文件转换成可操作的文本格式；将使用第二开源软件反编译解压的结果中的二进制的源码文件；使用第三开源软件还原二进制的源码文件以获得该应用程序的文件的源码；基于应用程序的文件的源码，使用匹配算法将源码进行扫描，并对指定关键词进行统计，获取指定的各个关键词在类文件中的数量和对应位置并使用矩阵存储，基于距离算法计算每两个关键词之间的相似距离；基于相似距离对关键词分类，并将矩阵中的每个关键词作为根节点，把与各个节点之间相似度高的关键词聚合在一起，与存储的所在的位置的矩阵比对，去除不同类别的关键词，进而归类存储；将终端中的特征数据库中存储的安全应用程序的特征与归类存储的特征进行对比，去除该应用程序的特征中包含的安全特征以避免增加信息处理量并增加信息处理时间和功耗以及浪费终端有限的处理资源；将归类存储并去除特征的数据作为提取的信息的其它部分，与其它信息一起被发送到判定服务器进行安全性认证。

[0007] 在一个实施例中，步骤S5进一步包括：终端接收判定服务器基于大数据的安全性认证结果，并基于该结果进一步确定是否为恶意，当为恶意时卸载该应用程序，当为安全时在终端中保留该应用程序，而当待定时将风险提示信息在显示屏上展示给用户以供用户了解安全属性并选择卸载还是保留；当保留该应用程序时，对该应用程序赋予权限，该权限包括存储权限、拍照权限，麦克风使用的权限、录音权限、调用终端传感器的权限、读取和发送短消息权限、拨打电话权限、识别终端安装的SIM卡号码的权限、读取通信录的权限、读取用户运动数据的权限、开启移动运营商通信网络连接权限、开启无线保真连接权限、读取其它应用程序的权限、读取即时通讯软件的通信记录的权限，赋予权限包括赋予启用权限或者赋予禁用权限；当确定卸载时，将该应用程序的信息发送到判定服务器以更新判定服务器中用于大数据分析、判定和确认的数据库。

[0008] 在一个实施例中，步骤S6中，当该应用程序在终端上执行时，获取其运行参数并进行分析包括：执行应用程序，获取其运行过程中的行为参数，该行为参数包括系统API、文件权限的变化、进程和线程运行数据、调用数据、网络访问请求数据、发送的网络数据，将该行为参数记录在日志文件中；监控应用程序中可移植的执行文件的创建操作，确定其创建主体，在终端存储器中建立可移植的执行文件与其创建主体间的对应关系；使用模拟工具自行运行和模拟终端用户的运行操作，以获得日志文件记录和网络数据分组文件记录；在模拟工具运行结束，并且在网络链路开启接通和随着时间的流逝而数据通信结束之后，将日志文件记录和网络数据分组文件记录存储在第一存储位置中；对日志文件记录和网络数据分组文件记录进行分析，其中使用特征提取对日志文件记录和网络数据分组文件记录的特征量化，将权限、API、URL和字符串转换成数值特征，使用采用基于均值和方差的特征选择算法选择特征的子集，结合分类和聚类以及标签构建规则对数值特征进行预测，基于该数值特征与预设配置文件中的参数的数值匹配而确定其运行行为属性，即安装的该应用程序对于终端来说是否安全，并将其作为分析的结果的第一部分；当结果为安全或相反时，将应用程序中可移植的执行文件与其创建主体的对应关系作为分析的结果的第二部分，当为不安全即恶意时，另外将创建主体的相关信息进行标记以作为标识该应用程序会对终端造成影响的恶意标识信息并作为第二部分的补充部分，以供发送到判定服务器更新大数据分析判定和确认的数据库，并且在终端进行记录并存储到安全信息数据库中以作为恶意的来源，在后续安装时可将该来源的应用程序作为来自恶意来源的应用程序而提供和显示给用户，供用户可选地对该源头进行彻底查杀并掐断该源头和来自其的所有应用程序的安装以及该源头对终端的任何访问请求；聚合分析的结果的第一部分和分析的结果的第二部分以作为该应用程序的信息。

[0009] 在一个实施例中，步骤S6中，当该应用程序在终端上执行时，获取其运行参数并进行分析包括：当应用程序运行的同时移动网络也开启时，周期性地获取终端的流量数据，将应用程序收发的流量数据进行矢量化，提取其中的矢量片段，并存储到运行数据库中以供后续使用，同时截取某个时段内的多个矢量片段，将其与运行数据库中存储的历史矢量数据进行匹配，若与安全的历史矢量数据匹配则初步判定为非恶意应用程序行为，若与恶意的历史矢量数据匹配则初步判定为恶意应用程序行为，将得到的应用程序行为作为分析的结果。

[0010] 在一个实施例中，在步骤S7中，基于分析的结果进一步确定在终端中保留该应用程序还是卸载该应用程序，并将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库进一步包括：终端基于分析的结果的第一部分，当为安全的应用程序时保留该应用程序，而当为恶意时卸载该应用程序，并将包括分析的结果的第一部分和分析的结果的第二部分的应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库，其中为恶意时，分析的结果的第二部分还包括有将创建主体的相关信息进行标记以作为标识该应用程序会对终端造成影响的恶意标识信息的补充部分。在卸载应用程序之后，当终端启动网络通信时激活监控程序，进而使得该监控程序实时截取通过网络收发的数据，并将发送的数据宿和/或接收的数据源与之前确定的恶意的来源进行特征匹配，当符合匹配标准时将该结果显示给用户并分析待发送的数据所在的位置以及对该数据进行调用的实体的名称和位置，并将该调用的实体的名称和位置进行定点移除，之后显

示移除成功与否的结果，如果不成功则重复上述移除操作并展示给用户移除进程，直到符合预设要求为止。分析待发送的数据所在的位置的同时还分析待发送的数据，以确定是否含有用户的账号、联系人、验证码、联系方式的信息，如果存在则将风险提示给用户。

[0011] 本发明的目的之二是提供一种基于终端的大数据分析处理系统，包括终端和判定服务器，其中终端包括：处理器，权限管理模块，解释引擎，消息分析模块，私密存储库，常规存储库；判定服务器内部设置有用于大数据分析、确认和判定的数据库；所述基于终端的大数据分析处理系统执行前述的基于终端的大数据分析处理方法。

## 附图说明

[0012] 在附图中通过实例的方式而不是通过限制的方式来示出本发明的实施例，其中相同的附图标记表示相同的元件，其中：

[0013] 根据本发明的示范性实施例，图1图示一种基于终端的大数据分析处理方法的简要流程图。

[0014] 根据本发明的示范性实施例，图2图示图1的一种基于终端的大数据分析处理方法的具体实现的流程图。

[0015] 根据本发明的示范性实施例，图3图示一种基于终端的大数据分析处理系统。

## 具体实施方式

[0016] 在进行以下具体实施方式之前，阐述贯穿本专利文档所使用的某些词语和短语的定义可能是有利的：术语“包括”和“包含”及其派生词意味着包括而没有限制；术语“或”是包含的，意味着和/或；短语“与...相关联”、“与其相关联”及其派生词可能意味着包括，被包括在...内，与...互连，包含，被包含在...内，连接到...或与...连接，耦合到...或与...耦合，可与...通信，与...合作，交织，并列，接近...，被绑定到...或与...绑定，具有，具有...的属性，等等；而术语“控制器”意味着控制至少一个操作的任何设备、系统或其部件，这样的设备可能以硬件、固件或软件或者其中至少两个的一些组合来实现。应当注意的是：与任何特定的控制器相关联的功能性可能是集中式或分布式的，无论是本地还是远程。贯穿本专利文档提供用于某些词语和短语的定义，本领域技术人员应当理解：如果不是大多数情况下，在许多情况下，这样的定义适用于现有的以及这样定义的词语和短语的未来使用。

[0017] 在下面的描述中，参考附图并以图示的方式示出几个具体的实施例。将理解的是：可设想并且可做出其他实施例而不脱离本公开的范围或精神。因此，以下详细描述不应被认为具有限制意义。

[0018] 根据本发明的示范性实施例，图1图示一种基于终端的大数据分析处理方法的简要流程图。该方法包括以下步骤：

[0019] (A)终端经由无线网络查询应用程序并将标识应用程序的可用网络来源的信息发送到判定服务器；

[0020] (B)终端基于判定服务器根据大数据获得的判定结果，如果恶意则确定重新尝试从其它可用资源下载，如果为安全则直接下载该应用程序，如果为待定则由用户确定风险等级后选择直接下载还是重新下载：

[0021] (C)终端下载并安装应用程序，提取该应用程序的信息并发送给判定服务器，基于判定服务器的分析结果，确定在终端保留还是卸载应用程序；

[0022] (D)终端执行应用程序时，获取其运行参数并进行分析，基于分析结果再进一步确定在终端中保留该应用程序还是卸载该应用程序；

[0023] (E)终端再次确定保留该应用程序之后，在应用程序运行、访问终端上的敏感或隐私数据时进行权限管理以将其使能或禁止；以及

[0024] (F)终端接收新传入的即时通讯消息之后并且当该应用程序请求访问该新传入的即时通讯消息时，基于新传入的新的即时通讯消息所包含的信息种类是否符合预设规定而存储到不同类别的数据库中，并且根据应用程序的读取权限和新传入的新的即时通讯消息的时间属性而确定在规定时段内是否使能或禁止该应用程序的访问。

[0025] 根据本发明的示范性实施例，图2图示图1的一种基于终端的大数据分析处理方法的具体实现的流程图。该方法进一步包括以下步骤：

[0026] 步骤S1，终端经由浏览器、通过无线网络搜索所需的应用程序，并获取含有可用应用程序的资源服务器的名称和/或IP信息，该名称和/或IP信息标识提供可用的应用程序下载的资源服务器；

[0027] 步骤S2，终端将该资源服务器的名称和/或IP信息进行打包处理，发送给判定服务器进行恶意与否的确认；

[0028] 步骤S3，判定服务器基于内置数据库中的涉及资源服务器的大数据进行判定和确认，并将结果通过无线链路返回给终端，终端根据判定服务器判定确认的恶意与否的结果执行对应操作：如果恶意则阻断与该资源服务器的通信链路并继续尝试步骤S1中获取的其它可用资源服务器且顺次执行步骤S2和S3，直到判定服务器确认非恶意或者尝试次数达到用户先前预设的次数；如果安全则直接下载该应用程序，如果待定则由用户选择是直接下载还是重新下载；

[0029] 步骤S4，下载该应用程序后，终端直接安装或将开始安装按钮显示在显示器上由用户手动安装，安装该应用程序时赋予该应用程序最少的可用权限，完毕后提取该应用程序的信息，并对该应用程序进行签名处理，将提取的信息再次经由无线网络发送到判定服务器进行安全性认证；

[0030] 步骤S5，终端根据判定服务器基于大数据的安全性认证结果，再次确定在终端中保留该应用程序还是卸载该应用程序；当保留该应用程序时，对该应用程序更新并添加或减少其对应的可用权限，而当卸载时将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库；

[0031] 步骤S6，当该应用程序在终端上执行时，获取其运行参数并进行分析；

[0032] 步骤S7，基于分析的结果再进一步确定在终端中保留该应用程序还是卸载该应用程序，并将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库；

[0033] 步骤S8，当该应用程序请求访问终端上的用户隐私数据时，终端根据权限配置表确认其访问权限，并执行对应操作，其中该终端上的用户隐私数据在安装该应用程序之前进行了格式转换以增强其读取安全性；

[0034] 步骤S9，当终端有新的即时通讯消息传入并且该应用程序请求访问时，终端基于

该新传入的即时通讯消息中包含时间属性而将新传入的即时通讯消息存储到不同数据库中，并确定该新传入的即时通讯消息中包含的信息的类别是否符合预设规则，同时基于应用程序的可用权限而在指定的时段内对该应用程序的访问进行使能或禁止。

[0035] 根据以上所述的基于终端的大数据分析处理方法，能够利用大数据和信息安全技术，在安装阶段对应用程序进行安全性检测，并且对终端有危害的应用程序进行拦截，并对其源头进行确认和阻断；并且针对应用程序对于终端中用户隐私信息的合法或非法访问问题，通过合理管理而进行隐私信息读取并且确保读取不超越预设权限，或者通过设置避免应用程序对隐私程序的不合理访问，进而基于大数据和权限管理实现系统的安全。

[0036] 优选地，步骤S1进一步包括：直接经由终端安装的浏览器，通过输入期望的应用程序的名称，通过搜索引擎进行搜索；或者在当前的非浏览器应用中，通过用户手指长按屏幕，在屏幕上出现选择文字的选项，用户通过选择和高亮应用程序的全部或部分名称，并在选定后点击屏幕上出现的搜索按钮，通过点击该搜索按钮而出现一个或多个浏览器的选择图标以供选择，在选择对应的浏览器图标后进行搜索；或者在当前的非浏览器应用中，通过选择该非浏览器应用中的搜索图标，在屏幕上出现输入框，通过输入期望的应用程序名称后，该非浏览器应用要么直接调用默认的第三方浏览器进行搜索，要么出现一个或多个浏览器的选择图标以供选择并且在选择对应的浏览器图标后进行搜索；或者在内嵌有浏览器的即时通讯应用中，要么通过用户手指长按屏幕并在屏幕上出现选择文字的选项，通过选择和高亮应用程序的全部或部分名称并在选定后点击屏幕上出现的搜索按钮而调用嵌入的浏览器进行搜索，要么通过选择该非浏览器应用中的搜索图标而在屏幕上出现输入框，通过输入期望的应用程序名称而调用嵌入的浏览器进行搜索。在经由无线网络搜索所需的应用程序之后，根据结果获取用于标识含有应用程序的资源服务器的名称和/或IP地址。

[0037] 优选地，步骤S2进一步包括：终端选择该资源服务器的名称和/或IP信息中的任一者或两者，并将其以固定的包传输格式打包在待传输的包中，并将包的报头设置为请求属性，在待传输的包中的名称和/或IP信息中的任一者或两者之后通过固定的结束符终止，以便于判定服务器识别，之后将该包通过无线链路发送到判定服务器，以供进行恶意与否的确认。

[0038] 优选地，步骤S3进一步包括：判定服务器内部设置有用于大数据分析、确认和判定的数据库，该数据库存储有用于终端的应用程序的安全属性信息，包括恶意、安全和待定，该安全属性信息随着时间的流逝而进行更新，其更新方式通过用户上传、信息中心通知等方式中的任一种而进行；判定服务器接收终端传输的包，并基于预设的拆分包规则，提取包中的资源服务器的名称和/或IP信息中的任一者或两者，并将其输入到内部设置的数据库，以进行信息匹配，当有符合安全或恶意的匹配项以及无匹配而被确认为待定时，将该明确和待定的安全属性信息的结果进行打包，经由无线链路发送到终端；终端接收该包并拆分包，提取其中的安全属性信息，如果为恶意则阻断与该资源服务器的通信链路，并继续尝试步骤S1中获取的其它资源服务器且顺次执行步骤S2和S3，直到判定服务器确认非恶意或者尝试次数达到用户预设次数；如果是安全则由用户选择是否下载该应用程序：如果是安全则由用户选择是否下载或直接下载该应用程序，其中如果是安全则直接下载该应用程序，而如果是待定则由用户选择是否下载该应用程序，若下载则进行后续步骤，若不下载则确定直接退出该方法还是继续尝试步骤S1中获取的其它资源服务器且顺次执行步骤S2和S3

直到判定服务器确认符合用户期望的安全属性或尝试次数达到用户预设次数。其中判定服务器内部设置的用于大数据分析、确认和判定的数据库所存储的待定的安全属性的确定方法为:基于终端将包通过无线链路发送到判定服务器后,在数据库开始确定安全属性信息的时刻,将数据库中涉及该应用的安全属性的恶意类别占数据库中该应用程序的所有记录的比例小于第一阈值,并且安全属性的安全类别占数据库中该应用程序的所有记录的比例小于第二阈值时,将数据库所存储的该应用程序的安全属性确定为待定。

[0039] 优选地,步骤S4进一步包括:在下载后终端安装该应用程序并提取其信息,对该应用程序进行签名处理,并将提取的信息发送到判定服务器进行安全性认证的步骤中,其中的终端在安装该应用程序的过程中,更改应用程序的文件后缀名以进行解压而得到其中包括的经过编译和工具打包形成的第一文件,获得变换工具以将包括类别名称的类别文件拷贝到第一目录位置,在第一目录位置处通过类别转换命令而生成应用程序中的分组数据;通过遍历分组数据的库函数而获取调取的函数,通过调取的函数的行为信息确定其行为属性,其中该行为信息包括访问行为信息、创建进程行为信息、操作进程行为信息、操作注册表行为信息、申请调取其它应用程序的标识符和权限的行为信息、安装行为信息、压缩打包行为信息和移动数据传输行为信息,而行为属性包括恶意与否;根据行为属性确定调取的函数的行为执行路径,将该执行路径进行记录,作为提取的信息的一部分,以在后续步骤中上传到判定服务器,通过将该执行路径的部分或全部与判定服务器中的基于字节码的路径大数据进行分析,进而进行安全性认证。其中终端对该应用程序进行签名处理的过程中,基于解压后的应用程序,获取应用程序中所有文件;将第一类型的文件用安全哈希算法计算摘要信息,并对该摘要信息进行编码,之后将编码值存入不同于第一类型的第二类型的第一文件中,以及将先前保存在第二类型的第一文件中的摘要信息和私钥信息生成一组签名信息并保存在第二类型的与第一文件不同的第二文件中的第一位置,将签名信息和公钥存入第二文件中的第二位置中,其中第一类型和第二类型涉及不同目录类型的文件。

[0040] 优选地,在上述步骤S4中,提取信息进一步包括提取信息的其它部分,即:将应用程序的文件重命名为后缀名为压缩包形式的文件并进行解压,进而得到第一配置文件,使用第一开源软件将第一配置文件转换成可操作的文本格式;将使用第二开源软件反编译解压的结果中的二进制的源码文件;使用第三开源软件还原二进制的源码文件以获得该应用程序的文件的源码;基于应用程序的文件的源码,使用匹配算法将源码进行扫描,并对指定关键词进行统计,获取指定的各个关键词在类文件中的数量和对应位置并使用矩阵存储,基于距离算法计算每两个关键词之间的相似距离;基于相似距离对关键词分类,并将矩阵中的每个关键词作为根节点,把与各个节点之间相似度高的关键词聚合在一起,与存储的所在的位置的矩阵比对,去除不同类别的关键词,进而归类存储;将终端中的特征数据库中存储的安全应用程序的特征与归类存储的特征进行对比,去除该应用程序的特征中包含的安全特征以避免增加信息处理量并增加信息处理时间和功耗以及浪费终端有限的处理资源;将归类存储并去除特征的数据作为提取的信息的其它部分,与其它信息一起被发送到判定服务器进行安全性认证。

[0041] 优选地,步骤S5进一步包括:终端接收判定服务器基于大数据的安全性认证结果,并基于该结果进一步确定是否为恶意,当为恶意时卸载该应用程序,当为安全时在终端中保留该应用程序,而当待定时将风险提示信息在显示屏上展示给用户以供用户了解安全属

性并选择卸载还是保留;当保留该应用程序时,对该应用程序赋予权限,该权限包括存储权限、拍照权限,麦克风使用的权限、录音权限、调用终端传感器的权限、读取和发送短消息权限、拨打电话权限、识别终端安装的SIM卡号码的权限、读取通信录的权限、读取用户运动数据的权限、开启移动运营商通信网络连接权限、开启无线保真连接权限、读取其它应用程序的权限、读取即时通讯软件的通信记录的权限,赋予权限包括赋予启用权限或者赋予禁用权限;当确定卸载时,将该应用程序的信息发送到判定服务器以更新判定服务器中用于大数据分析、判定和确认的数据库。

[0042] 优选地,步骤S6中,当该应用程序在终端上执行时,获取其运行参数并进行分析包括:执行应用程序,获取其运行过程中的行为参数,该行为参数包括系统API、文件权限的变化、进程和线程运行数据、调用数据、网络访问请求数据、发送的网络数据,将该行为参数记录在日志文件中;监控应用程序中可移植的执行文件的创建操作,确定其创建主体,在终端存储器中建立可移植的执行文件与其创建主体间的对应关系;使用模拟工具自行运行和模拟终端用户的运行操作,以获得日志文件记录和网络数据分组文件记录;在模拟工具运行结束,并且在网络链路开启接通和随着时间的流逝而数据通信结束之后,将日志文件记录和网络数据分组文件记录存储在第一存储位置中;对日志文件记录和网络数据分组文件记录进行分析,其中使用特征提取对日志文件记录和网络数据分组文件记录的特征量化,将权限、API、URL和字符串转换成数值特征,使用采用基于均值和方差的特征选择算法选择特征的子集,结合分类和聚类以及标签构建规则对数值特征进行预测,基于该数值特征与预设配置文件中的参数的数值匹配而确定其运行行为属性,即安装的该应用程序对于终端来说是否安全,并将其作为分析的结果的第一部分;当结果为安全或相反时,将应用程序中可移植的执行文件与其创建主体的对应关系作为分析的结果的第二部分,当为不安全即恶意时,另外将创建主体的相关信息进行标记以作为标识该应用程序会对终端造成影响的恶意标识信息并作为第二部分的补充部分,以供发送到判定服务器更新大数据分析判定和确认的数据库,并且在终端进行记录并存储到安全信息数据库中以作为恶意的来源,在后续安装时可将该来源的应用程序作为来自恶意来源的应用程序而提供和显示给用户,供用户可选地对该源头进行彻底查杀并掐断该源头和来自其的所有应用程序的安装以及该源头对终端的任何访问请求;聚合分析的结果的第一部分和分析的结果的第二部分以作为该应用程序的信息。

[0043] 替代地,步骤S6中,当该应用程序在终端上执行时,获取其运行参数并进行分析包括:当应用程序运行的同时移动网络也开启时,周期性地获取终端的流量数据,将应用程序收发的流量数据进行矢量化,提取其中的矢量片段,并存储到运行数据库中以供后续使用,同时截取某个时段内的多个矢量片段,将其与运行数据库中存储的历史矢量数据进行匹配,若与安全的历史矢量数据匹配则初步判定为非恶意应用程序行为,若与恶意的历史矢量数据匹配则初步判定为恶意应用程序行为,将得到的应用程序行为作为分析的结果。

[0044] 优选地,在步骤S7中,基于分析的结果进一步确定在终端中保留该应用程序还是卸载该应用程序,并将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库进一步包括:终端基于分析的结果的第一部分,当为安全的应用程序时保留该应用程序,而当为恶意时卸载该应用程序,并将包括分析的结果的第一部分和分析的结果的第二部分的应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认

的数据库，其中为恶意时，分析的结果的第二部分还包括有将创建主体的相关信息进行标记以作为标识该应用程序会对终端造成影响的恶意标识信息的补充部分。

[0045] 优选地，在步骤S7中，在执行完上述步骤之后，进一步执行以下操作：在卸载应用程序之后，当终端启动网络通信时激活监控程序，进而使得该监控程序实时截取通过网络收发的数据，并将发送的数据宿和/或接收的数据源与之前确定的恶意的来源进行特征匹配，当符合匹配标准时将该结果显示给用户并分析待发送的数据所在的位置以及对该数据进行调用的实体的名称和位置，并将该调用的实体的名称和位置进行定点移除，之后显示移除成功与否的结果，如果不成功则重复上述移除操作并展示给用户移除进程，直到符合预设要求为止。

[0046] 进一步地，分析待发送的数据所在的位置的同时还分析待发送的数据，以确定是否含有用户的账号、联系人、验证码、联系方式的信息，如果存在则将风险提示给用户。

[0047] 优选地，步骤S8中，当该应用程序请求访问终端上的用户隐私数据时，终端根据权限配置表确认其访问权限，并执行对应操作进一步包括：当该应用程序请求访问终端上的用户隐私数据时，应用程序将访问请求发送给终端的处理器，处理器将应用程序标识发送至权限管理模块，以根据权限管理模块中的权限配置表确定该应用程序的访问权限，当应用程序具有复数种隐私数据中的一种或多种的访问权限时，处理器确定该应用程序请求访问的终端上的用户隐私数据的访问权限是否符合权限配置表确定的访问权限，如果符合则给应用程序分配一个对应的解释引擎，处理器发布跳转指令，并经过执行跳转指令后将应用程序引导至解释引擎的入口，以用于由该解释引擎对请求访问的终端上的用户隐私数据进行解释，并将解释的用户隐私数据发送给该应用程序。

[0048] 优选地，该用户隐私数据是为了保障用户信息安全而被转换的数据，其在终端中存储时不会明码存储而被恶意代码或文件或软件攻击获取进而给用户造成不可挽回的损失，其中该用户隐私数据首先由原始函数的代码形式转换成仅仅可以由终端的解释引擎解释、对于第三方软件来说无法有效分割破解并且看上去没有明显含义的字节码，该字节码以片段形式由解释引擎进行解释，并且该片段长度由该解释引擎限定，同时在各个片段之间、在前一个片段的末尾以解释引擎可识别的、表示间隔的、以有限数据长度的字节码形式的分隔符；为字节码设定跳转指令，并存储在寄存器中，同时擦除由原始函数的代码形式表示的用户隐私数据；当应用程序请求访问终端上的用户隐私数据时，如果处理器确定该应用程序请求访问的终端上的用户隐私数据的访问权限是否符合权限配置表确定的访问权限，则处理器调取并发布跳转指令，并经过执行跳转指令后将应用程序引导至解释引擎的入口，以用于由该解释引擎对请求访问的终端上的用户隐私数据进行解释，并将解释的用户隐私数据发送给该应用程序。

[0049] 优选地，步骤S9中，当终端有新的即时通讯消息传入并且该应用程序请求访问时，终端基于访问设置而对该应用程序的访问使能或禁止进一步包括：当终端有新的即时通讯消息传入时，终端对该新传入的即时通讯消息进行接收，并由终端的消息分析模块分析其中包含的涉密信息，终端的消息分析模块判断传入的即时通讯消息中是否包含用户密码、账号、验证码中的任一个或多个与有效时间的组合的信息，当包含其中的任一个或多个与有效时间的组合的信息时，将该新传入的即时通讯消息存储到终端的私密存储库中，否则将新传入的即时通讯消息存储到终端的常规存储库中；当包含其中的任一个或多个与有效

时间的组合的信息，且当安装的应用程序试图访问该传入的即时通讯消息时，权限管理模块验证该应用程序是否具有对传入的即时通讯消息的访问权限，(i)如果不具有访问权限，则权限管理模块通知终端的私密存储库不将新传入的即时通讯消息发送给该应用程序，以及(ii)如果具有访问权限，则权限管理模块向私密存储库发送应用程序对私密存储库中消息的读取请求，并且权限管理模块通知终端的消息分析模块判断当前时段是否在存储的新传入的即时通讯消息的有效读取时段中，当处于新传入的即时通讯消息的有效读取时段中时，则由私密存储库将其中存储的新传入的即时通讯消息发送给应用程序，否则当不处于新传入的即时通讯消息的有效读取时段中，即处于新传入的即时通讯消息的禁止读取时段中时，私密存储库拒绝将其中存储的新传入的即时通讯消息发送给应用程序，直到其禁止读取时段解除，此时即使应用程序尝试读取私密信息成功，由于已经随着时间的过去而超出新传入的即时通讯消息的可以访问的有效读取时段，所以即使应用程序读取到私密信息，也因为过了有效时段而无法对终端构成攻击，极大地降低了恶意应用程序对终端的私密信息的窃取和泄露；以及当将新传入的即时通讯消息存储到终端的常规存储库中，且当安装的应用程序试图访问该传入的即时通讯消息时，权限管理模块验证该应用程序是否具有对传入的即时通讯消息的访问权限，(i)如果不具有访问权限，则权限管理模块通知终端的常规存储库不将新传入的即时通讯消息发送给该应用程序，以及(ii)如果具有访问权限，则限管理模块向常规存储库发送应用程序对常规存储库中消息的读取请求，并且由常规存储库将其中存储的新传入的即时通讯消息发送给应用程序。

[0050] 根据本发明的示范性实施例，图3图示一种基于终端的大数据分析处理系统，包括终端和判定服务器，其中终端包括：处理器，权限管理模块，解释引擎，消息分析模块，私密存储库，常规存储库；判定服务器内部设置有用于大数据分析、确认和判定的数据库。

[0051] 优选地，所述基于终端的大数据分析处理系统用于执行以下方法和步骤：终端经由无线网络查询应用程序并将标识应用程序的可用网络来源的信息发送到判定服务器；终端基于判定服务器根据大数据获得的判定结果，如果恶意则确定重新尝试从其它可用资源下载，如果为安全则直接下载该应用程序，如果为待定则由用户确定风险等级后选择直接下载还是重新下载：终端下载并安装应用程序，提取该应用程序的信息并发送给判定服务器，基于判定服务器的分析结果，确定在终端保留还是卸载应用程序；终端执行应用程序时，获取其运行参数并进行分析，基于分析结果再进一步确定在终端中保留该应用程序还是卸载该应用程序；终端再次确定保留该应用程序之后，在应用程序运行、访问终端上的敏感或隐私数据时进行权限管理以将其使能或禁止；以及终端接收新传入的即时通讯消息之后并且当该应用程序请求访问该新传入的即时通讯消息时，基于新传入的新的即时通讯消息所包含的信息种类是否符合预设规定而存储到不同类别的数据库中，并且根据应用程序的读取权限和新传入的新的即时通讯消息的时间属性而确定在规定时段内是否使能或禁止该应用程序的访问。

[0052] 优选地，所述基于终端的大数据分析处理系统进一步执行以下步骤：步骤S1，终端经由浏览器、通过无线网络搜索所需的应用程序，并获取含有可用应用程序的资源服务器的名称和/或IP信息，该名称和/或IP信息标识提供可用的应用程序下载的资源服务器；步骤S2，终端将该资源服务器的名称和/或IP信息进行打包处理，发送给判定服务器进行恶意与否的确认；步骤S3，判定服务器基于内置数据库中的涉及资源服务器的大数据进行判定

和确认，并将结果通过无线链路返回给终端，终端根据判定服务器判定确认的恶意与否的结果执行对应操作：如果恶意则阻断与该资源服务器的通信链路并继续尝试步骤S1中获取的其它可用资源服务器且顺次执行步骤S2和S3，直到判定服务器确认非恶意或者尝试次数达到用户先前预设的次数；如果安全则直接下载该应用程序，如果待定则由用户选择是直接下载还是重新下载；步骤S4，下载该应用程序后，终端直接安装或将开始安装按钮显示在显示器上由用户手动安装，安装该应用程序时赋予该应用程序最少的可用权限，完毕后提取该应用程序的信息，并对该应用程序进行签名处理，将提取的信息再次经由无线网络发送到判定服务器进行安全性认证；步骤S5，终端根据判定服务器基于大数据的安全性认证结果，再次确定在终端中保留该应用程序还是卸载该应用程序；当保留该应用程序时，对该应用程序更新并添加或减少其对应的可用权限，而当卸载时将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库；步骤S6，当该应用程序在终端上执行时，获取其运行参数并进行分析；步骤S7，基于分析的结果再进一步确定在终端中保留该应用程序还是卸载该应用程序，并将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库；步骤S8，当该应用程序请求访问终端上的用户隐私数据时，终端根据权限配置表确认其访问权限，并执行对应操作，其中该终端上的用户隐私数据在安装该应用程序之前进行了格式转换以增强其读取安全性；步骤S9，当终端有新的即时通讯消息传入并且该应用程序请求访问时，终端基于该新传入的即时通讯消息中包含时间属性而将新传入的即时通讯消息存储到不同数据库中，并确定该新传入的即时通讯消息中包含的信息的类别是否符合预设规则，同时基于应用程序的可用权限而在指定的时段内对该应用程序的访问进行使能或禁止。

[0053] 根据以上所述的基于终端的大数据分析处理系统，能够利用大数据和信息安全技术，在安装阶段对应用程序进行安全性检测，并且对终端有危害的应用程序进行拦截，并对其源头进行确认和阻断；并且针对应用程序对于终端中用户隐私信息的合法或非法访问问题，通过合理管理而进行隐私信息读取并且确保读取不超越预设权限，或者通过设置避免应用程序对隐私程序的不合理访问，进而基于大数据和权限管理实现系统的安全。

[0054] 优选地，所述基于终端的大数据分析处理系统进一步执行以下步骤S1：直接经由终端安装的浏览器，通过输入期望的应用程序的名称，通过搜索引擎进行搜索；或者在当前的非浏览器应用中，通过用户手指长按屏幕，在屏幕上出现选择文字的选项，用户通过选择和高亮应用程序的全部或部分名称，并在选定后点击屏幕上出现的搜索按钮，通过点击该搜索按钮而出现一个或多个浏览器的选择图标以供选择，在选择对应的浏览器图标后进行搜索；或者在当前的非浏览器应用中，通过选择该非浏览器应用中的搜索图标，在屏幕上出现输入框，通过输入期望的应用程序名称后，该非浏览器应用要么直接调用默认的第三方浏览器进行搜索，要么出现一个或多个浏览器的选择图标以供选择并且在选择对应的浏览器图标后进行搜索；或者在内嵌有浏览器的即时通讯应用中，要么通过用户手指长按屏幕并在屏幕上出现选择文字的选项，通过选择和高亮应用程序的全部或部分名称并在选定后点击屏幕上出现的搜索按钮而调用嵌入的浏览器进行搜索，要么通过选择该非浏览器应用中的搜索图标而在屏幕上出现输入框，通过输入期望的应用程序名称而调用嵌入的浏览器进行搜索。在经由无线网络搜索所需的应用程序之后，根据结果获取用于标识含有应用程序的资源服务器的名称和/或IP地址。

[0055] 优选地，所述基于终端的大数据分析处理系统进一步执行以下步骤S2进一步包括：终端选择该资源服务器的名称和/或IP信息中的任一者或两者，并将其以固定的包传输格式打包在待传输的包中，并将包的报头设置为请求属性，在待传输的包中的名称和/或IP信息中的任一者或两者之后通过固定的结束符终止，以便于判定服务器识别，之后将该包通过无线链路发送到判定服务器，以供进行恶意与否的确认。

[0056] 优选地，所述基于终端的大数据分析处理系统进一步执行以下步骤S3：判定服务器内部设置有用于大数据分析、确认和判定的数据库，该数据库存储有用于终端的应用程序的安全属性信息，包括恶意、安全和待定，该安全属性信息随着时间的流逝而进行更新，其更新方式通过用户上传、信息中心通知等方式中的任一种而进行；判定服务器接收终端传输的包，并基于预设的拆分包规则，提取包中的资源服务器的名称和/或IP信息中的任一者或两者，并将其输入到内部设置的数据库，以进行信息匹配，当有符合安全或恶意的匹配项以及无匹配而被确认为待定时，将该明确和待定的安全属性信息的结果进行打包，经由无线链路发送到终端；终端接收该包并拆分包，提取其中的安全属性信息，如果为恶意则阻断与该资源服务器的通信链路，并继续尝试步骤S1中获取的其它资源服务器且顺次执行步骤S2和S3，直到判定服务器确认非恶意或者尝试次数达到用户预设次数；如果是安全则由用户选择是否下载该应用程序：如果是安全则由用户选择是否下载或直接下载该应用程序，其中如果是安全则直接下载该应用程序，而如果是待定则由用户选择是否下载该应用程序，若下载则进行后续步骤，若不下载则确定直接退出该方法还是继续尝试步骤S1中获取的其它资源服务器且顺次执行步骤S2和S3直到判定服务器确认符合用户期望的安全属性或尝试次数达到用户预设次数。其中判定服务器内部设置的用于大数据分析、确认和判定的数据库所存储的待定的安全属性的确定方法为：基于终端将包通过无线链路发送到判定服务器后，在数据库开始确定安全属性信息的时刻，将数据库中涉及该应用的安全属性的恶意类别占数据库中该应用程序的所有记录的比例小于第一阈值，并且安全属性的安全类别占数据库中该应用程序的所有记录的比例小于第二阈值时，将数据库所存储的该应用程序的安全属性确定为待定。

[0057] 优选地，所述基于终端的大数据分析处理系统进一步执行以下步骤S4：在下载后终端安装该应用程序并提取其信息，对该应用程序进行签名处理，并将提取的信息发送到判定服务器进行安全性认证的步骤中，其中的终端在安装该应用程序的过程中，更改应用程序的文件后缀名以进行解压而得到其中包括的经过编译和工具打包形成的第一文件，获得变换工具以将包括类别名称的类别文件拷贝到第一目录位置，在第一目录位置处通过类别转换命令而生成应用程序中的分组数据；通过遍历分组数据的库函数而获取调取的函数，通过调取的函数的行为信息确定其行为属性，其中该行为信息包括访问行为信息、创建进程行为信息、操作进程行为信息、操作注册表行为信息、申请调取其它应用程序的标识符和权限的行为信息、安装行为信息、压缩打包行为信息和移动数据传输行为信息，而行为属性包括恶意与否；根据行为属性确定调取的函数的行为执行路径，将该执行路径进行记录，作为提取的信息的一部分，以在后续步骤中上传到判定服务器，通过将该执行路径的部分或全部与判定服务器中的基于字节码的路径大数据进行分析，进而进行安全性认证。其中终端对该应用程序进行签名处理的过程中，基于解压后的应用程序，获取应用程序中所有文件；将第一类型的文件用安全哈希算法计算摘要信息，并对该摘要信息进行编码，之后将

编码值存入不同于第一类型的第二类型的第一文件中，以及将先前保存在第二类型的第一文件中的摘要信息和私钥信息生成一组签名信息并保存在第二类型的与第一文件不同的第二文件中的第一位置，将签名信息和公钥存入第二文件中的第二位置中，其中第一类型和第二类型涉及不同目录类型的文件。提取信息进一步包括提取信息的其它部分，即：将应用程序的文件重命名为后缀名为压缩包形式的文件并进行解压，进而得到第一配置文件，使用第一开源软件将第一配置文件转换成可操作的文本格式；将使用第二开源软件反编译解压的结果中的二进制的源码文件；使用第三开源软件还原二进制的源码文件以获得该应用程序的文件的源码；基于应用程序的文件的源码，使用匹配算法将源码进行扫描，并对指定关键词进行统计，获取指定的各个关键词在类文件中的数量和对应位置并使用矩阵存储，基于距离算法计算每两个关键词之间的相似距离；基于相似距离对关键词分类，并将矩阵中的每个关键词作为根节点，把与各个节点之间相似度高的关键词聚合在一起，与存储的所在的位置的矩阵比对，去除不同类别的关键词，进而归类存储；将终端中的特征数据库中存储的安全应用程序的特征与归类存储的特征进行对比，去除该应用程序的特征中包含的安全特征以避免增加信息处理量并增加信息处理时间和功耗以及浪费终端有限的处理资源；将归类存储并去除特征的数据作为提取的信息的其它部分，与其它信息一起被发送到判定服务器进行安全性认证。

[0058] 优选地，所述基于终端的大数据分析处理系统进一步执行以下步骤S5：终端接收判定服务器基于大数据的安全性认证结果，并基于该结果进一步确定是否为恶意，当为恶意时卸载该应用程序，当为安全时在终端中保留该应用程序，而当待定时将风险提示信息在显示屏上展示给用户以供用户了解安全属性并选择卸载还是保留；当保留该应用程序时，对该应用程序赋予权限，该权限包括存储权限、拍照权限，麦克风使用的权限、录音权限、调用终端传感器的权限、读取和发送短消息权限、拨打电话权限、识别终端安装的SIM卡号码的权限、读取通信录的权限、读取用户运动数据的权限、开启移动运营商通信网络连接权限、开启无线保真连接权限、读取其它应用程序的权限、读取即时通讯软件的通信记录的权限，赋予权限包括赋予启用权限或者赋予禁用权限；当确定卸载时，将该应用程序的信息发送到判定服务器以更新判定服务器中用于大数据分析、判定和确认的数据库。

[0059] 优选地，所述基于终端的大数据分析处理系统进一步执行以下步骤S6，当该应用程序在终端上执行时，获取其运行参数并进行分析包括：执行应用程序，获取其运行过程中的行为参数，该行为参数包括系统API、文件权限的变化、进程和线程运行数据、调用数据、网络访问请求数据、发送的网络数据，将该行为参数记录在日志文件中；监控应用程序中可移植的执行文件的创建操作，确定其创建主体，在终端存储器中建立可移植的执行文件与其创建主体间的对应关系；使用模拟工具自行运行和模拟终端用户的运行操作，以获得日志文件记录和网络数据分组文件记录；在模拟工具运行结束，并且在网络链路开启接通和随着时间的流逝而数据通信结束之后，将日志文件记录和网络数据分组文件记录存储在第一存储位置中；对日志文件记录和网络数据分组文件记录进行分析，其中使用特征提取对日志文件记录和网络数据分组文件记录的特征量化，将权限、API、URL和字符串转换成数值特征，使用采用基于均值和方差的特征选择算法选择特征的子集，结合分类和聚类以及标签构建规则对数值特征进行预测，基于该数值特征与预设配置文件中的参数的数值匹配而确定其运行行为属性，即安装的该应用程序对于终端来说是否安全，并将其作为分析的结

果的第一部分;当结果为安全或相反时,将应用程序中可移植的执行文件与其创建主体的对应关系作为分析的结果的第二部分,当为不安全即恶意时,另外将创建主体的相关信息进行标记以作为标识该应用程序会对终端造成影响的恶意标识信息并作为第二部分的补充部分,以供发送到判定服务器更新大数据分析判定和确认的数据库,并且在终端进行记录并存储到安全信息数据库中以作为恶意的来源,在后续安装时可将该来源的应用程序作为来自恶意来源的应用程序而提供和显示给用户,供用户可选地对该源头进行彻底查杀并掐断该源头和来自其的所有应用程序的安装以及该源头对终端的任何访问请求;聚合分析的结果的第一部分和分析的结果的第二部分以作为该应用程序的信息。

[0060] 替代地,步骤S6中,当应用程序在终端上执行时,获取其运行参数并进行分析包括:当应用程序运行的同时移动网络也开启时,周期性地获取终端的流量数据,将应用程序收发的流量数据进行矢量化,提取其中的矢量片段,并存储到运行数据库中以供后续使用,截取某个时段内的多个矢量片段,将其与运行数据库中存储的历史矢量数据匹配,若与安全的历史矢量数据匹配则初步判定为非恶意应用程序行为,若与恶意的历史矢量数据匹配则初步判定为恶意应用程序行为,将得到的应用程序行为作为分析的结果。

[0061] 优选地,所述基于终端的大数据分析处理系统进一步执行以下步骤S7,基于分析的结果进一步确定在终端中保留该应用程序还是卸载该应用程序,并将该应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库进一步包括:终端基于分析的结果的第一部分,当为安全的应用程序时保留该应用程序,而当为恶意时卸载该应用程序,并将包括分析的结果的第一部分和分析的结果的第二部分的应用程序的信息发送到判定服务器以更新用于大数据分析、判定和确认的数据库,其中为恶意时,分析的结果的第二部分还包括有将创建主体的相关信息进行标记以作为标识该应用程序会对终端造成影响的恶意标识信息的补充部分。在执行完上述步骤之后,进一步执行以下操作:在卸载应用程序之后,当终端启动网络通信时激活监控程序,进而使得该监控程序实时截取通过网络收发的数据,并将发送的数据宿和/或接收的数据源与之前确定的恶意的来源进行特征匹配,当符合匹配标准时将该结果显示给用户并分析待发送的数据所在的位置以及对该数据进行调用的实体的名称和位置,并将该调用的实体的名称和位置进行定点移除,之后显示移除成功与否的结果,如果不成功则重复上述移除操作并展示给用户移除进程,直到符合预设要求为止。分析待发送的数据所在的位置的同时还分析待发送的数据,以确定是否含有用户的账号、联系人、验证码、联系方式的信息,如果存在则将风险提示给用户。

[0062] 优选地,所述基于终端的大数据分析处理系统进一步执行以下步骤S8,当该应用程序请求访问终端上的用户隐私数据时,终端根据权限配置表确认其访问权限,并执行对应操作进一步包括:当该应用程序请求访问终端上的用户隐私数据时,应用程序将访问请求发送给终端的处理器,处理器将应用程序标识发送至权限管理模块,以根据权限管理模块中的权限配置表确定该应用程序的访问权限,当应用程序具有复数种隐私数据中的一种或多种的访问权限时,处理器确定该应用程序请求访问的终端上的用户隐私数据的访问权限是否符合权限配置表确定的访问权限,如果符合则给应用程序分配一个对应的解释引擎,处理器发布跳转指令,并经过执行跳转指令后将应用程序引导至解释引擎的入口,以用于由该解释引擎对请求访问的终端上的用户隐私数据进行解释,并将解释的用户隐私数据发送给该应用程序。

[0063] 优选地，所述基于终端的大数据分析处理系统进一步执行以下步骤S9，当终端有新的即时通讯消息传入并且该应用程序请求访问时，终端基于访问设置而对该应用程序的访问使能或禁止进一步包括：当终端有新的即时通讯消息传入时，终端对该新传入的即时通讯消息进行接收，并由终端的消息分析模块分析其中包含的涉密信息，终端的消息分析模块判断传入的即时通讯消息中是否包含用户密码、账号、验证码中的任一个或多个与有效时间的组合的信息，当包含其中的任一个或多个与有效时间的组合的信息时，将该新传入的即时通讯消息存储到终端的私密存储库中，否则将新传入的即时通讯消息存储到终端的常规存储库中；当包含其中的任一个或多个与有效时间的组合的信息，且当安装的应用程序试图访问该传入的即时通讯消息时，权限管理模块验证该应用程序是否具有对传入的即时通讯消息的访问权限，(i)如果不具有访问权限，则权限管理模块通知终端的私密存储库不将新传入的即时通讯消息发送给该应用程序，以及(ii)如果具有访问权限，则权限管理模块向私密存储库发送应用程序对私密存储库中消息的读取请求，并且权限管理模块通知终端的消息分析模块判断当前时段是否在存储的新传入的即时通讯消息的有效读取时段中，当处于新传入的即时通讯消息的有效读取时段中时，则由私密存储库将其中存储的新传入的即时通讯消息发送给应用程序，否则当不处于新传入的即时通讯消息的有效读取时段中，即处于新传入的即时通讯消息的禁止读取时段中时，私密存储库拒绝将其中存储的新传入的即时通讯消息发送给应用程序，直到其禁止读取时段解除，此时即使应用程序尝试读取私密信息成功，由于已经随着时间的过去而超出新传入的即时通讯消息的可以访问的有效读取时段，所以即使应用程序读取到私密信息，也因为过了有效时段而无法对终端构成攻击，极大地降低了恶意应用程序对终端的私密信息的窃取和泄露；以及当将新传入的即时通讯消息存储到终端的常规存储库中，且当安装的应用程序试图访问该传入的即时通讯消息时，权限管理模块验证该应用程序是否具有对传入的即时通讯消息的访问权限，(i)如果不具有访问权限，则权限管理模块通知终端的常规存储库不将新传入的即时通讯消息发送给该应用程序，以及(ii)如果具有访问权限，则限管理模块向常规存储库发送应用程序对常规存储库中消息的读取请求，并且由常规存储库将其中存储的新传入的即时通讯消息发送给应用程序。

[0064] 上述的各个技术术语是本领域中的具有通常含义的常规技术术语，为了不模糊本发明的重点，在此不对其进行进一步的解释。

[0065] 综上，在本发明的技术方案中，通过采用了一种基于终端的大数据分析处理方法及系统，其能够利用大数据和信息安全技术，在安装阶段对应用程序进行安全性检测，并且对终端有危害的应用程序进行拦截，并对其源头进行确认和阻断；并且针对应用程序对于终端中用户隐私信息的合法或非法访问问题，本发明对于终端的隐私信息进行加密处理，对于合法访问，通过合理管理而进行隐私信息读取并且确保读取不超越预设权限，而对于非法访问，通过时间设置或者权限阻断设置而避免应用程序对隐私程序的不合理访问。通过本发明的方法及系统，可以基于大数据和权限管理实现系统的安全，并且最终保证应用程序在终端上的下载、运行和数据访问的安全性。

[0066] 将理解的是：可以硬件、软件或硬件和软件的组合的形式实现本发明的示例和实施例。如上所述，可存储任何执行这种方法的主体，以挥发性或非挥发性存储的形式，例如存储设备，像ROM，无论可抹除或可重写与否，或者以存储器的形式，诸如例如RAM、存储器芯

片、设备或集成电路或在光或磁可读的介质上，诸如例如CD、DVD、磁盘或磁带。将理解的是：存储设备和存储介质是适合于存储一个或多个程序的机器可读存储的示例，当被执行时，所述一个或多个程序实现本发明的示例。经由任何介质，诸如通过有线或无线耦合载有的通信信号，可以电子地传递本发明的示例，并且示例适当地包含相同内容。

[0067] 应当注意的是：因为本发明解决了利用大数据和信息安全技术，在安装阶段对应用程序进行安全性检测，并且对终端有危害的应用程序进行拦截，并对其源头进行确认和阻断；并且针对应用程序对于终端中用户隐私信息的合法或非法访问问题，对于终端的隐私信息进行加密处理，对于合法访问通过合理管理而进行隐私信息读取并且确保读取不超越预设权限，对于非法访问通过时间设置或者权限阻断设置而避免应用程序对隐私程序的不合理访问。通过本发明的方法及系统，可以基于大数据和权限管理实现系统的安全，并且最终保证应用程序在终端上的下载、运行和数据访问的安全性的技术问题，采用了本技术领域中技术人员在阅读本说明书之后根据其教导所能理解的技术手段，并获取了有益技术效果，所以在所附权利要求中要求保护的方案属于专利法意义上的技术方案。另外，因为所附权利要求要求保护的技术方案可以在工业中制造或使用，因此该方案具备实用性。

[0068] 以上所述，仅为本发明的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，都应包涵在本发明的保护范围之内。除非以其他方式明确陈述，否则公开的每个特征仅是一般系列的等效或类似特征的一个示例。因此，本发明的保护范围应该以权利要求书的保护范围为准。

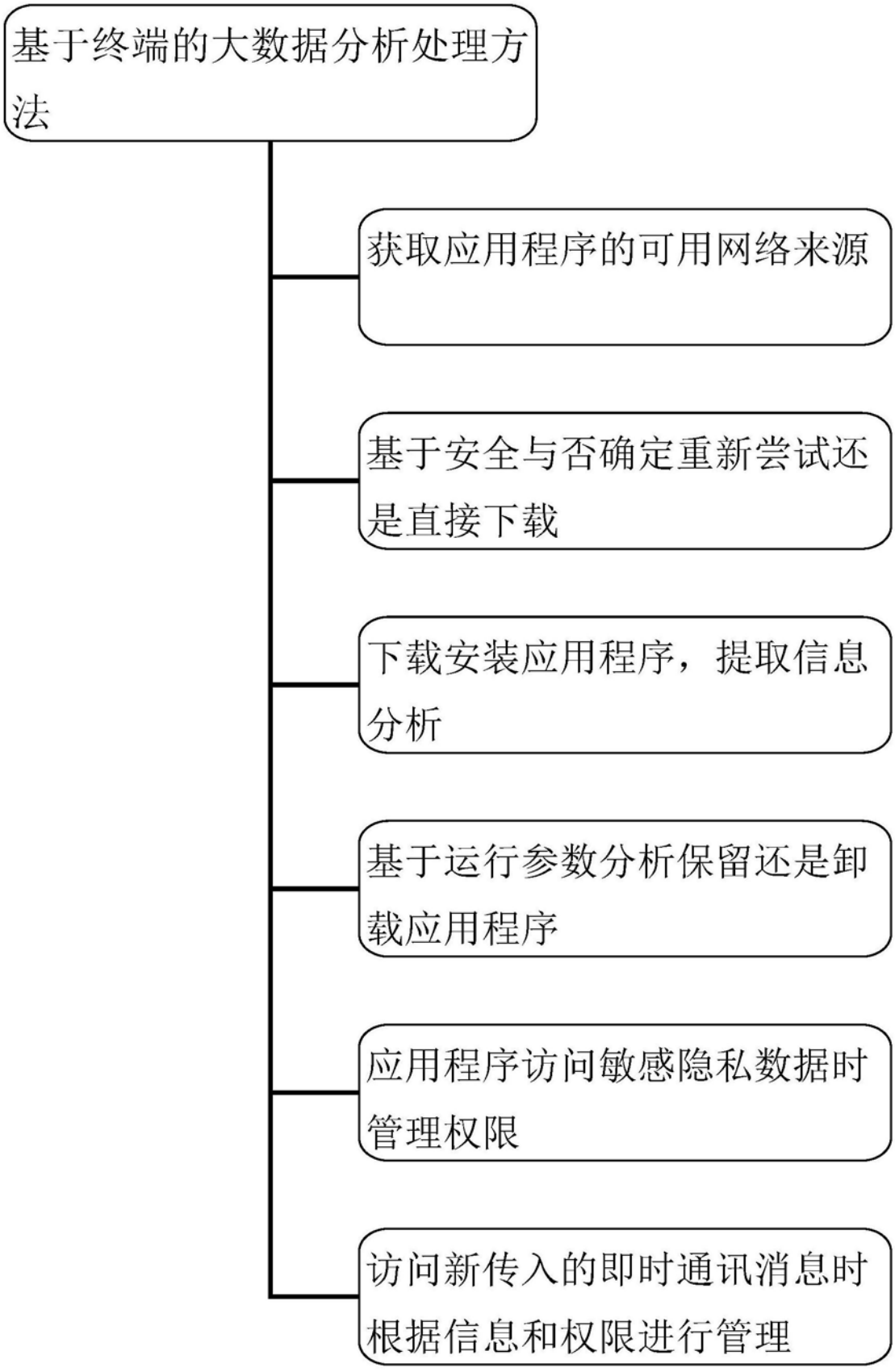

基于终端的大数据分析处理方法
获取应用程序的可用网络来源
基于安全与否确定重新尝试还是直接下载
下载安装应用程序，提取信息分析
基于运行参数分析保留还是卸载应用程序
应用程序访问敏感隐私数据时管理权限
访问新传入的即时通讯消息时根据信息和权限进行管理

图1

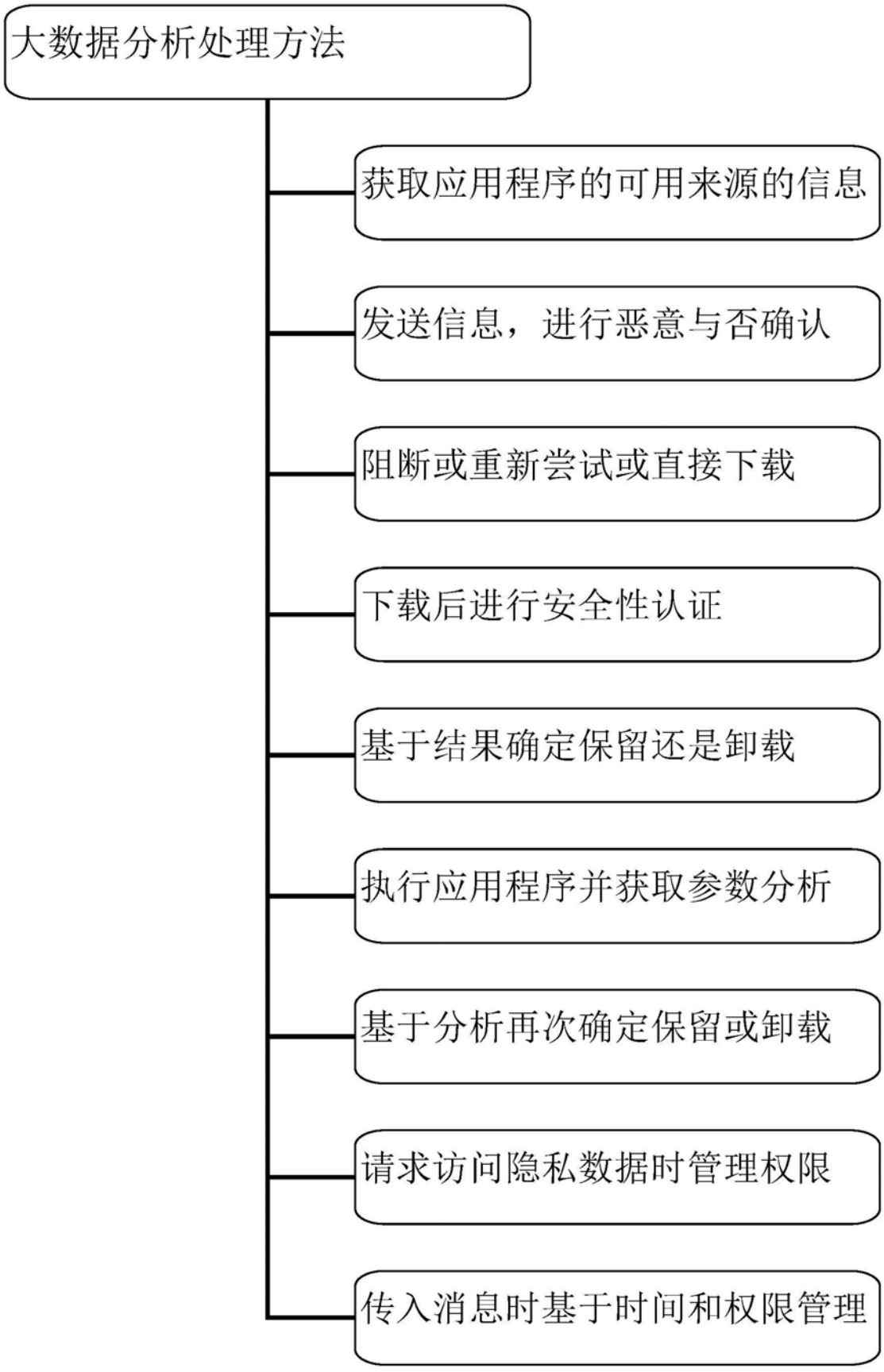

大数据分析处理方法
获取应用程序的可用来源的信息
发送信息，进行恶意与否确认
阻断或重新尝试或直接下载
下载后进行安全性认证
基于结果确定保留还是卸载
执行应用程序并获取参数分析
基于分析再次确定保留或卸载
请求访问隐私数据时管理权限
传入消息时基于时间和权限管理

图2

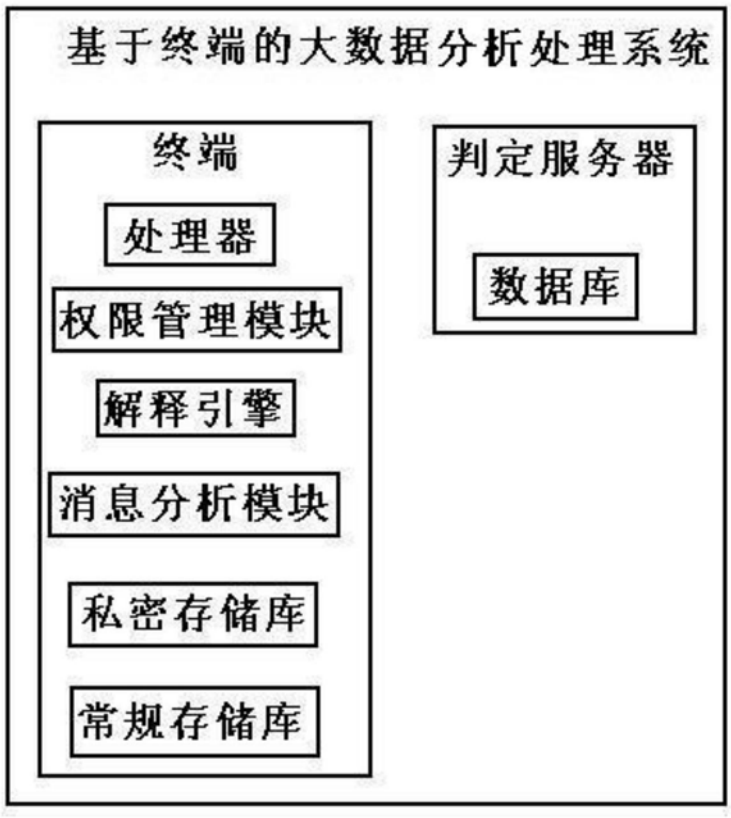

基于终端的大数据分析处理系统
终端
处理器
权限管理模块
解释引擎
消息分析模块
私密存储库
常规存储库
判定服务器
数据库

图3