(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 110929282 A
(43)申请公布日 2020.03.27

(21)申请号 201911234338.2

(22)申请日 2019.12.05

(71)申请人 武汉深佰生物科技有限公司
地址 430000 湖北省武汉市东湖新技术开发区高新大道666号生物创新园B5栋众创空间K003室

(72)发明人 张利达 李德欣

(74)专利代理机构 湖北天领艾匹律师事务所 42252
代理人 罗浩

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
G06F 21/31(2013.01)
G06F 21/55(2013.01)
G06F 21/56(2013.01)

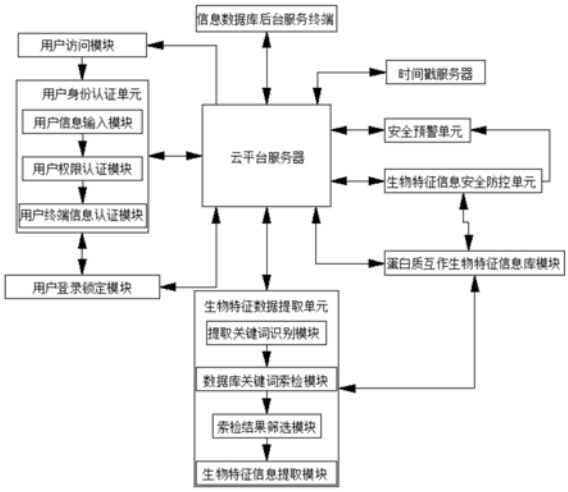
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种基于蛋白互作的生物特征信息预警方法

(57)摘要

本发明公开了一种基于蛋白互作的生物特征信息预警方法，本发明涉及生物信息处理技术领域。生物体蛋白质相互作用的识别精准而且高效，是保障生物体识别并对外界产生反应的基础。本发明基于蛋白互作的生物特征信息预警方法，可实现通过在生物特征数据库信息系统内建立安全预警和防护系统，来告警和防控数据库信息的遗失，很好的达到了通过双重登录权限认证和多次登录失败锁定功能，来使提高数据库系统信息安全性的目的，大大提高了数据库的安全性，很好的避免了数据库受到外来病毒程序的侵入窃取数据信息的情况发生，防止用户越权危险操作影响生物特征数据库的信息安全，同时，可实现对多种数据库进行选择使用，能够适用于多种数据库的安全预警，从而给人们使用蛋白互作的生物特征信息数据库的信息十分有益。



CN 110929282 A

1.一种基于蛋白互作的生物特征信息预警方法,其特征在于:具体包括以下步骤:

S1、首先通过用户访问模块对整个蛋白互作的生物特征信息系统进行访问,然后通过用户身份认证单元内的用户信息输入模块将个人信息输入到系统内,系统通过用户权限认证模块进行用户信息的识别、对比和权限分析,认证成功后,再通过用户终端信息认证模块向用户使用终端发送认证信息进行再次认证;

S2、若经过步骤S1的双重认证失败三次后,云平台服务器控制用户登录锁定模块将用户访问终端页面进行锁定,无法进行登录,若再次登录,需要与信息数据库后台服务终端联系进行登录;

S3、若经过步骤S1的双重认证成功后,向系统内输入所需生物特征信息的关键词,然后通过云平台服务器控制生物特征数据提取单元内的提取关键词识别模块对输入的关键词进行数据化处理并识别,之后通过数据库关键词索检模块向蛋白质互作生物特征信息库模块内索检关键词信息数据,然后通过索检结果筛选模块筛选出与关键词信息相近的数据,之后通过生物特征信息提取模块将数据提取出来;

S4、在数据处理过程中,云平台服务器会控制生物特征信息安全防控单元内的侵入性病毒程序识别模块进行病毒识别,然后通过防火墙系统更新模块和时间戳服务器对系统内的防火墙程序进行实时更新,若识别出病毒程序,侵入算法地址追踪模块能够快速追踪和锁定算法载入系统的终端地址,然后系统安全杀毒模块能够对系统进行杀毒处理;

S5、同时,云平台服务器会控制安全预警单元内的危险信息接收模块接收来自生物特征信息安全防控单元发送的危险指令,然后通过预警指令生成发送模块生成并发送至信息数据库后台服务终端,来供后台服务人员对系统进行安全性检查;

S6、若登录认证成功后的用户在系统内出现危险操作或越权操作时,危险操作告警模块会将告警信息发送至用户的操作终端页面进行警告,若用户继续执行操作,危险用户强制退出模块控制用户终端页面推出系统进行重新登录。

2.根据权利要求1所述的一种基于蛋白互作的生物特征信息预警方法,其特征在于:所述步骤S1中用户身份认证单元包括用户信息输入模块、用户权限认证模块和用户终端信息认证模块,所述用户信息输入模块的输出端与用户权限认证模块的输入端连接,且用户权限认证模的输出端与用户终端信息认证模块的输入端连接。

3.根据权利要求1所述的一种基于蛋白互作的生物特征信息预警方法,其特征在于:所述步骤S3中生物特征数据提取单元包括提取关键词识别模块、数据库关键词检索模块、检索结果筛选模块和生物特征信息提取模块,所述提取关键词识别模块的输出端与数据库关键词检索模块的输入端连接,且数据库关键词检索模块的输出端与检索结果筛选模块的输入端连接,所述检索结果筛选模块的输出端与生物特征信息提取模块的输入端连接。

4.根据权利要求1所述的一种基于蛋白互作的生物特征信息预警方法,其特征在于:所述步骤S4中生物特征信息安全防控单元包括侵入性病毒程序识别模块、防火墙系统更新模块、侵入算法地址追踪模块和系统安全杀毒模块。

5.根据权利要求1所述的一种基于蛋白互作的生物特征信息预警方法,其特征在于:所述步骤S5和步骤S6中安全预警单元包括危险信息接收模块、预警指令生成发送模块、危险操作告警模块和危险用户强制退出模块。

6.根据权利要求1所述的一种基于蛋白互作的生物特征信息预警方法,其特征在于:所

述步骤S2中云平台服务器与用户登录锁定模块实现双向连接。

7.根据权利要求1所述的一种基于蛋白互作的生物特征信息预警方法,其特征在于:所述步骤S3中蛋白质互作生物特征信息库模块为BIND数据库、DIP数据库或STRING数据库中的一种。

一种基于蛋白互作的生物特征信息预警方法

技术领域

[0001] 本发明涉及生物信息处理技术领域，具体为一种基于蛋白互作的生物特征信息预警方法。

背景技术

[0002] 蛋白质相互作用几乎参与了所有的生命活动过程，从遗传物质的复制、基因的表达调控到细胞的代谢过程、细胞的信号转导，以及细胞与细胞之间的短程、远程通讯，生物体的形态形成、病原微生物的致病和宿主对病原微生物的免疫等，研究蛋白质相互作用不仅具有重要的理论意义，还可以为探明致病微生物的致病机理，开发新药，提高人民的生活质量提供指导。

[0003] 随着实验技术的发展，目前研究蛋白质相互作用的技术方法已有酵母双杂交、细菌双杂交、哺乳动物细胞双杂交、CST标记pull-down、免疫共沉淀、亲和色谱表面等离子共振、荧光共振能量转移、质谱、蛋白质芯片X射线晶体衍射、核磁共振等多种，这些技术为蛋白质相互作用研究做出了重大贡献，也积累了宝贵的资料，但是，应用实验的方法研究蛋白质相互作用往往受到成本高、费时费力的固有缺点的限制，生物信息学综合数学、物理、化学、信息科学众家之长，以计算为手段辅助研究蛋白质相互作用，极大地降低了研究成本，缩短了研究周期，而且开辟了一条新的研究道路。

[0004] 目前在使用蛋白相互作用来进行研究时，需要使用数据库，然而，现有的数据库安全性较差，易受到外来病毒程序的侵入窃取数据信息，以及用户越权危险操作影响生物特征数据库的信息安全，不能实现通过在生物特征数据库信息系统内建立安全预警和防护系统，来告警和防控数据库信息的遗失，无法达到通过双重登录权限认证和多次登录失败锁定功能，来使提高数据库系统信息安全性的目的，从而给人们使用蛋白互作的生物特征信息数据库的信息十分不利。

发明内容

[0005] (一)解决的技术问题

[0006] 针对现有技术的不足，本发明提供了一种基于蛋白互作的生物特征信息预警方法，解决了现有的数据库安全性较差，易受到外来病毒程序的侵入窃取数据信息，以及用户越权危险操作影响生物特征数据库的信息安全，不能实现通过在生物特征数据库信息系统内建立安全预警和防护系统，来告警和防控数据库信息的遗失，无法达到通过双重登录权限认证和多次登录失败锁定功能，来使提高数据库系统信息安全性目的的问题。

[0007] (二)技术方案

[0008] 为实现以上目的，本发明通过以下技术方案予以实现：一种基于蛋白互作的生物特征信息预警方法，具体包括以下步骤：

[0009] S1、首先通过用户访问模块对整个蛋白互作的生物特征信息系统进行访问，然后通过用户身份认证单元内的用户信息输入模块将个人信息输入到系统内，系统通过用户权

限认证模块进行用户信息的识别、对比和权限分析，认证成功后，再通过用户终端信息认证模块向用户使用终端发送认证信息进行再次认证；

[0010] S2、若经过步骤S1的双重认证失败三次后，云平台服务器控制用户登录锁定模块将用户访问终端页面进行锁定，无法进行登录，若再次登录，需要与信息数据库后台服务终端联系进行登录；

[0011] S3、若经过步骤S1的双重认证成功后，向系统内输入所需生物特征信息的关键词，然后通过云平台服务器控制生物特征数据提取单元内的提取关键词识别模块对输入的关键词进行数据化处理并识别，之后通过数据库关键词索检模块向蛋白质互作生物特征信息库模块内索检关键词信息数据，然后通过索检结果筛选模块筛选出与关键词信息相近的数据，之后通过生物特征信息提取模块将数据提取出来；

[0012] S4、在数据处理过程中，云平台服务器会控制生物特征信息安全防控单元内的侵入性病毒程序识别模块进行病毒识别，然后通过防火墙系统更新模块和时间戳服务器对系统内的防火墙程序进行实时更新，若识别出病毒程序，侵入算法地址追踪模块能够快速追踪和锁定算法载入系统的终端地址，然后系统安全杀毒模块能够对系统进行杀毒处理；

[0013] S5、同时，云平台服务器会控制安全预警单元内的危险信息接收模块接收来自生物特征信息安全防控单元发送的危险指令，然后通过预警指令生成发送模块生成并发送至信息数据库后台服务终端，来供后台服务人员对系统进行安全性检查；

[0014] S6、若登录认证成功后的用户在系统内出现危险操作或越权操作时，危险操作告警模块会将告警信息发送至用户的操作终端页面进行警告，若用户继续执行操作，危险用户强制退出模块控制用户终端页面推出系统进行重新登录。

[0015] 优选的，所述步骤S1中用户身份认证单元包括用户信息输入模块、用户权限认证模块和用户终端信息认证模块，所述用户信息输入模块的输出端与用户权限认证模块的输入端连接，且用户权限认证模的输出端与用户终端信息认证模块的输入端连接。

[0016] 优选的，所述步骤S3中生物特征数据提取单元包括提取关键词识别模块、数据库关键词检索模块、检索结果筛选模块和生物特征信息提取模块，所述提取关键词识别模块的输出端与数据库关键词检索模块的输入端连接，且数据库关键词检索模块的输出端与检索结果筛选模块的输入端连接，所述检索结果筛选模块的输出端与生物特征信息提取模块的输入端连接。

[0017] 优选的，所述步骤S4中生物特征信息安全防控单元包括侵入性病毒程序识别模块、防火墙系统更新模块、侵入算法地址追踪模块和系统安全杀毒模块。

[0018] 优选的，所述步骤S5和步骤S6中安全预警单元包括危险信息接收模块、预警指令生成发送模块、危险操作告警模块和危险用户强制退出模块。

[0019] 优选的，所述步骤S2中云平台服务器与用户登录锁定模块实现双向连接。

[0020] 优选的，所述步骤S3中蛋白质互作生物特征信息库模块为BIND数据库、DIP数据库或STRING数据库中的一种。

[0021] (三)有益效果

[0022] 本发明提供了一种基于蛋白互作的生物特征信息预警方法。与现有技术相比具备以下有益效果：

[0023] (1)、该基于蛋白互作的生物特征信息预警方法，具体包括以下步骤：S1、首先通过

用户访问模块对整个蛋白互作的生物特征信息系统进行访问，然后通过用户身份认证单元内的用户信息输入模块将个人信息输入到系统内，系统通过用户权限认证模块进行用户信息的识别、对比和权限分析，认证成功后，S2、若经过步骤S1的双重认证失败三次后，云平台服务器控制用户登录锁定模块将用户访问终端页面进行锁定，无法进行登录，若再次登录，需要与信息数据库后台服务终端联系进行登录，S3、若经过步骤S1的双重认证成功后，向系统内输入所需生物特征信息的关键词，然后通过云平台服务器控制生物特征数据提取单元内的提取关键词识别模块对输入的关键词进行数据化处理并识别，S4、在数据处理过程中，云平台服务器会控制生物特征信息安全防控单元内的侵入性病毒程序识别模块进行病毒识别，然后通过防火墙系统更新模块和时间戳服务器对系统内的防火墙程序进行实时更新，若识别出病毒程序，侵入算法地址追踪模块能够快速追踪和锁定算法载入系统的终端地址，然后系统安全杀毒模块能够对系统进行杀毒处理，S5、同时，云平台服务器会控制安全预警单元内的危险信息接收模块接收来自生物特征信息安全防控单元发送的危险指令，然后通过预警指令生成发送模块生成并发送至信息数据库后台服务终端，来供后台服务人员对系统进行安全性检查，S6、若登录认证成功后的用户在系统内出现危险操作或越权操作时，危险操作告警模块会将告警信息发送至用户的操作终端页面进行警告，若用户继续执行操作，危险用户强制退出模块控制用户终端页面推出系统进行重新登录，可实现通过在生物特征数据库信息系统内建立安全预警和防护系统，来告警和防控数据库信息的遗失，很好的达到了通过双重登录权限认证和多次登录失败锁定功能，来使提高数据库系统信息安全性的目的，大大提高了数据库的安全性，很好的避免了数据库受到外来病毒程序的侵入窃取数据信息的情况发生，防止用户越权危险操作影响生物特征数据库的信息安全，从而给人们使用蛋白互作的生物特征信息数据库的信息十分有益。

[0024] (2)、该基于蛋白互作的生物特征信息预警方法，通过在蛋白质互作生物特征信息库模块为BIND数据库、DIP数据库或STRING数据库中的一种，可实现对多种数据库进行选择使用，能够适用于多种数据库的安全预警，从而使数据库的安全性得到大大提高。

附图说明

[0025] 图1为本发明系统的结构原理框图；

[0026] 图2为本发明生物特征信息安全防控单元的结构原理框图；

[0027] 图3为本发明安全预警单元的结构原理框图。

具体实施方式

[0028] 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。

[0029] 请参阅图1-3，本发明实施例提供一种技术方案：一种基于蛋白互作的生物特征信息预警方法，具体包括以下步骤：

[0030] S1、首先通过用户访问模块对整个蛋白互作的生物特征信息系统进行访问，然后通过用户身份认证单元内的用户信息输入模块将个人信息输入到系统内，系统通过用户权

限认证模块进行用户信息的识别、对比和权限分析，认证成功后，再通过用户终端信息认证模块向用户使用终端发送认证信息进行再次认证，用户身份认证单元包括用户信息输入模块、用户权限认证模块和用户终端信息认证模块，用户信息输入模块的输出端与用户权限认证模块的输入端连接，且用户权限认证模的输出端与用户终端信息认证模块的输入端连接；

[0031] S2、若经过步骤S1的双重认证失败三次后，云平台服务器控制用户登录锁定模块将用户访问终端页面进行锁定，无法进行登录，若再次登录，需要与信息数据库后台服务终端联系进行登录，云平台服务器与用户登录锁定模块实现双向连接；

[0032] S3、若经过步骤S1的双重认证成功后，向系统内输入所需生物特征信息的关键词，然后通过云平台服务器控制生物特征数据提取单元内的提取关键词识别模块对输入的关键词进行数据化处理并识别，之后通过数据库关键词索检模块向蛋白质互作生物特征信息库模块内索检关键词信息数据，然后通过索检结果筛选模块筛选出与关键词信息相近的数据，之后通过生物特征信息提取模块将数据提取出来，生物特征数据提取单元包括提取关键词识别模块、数据库关键词检索模块、检索结果筛选模块和生物特征信息提取模块，提取关键词识别模块的输出端与数据库关键词检索模块的输入端连接，且数据库关键词检索模块的输出端与检索结果筛选模块的输入端连接，检索结果筛选模块的输出端与生物特征信息提取模块的输入端连接，蛋白质互作生物特征信息库模块为BIND数据库、DIP数据库或STRING数据库中的一种；

[0033] S4、在数据处理过程中，云平台服务器会控制生物特征信息安全防控单元内的侵入性病毒程序识别模块进行病毒识别，然后通过防火墙系统更新模块和时间戳服务器对系统内的防火墙程序进行实时更新，若识别出病毒程序，侵入算法地址追踪模块能够快速追踪和锁定算法载入系统的终端地址，然后系统安全杀毒模块能够对系统进行杀毒处理，生物特征信息安全防控单元包括侵入性病毒程序识别模块、防火墙系统更新模块、侵入算法地址追踪模块和系统安全杀毒模块；

[0034] S5、同时，云平台服务器会控制安全预警单元内的危险信息接收模块接收来自生物特征信息安全防控单元发送的危险指令，然后通过预警指令生成发送模块生成并发送至信息数据库后台服务终端，来供后台服务人员对系统进行安全性检查；

[0035] S6、若登录认证成功后的用户在系统内出现危险操作或越权操作时，危险操作告警模块会将告警信息发送至用户的操作终端页面进行警告，若用户继续执行操作，危险用户强制退出模块控制用户终端页面推出系统进行重新登录，安全预警单元包括危险信息接收模块、预警指令生成发送模块、危险操作告警模块和危险用户强制退出模块。

[0036] 综上所述

[0037] 本发明可实现通过在生物特征数据库信息系统内建立安全预警和防护系统，来告警和防控数据库信息的遗失，很好的达到了通过双重登录权限认证和多次登录失败锁定功能，来使提高数据库系统信息安全性的目的，大大提高了数据库的安全性，很好的避免了数据库受到外来病毒程序的侵入窃取数据信息的情况发生，防止用户越权危险操作影响生物特征数据库的信息安全，从而给人们使用蛋白互作的生物特征信息数据库的信息十分有益。

[0038] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实

体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。

[0039] 尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同物限定。

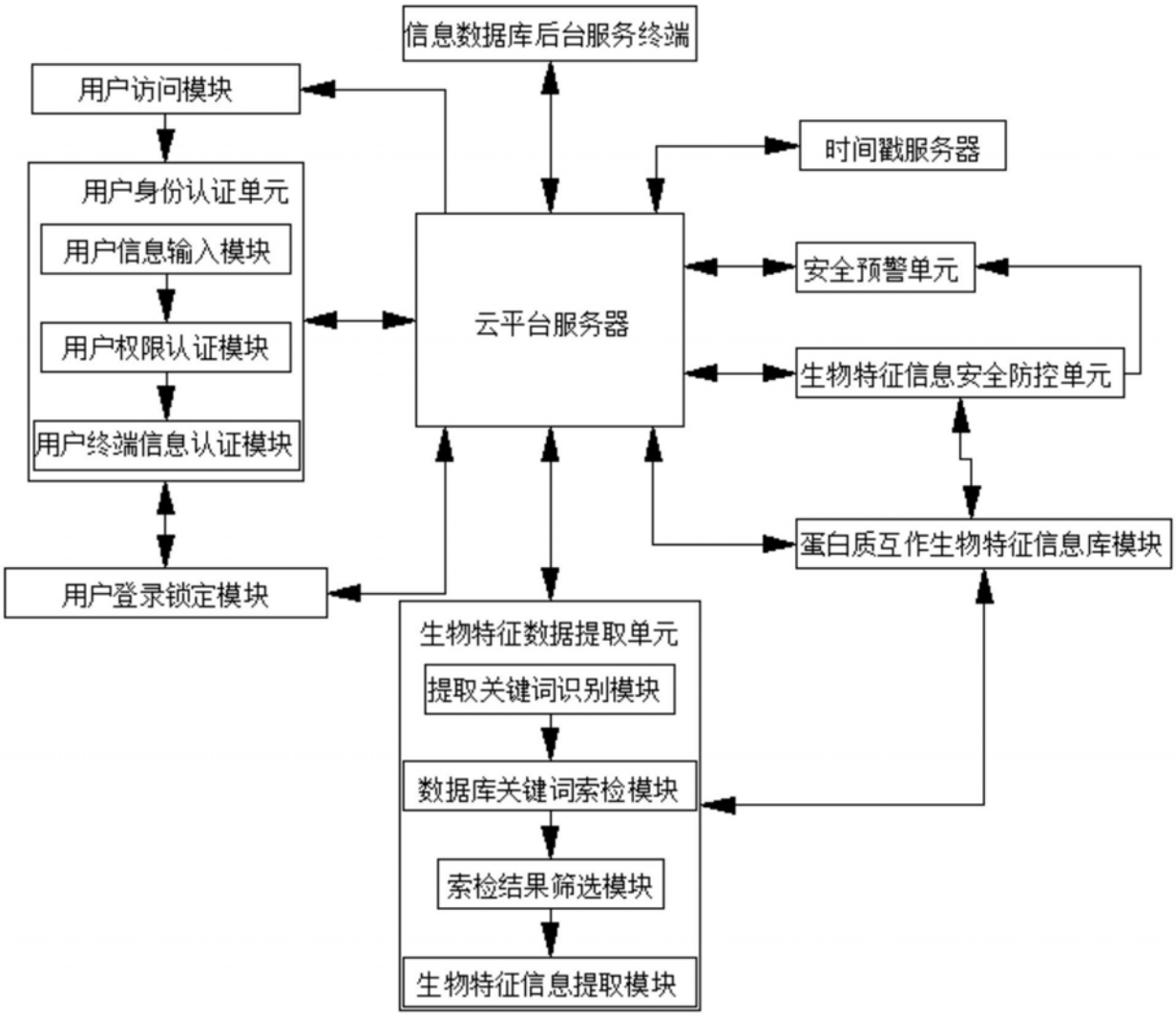

信息数据库后台服务终端
用户访问模块
时间戳服务器
用户身份认证单元
用户信息输入模块
安全预警单元
云平台服务器
用户权限认证模块
生物特征信息安全防控单元
用户终端信息认证模块
蛋白质互作生物特征信息库模块
用户登录锁定模块
生物特征数据提取单元
提取关键词识别模块
数据库关键词索检模块
索检结果筛选模块
生物特征信息提取模块

图1

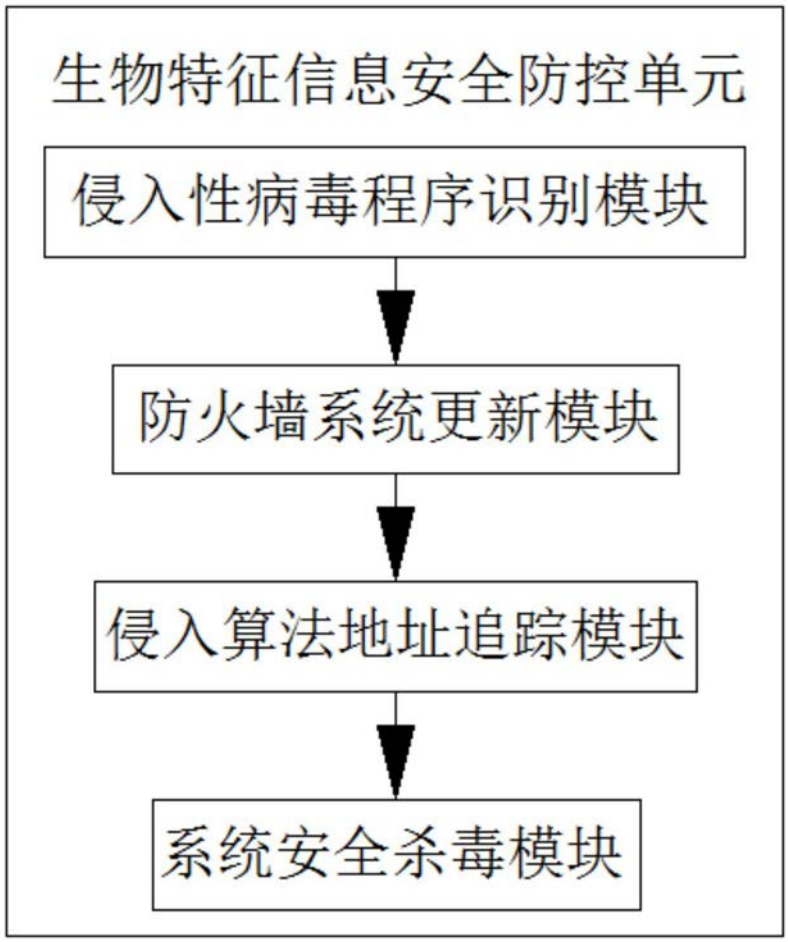

生物特征信息安全防控单元
侵入性病毒程序识别模块
防火墙系统更新模块
侵入算法地址追踪模块
系统安全杀毒模块

图2

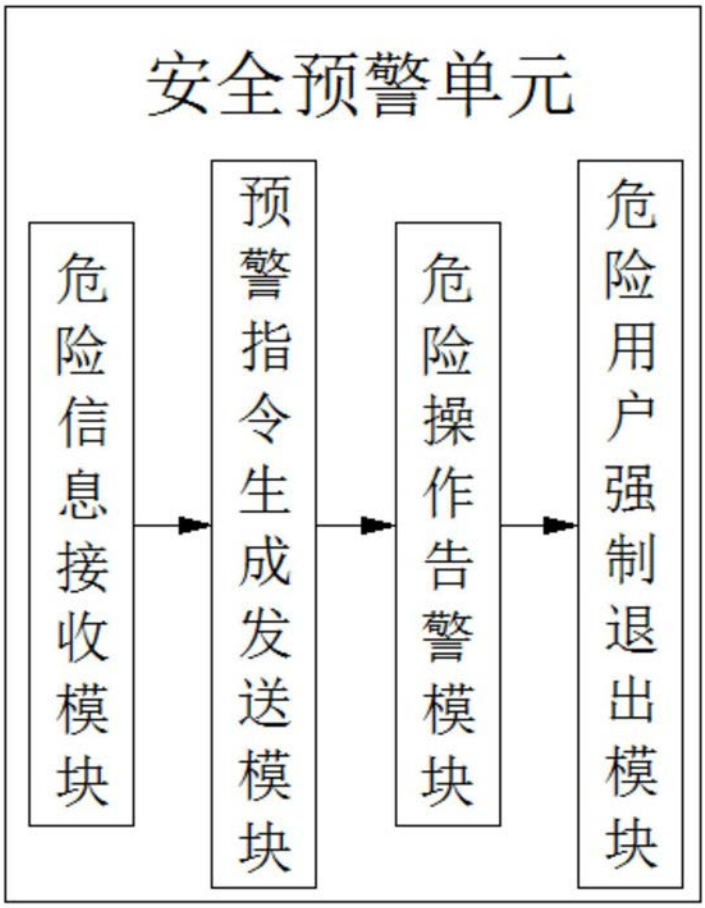


图3