(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 113791973 A
(43)申请公布日 2021.12.14

(21)申请号 202110972723.8
(22)申请日 2021.08.23
(71)申请人 湖北省农村信用社联合社网络信息中心
地址 430000 湖北省武汉市武昌区中北路1号
(72)发明人 荣容容 桂侃 张彤 李磊 陈广涛 李智 肖飞 罗小明 崔亚杰 张颖 武亮 刘龙
(74)专利代理机构 武汉蓝宝石专利代理事务所(特殊普通合伙) 42242
代理人 赵红万
(51)Int.Cl.
G06F 11/36(2006.01)
G06F 21/60(2013.01)
G06F 16/25(2019.01)

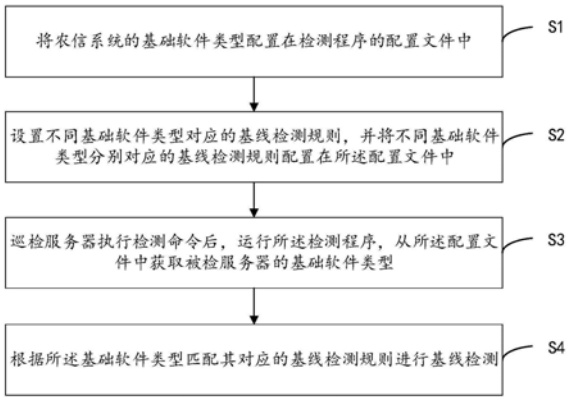
权利要求书2页 说明书6页 附图2页

(54)发明名称

基于农信系统的兼容性基线检测方法及系统

(57)摘要

本发明实施例提供了一种基于农信系统的兼容性基线检测方法及系统，首先将农信系统的基础软件类型配置在检测程序的配置文件中，并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中。在巡检服务器执行检测命令后，运行所述检测程序，从所述配置文件中获取被检服务器的基础软件类型。最后根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。本发明兼容农信系统中的各种常用的基础软件，如各种常用操作系统、数据库等。解决了现有的基线检查脚本只能检查某种系统，兼容性差，对多种基础软件的基线检测效率低下的问题。减少了人员参与作业的人力成本，降低了手工误操作风险，提高了基础软件基线检测效率。



CN 113791973 A

1.一种基于农信系统的兼容性基线检测方法,其特征在于,包括:

S1,将农信系统的基础软件类型配置在检测程序的配置文件中;

S2,设置不同基础软件类型对应的基线检测规则,并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中;

S3,巡检服务器执行检测命令后,运行所述检测程序,从所述配置文件中获取被检服务器的基础软件类型;

S4,根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。

2.根据权利要求1所述的基于农信系统的兼容性基线检测方法,其特征在于,所述基础软件类型至少包括操作系统和数据库系统;其中,操作系统至少包括AIX、Linux和Windows,数据库系统至少包括DB2和Oracle。

3.根据权利要求1所述的基于农信系统的兼容性基线检测方法,其特征在于,步骤S3具体包括:

巡检服务器执行检测命令后,远程调用被检测服务器上的检测程序,从所述配置文件中获取被检服务器的基础软件类型。

4.根据权利要求1所述的基于农信系统的兼容性基线检测方法,其特征在于,在步骤S3之后,该方法还包括:将被检服务器的已检测基础软件类型存储在指定文件中。

5.根据权利要求4所述的基于农信系统的兼容性基线检测方法,其特征在于,在步骤S3运行所述检测程序之后,该方法还包括:

若判断获知对基础软件进行二次检测,则从所述指定文件中获取存储的已检测基础软件类型,匹配其对应的基线检测规则进行基线检测。

6.根据权利要求2所述的基于农信系统的兼容性基线检测方法,其特征在于,步骤S4中,根据所述基础软件类型匹配其对应的基线检测规则进行基线检测,具体包括:若所述基础软件类型为数据库,则按照以下基线检测规则进行基线检测:

检测数据库的配置文件是否规范合理;

检测数据库的账号权限,检查各个权限账号是否有过多的不必要的权限,检测数据库的文件的权限,是否只归属数据库账户所有,其他程序是否可读可写;

检测数据库的网络连接端口对外的开放的程度,连接的安全性;

检测数据库是否可以运行危险语句。

7.根据权利要求2所述的基于农信系统的兼容性基线检测方法,其特征在于,步骤S4中,根据所述基础软件类型匹配其对应的基线检测规则进行基线检测,还包括:若所述基础软件类型为操作系统,则检测是否配置用户身份鉴别、建立分组、用户密码和访问控制。

8.根据权利要求1所述的基于农信系统的兼容性基线检测方法,其特征在于,在步骤S4之后,该方法还包括:

S5,基线检测完毕后,巡检服务器自动获取被检测服务器上的基线检测结果,生成检测报告。

9.一种基于农信系统的兼容性基线检测系统,其特征在于,包括:

配置模块,用于将农信系统的基础软件类型配置在检测程序的配置文件中;

设置模块,用于设置不同基础软件类型对应的基线检测规则,并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中;

软件类型检测模块，用于巡检服务器执行检测命令后，运行所述检测程序，从所述配置文件中获取被检服务器的基础软件类型；

基线检测模块，用于根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。

10.一种非暂态计算机可读存储介质，其上存储有计算机程序，其特征在于，该计算机程序被处理器执行时实现如权利要求1至8任一项所述基于农信系统的兼容性基线检测方法的步骤。

基于农信系统的兼容性基线检测方法及系统

技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种基于农信系统的兼容性基线检测方法及系统。

背景技术

[0002] 农信系统是农信银支付清算系统的简称，是根据全国农村信用社、农村合作银行、农村商业银行支付结算业务需求，应用现代化计算机网络和信息技术开发的集资金清算和信息服务为一体的支付清算平台，为所有入网机构提供异地支付清算和信息服务的系统。农信系统最初是以农村信用合作社为核心的，最早成立于上世纪50年代，起初目的是为了农民在资金上互帮互助。但随着时代的进步，逐渐发展为涉及范围更广的银行性质，主要业务是传统存贷款。

[0003] 目前，农信系统普遍构建了集传统业务和新兴业务于一体，覆盖同城、异地和跨行的统一的科技平台，业务发展多依赖于平台支撑，网络安全已经成为全系统重要的安全保障线，对农信系统进行安全基线检测对保障农信系统的安全运行非常重要。现有的基线检查脚本只能检查某种系统，并且通过手工运行某项基线检测。当对农信系统服务器中多种基础软件进行基线检测时，检测效率低下，检测不全。

[0004] 因此，现在亟需一种基于农信系统的兼容性基线检测方法及系统来解决上述问题。

发明内容

[0005] 本发明提供一种基于农信系统的兼容性基线检测方法及系统，用以解决目前基线检查脚本只能检查某种系统，当对农信系统服务器中多种基础软件进行基线检测时，检测效率低下，检测不全的问题。

[0006] 第一方面，本发明实施例提供一种基于农信系统的兼容性基线检测方法，包括：

[0007] S1，将农信系统的基础软件类型配置在检测程序的配置文件中；

[0008] S2，设置不同基础软件类型对应的基线检测规则，并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中；

[0009] S3，巡检服务器执行检测命令后，运行所述检测程序，从所述配置文件中获取被检服务器的基础软件类型；

[0010] S4，根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。

[0011] 优选的，所述基础软件类型至少包括操作系统和数据库系统；其中，操作系统至少包括AIX、Linux和Windows，数据库系统至少包括DB2和Oracle。

[0012] 优选的，步骤S3具体包括：

[0013] 巡检服务器执行检测命令后，远程调用被检测服务器上的检测程序，从所述配置文件中获取被检服务器的基础软件类型。

[0014] 优选的，在步骤S3之后，该方法还包括：将被检服务器的已检测基础软件类型存储

在指定文件中。

[0015] 优选的，在步骤S3运行所述检测程序之后，该方法还包括：

[0016] 若判断获知对基础软件进行二次检测，则从所述指定文件中获取存储的已检测基础软件类型，匹配其对应的基线检测规则进行基线检测。

[0017] 优选的，步骤S4中，根据所述基础软件类型匹配其对应的基线检测规则进行基线检测，具体包括：若所述基础软件类型为数据库，则按照以下基线检测规则进行基线检测：

[0018] 检测数据库的配置文件是否规范合理；

[0019] 检测数据库的账号权限，检查各个权限账号是否有过多的不必要的权限，检测数据库的文件的权限，是否只归属数据库账户所有，其他程序是否可读可写；

[0020] 检测数据库的网络连接端口对外的开放的程度，连接的安全性；

[0021] 检测数据库是否可以运行危险语句。

[0022] 优选的，步骤S4中，根据所述基础软件类型匹配其对应的基线检测规则进行基线检测，还包括：若所述基础软件类型为操作系统，则检测是否配置用户身份鉴别、建立分组、用户密码和访问控制。

[0023] 优选的，在步骤S4之后，该方法还包括：

[0024] S5，基线检测完毕后，巡检服务器自动获取被检测服务器上的基线检测结果，生成检测报告。

[0025] 第二方面，本发明实施例还提供一种基于农信系统的兼容性基线检测系统，包括：

[0026] 配置模块，用于将农信系统的基础软件类型配置在检测程序的配置文件中；

[0027] 设置模块，用于设置不同基础软件类型对应的基线检测规则，并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中；

[0028] 软件类型检测模块，用于巡检服务器执行检测命令后，运行所述检测程序，从所述配置文件中获取被检服务器的基础软件类型；

[0029] 基线检测模块，用于根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。

[0030] 第三方面，本发明实施例提供了一种电子设备，包括处理器、存储器、通信接口和总线；其中，所述处理器、存储器、通信接口通过所述总线完成相互间的通信；所述存储器存储有可被所述处理器执行的程序指令，所述处理器调用所述程序指令能够执行上述第一方面提供的基于农信系统的兼容性基线检测方法。

[0031] 第四方面，本发明实施例提供了一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令使所述计算机执行上述第一方面提供的基于农信系统的兼容性基线检测方法。

[0032] 本发明实施例提供的基于农信系统的兼容性基线检测方法及系统，首先将农信系统的基础软件类型配置在检测程序的配置文件中，并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中。在巡检服务器执行检测命令后，运行所述检测程序，从所述配置文件中获取被检服务器的基础软件类型。最后根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。本发明兼容农信系统中的各种常用的基础软件，如各种常用操作系统、数据库等。并且，减少了人员参与作业的人力成本，提高了基础软件基线检测效率。

附图说明

[0033] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0034] 图1是本发明实施例提供的一种基于农信系统的兼容性基线检测方法流程示意图；

[0035] 图2为本发明实施例提供的数据库的基线检测方法流程图。

[0036] 图3为本发明实施例提供的基于农信系统的兼容性基线检测系统的结构框图；

[0037] 图4为本发明实施例提供的电子设备的结构示意图。

具体实施方式

[0038] 为使本发明实施例的目的、技术方案和优点更加清楚，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他实施例，都属于本发明保护的范围。

[0039] 在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

[0040] 目前，农信系统普遍构建了集传统业务和新兴业务于一体，覆盖同城、异地和跨行的统一的科技平台，业务发展多依赖于平台支撑，网络安全已经成为全系统重要的安全保障线，对农信系统进行安全基线检测对保障农信系统的安全运行非常重要。现有的基线检查脚本只能检查某种系统，并且通过手工运行某项基线检测。当对农信系统服务器中多种基础软件进行基线检测时，检测效率低下，检测不全。

[0041] 因此，本发明实施例提出一种基于农信系统的兼容性基线检测方法，首先将农信系统的基础软件类型配置在检测程序的配置文件中，并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中。在巡检服务器执行检测命令后，运行所述检测程序，从所述配置文件中获取被检服务器的基础软件类型。最后根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。本发明兼容农信系统中的各种常用的基础软件，如各种常用操作系统、数据库等。解决了现有的基线检查脚本只能检查某种系统，兼容性差，对多种基础软件的基线检测效率低下的问题。以下将结合附图通过多个实施例进行展开说明和介绍。

[0042] 如图1所示，本发明实施例提供了一种基于农信系统的兼容性基线检测方法。首先对本发明实施例提供的方法的整体原理进行简要说明，该方法包括以下步骤：

[0043] 步骤S1，将农信系统的基础软件类型配置在检测程序的配置文件中。

[0044] 其中，信息系统的安全基线是一个信息系统的最小安全保证，即该信息系统最基本需要满足的安全要求。信息系统安全往往需要在付出成本与所能承受的安全风险之间进行平衡，而安全基线正是这个平衡的合理的分界线。若不满足系统最基本的安全要求，也就

无法承受由此带来的安全风险。

[0045] 因此,对农信系统进行安全基线检测对保障农信系统的安全运行非常重要。本申请的描述中,“基线”即是指“安全基线”。

[0046] 农信系统中使用的基础软件类型比较相似,本实施例中,农信系统的基础软件类型至少包括操作系统和数据库系统;其中,操作系统至少包括AIX系统、Linux系统和Windows系统,数据库系统至少包括DB2数据库和Oracle数据库。农信系统的基础软件类型还可以包括中间件、语言处理系统和办公软件。

[0047] 步骤S2,设置不同基础软件类型对应的基线检测规则,并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中。

[0048] 本实施例预先设置不同基础软件类型对应的基线检测规则,例如,分别设置AIX系统、Linux系统、Windows系统、DB2数据库和Oracle数据库各自对应的基线检测规则。将不同基础软件类型及其分别对应的基线检测规则配置在检测程序的配置文件中,为后续的基线检测作准备。

[0049] 步骤S3,巡检服务器执行检测命令后,运行所述检测程序,从所述配置文件中获取被检服务器的基础软件类型。

[0050] 具体地,在执行步骤S3之前,首先将检测程序通过巡检服务器批量部署到被检服务器上。然后执行S3,检测开始时,在巡检服务器执行检测命令,远程调用被检测服务器上的检测程序,从所述配置文件中获取被检服务器的基础软件类型。

[0051] 步骤S4,根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。

[0052] 若步骤S3获取的基础软件类型为操作系统,则检测是否配置用户身份鉴别、建立分组、用户密码和访问控制。

[0053] 若步骤S3获取的基础软件类型为数据库,则检测数据库的配置文件、账号权限、网络连接和危险语句,图2为本发明实施例提供的数据库的基线检测方法流程图,参照图2,数据库的基线检测具体包括以下步骤:

[0054] 201,检测数据库的配置文件是否规范合理;

[0055] 202,检测数据库的账号权限,检查各个权限账号是否有过多的不必要的权限,检测数据库的文件的权限,是否只归属数据库账户所有,其他程序是否可读可写;

[0056] 203,检测数据库的网络连接端口对外的开放的程度,连接的安全性;

[0057] 204,检测数据库是否可以运行危险语句。

[0058] 可以理解的是,在农信系统中,由于服务器数量较多,现有的基础软件基线检查的方式一般为抽样检查及优先检查重要系统,在选中的服务器上面登录,以手工输入命令行的方式检查,检查后将结果汇总,检测效率低下。并且,现有基线检查脚本只能检查某种系统,兼容性较差。而本发明提供的基于农信系统的兼容性基线检测方法,能兼容各种基础软件,操作系统如AIX、Linux,数据库如DB2、Oracle等。自动检测服务器上安装的基础软件的类型,并根据软件类型,检测软件的基线。

[0059] 本发明实施例提供的基于农信系统的兼容性基线检测方法及系统,首先将农信系统的基础软件类型配置在检测程序的配置文件中,并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中。在巡检服务器执行检测命令后,运行所述检测程序,从所述配置文件中获取被检服务器的基础软件类型。最后根据所述基础软件类型匹配其对应的

基线检测规则进行基线检测。本发明兼容农信系统中的各种常用的基础软件，如各种常用操作系统、数据库等。并且，减少了人员参与作业的人力成本，提高了基础软件基线检测效率。

[0060] 基于上述实施例的内容，在一个实施例中，在步骤S2之后，该方法还包括：将被检服务器的已检测基础软件类型存储在指定文件中。相应的，在步骤S2运行所述检测程序之后，基线检测还包括：若判断获知对基础软件进行二次检测，则从所述指定文件中获取存储的已检测基础软件类型，匹配其对应的基线检测规则进行基线检测。

[0061] 本发明实施例将被检服务器的已检测基础软件类型存储在指定文件中，以便于下次基线检测时能够直接获取基础软件类型，进一步提高了检测效率。

[0062] 基于上述实施例的内容，在一个实施例中，在步骤S4之后，该方法还包括：

[0063] S5，基线检测完毕后，巡检服务器自动获取被检测服务器上的基线检测结果，生成检测报告，并以农信系统的方式进行展示。

[0064] 本发明实施例中，在获得检测报告后，可以根据检测报告，对农信系统的基础软件给出合理的配置建议，以提高农信系统的信息安全。

[0065] 在一个实施例中，图3为本发明实施例提供的基于农信系统的兼容性基线检测系统的结构框图，参照图3，本发明实施例还提供一种基于农信系统的兼容性基线检测系统，包括：

[0066] 配置模块301，用于将农信系统的基础软件类型配置在检测程序的配置文件中；

[0067] 设置模块302，用于设置不同基础软件类型对应的基线检测规则，并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中；

[0068] 软件类型检测模块303，用于巡检服务器执行检测命令后，运行所述检测程序，从所述配置文件中获取被检服务器的基础软件类型；

[0069] 基线检测模块304，用于根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。

[0070] 可以理解的是，本发明提供的基于农信系统的兼容性基线检测系统，与前述各实施例提供的基于农信系统的兼容性基线检测方法相对应，具体的如何利用该系统进行基线检测，可以参照前述实施例中基于农信系统的兼容性基线检测方法的相关技术特征，本实施例在此不再赘述。

[0071] 本发明实施例提供的基于农信系统的兼容性基线检测系统，首先将农信系统的基础软件类型配置在检测程序的配置文件中，并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中。在巡检服务器执行检测命令后，运行所述检测程序，从所述配置文件中获取被检服务器的基础软件类型。最后根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。本发明兼容各种农信系统中的常用基础软件，如各种常用操作系统、数据库等。并且，减少了人员参与作业的人力成本，提高了基础软件基线检测效率。

[0072] 在一个实施例中，本发明实施例提供了本发明实施例提供了一种电子设备，如图4所示，该电子设备可以包括：处理器(processor)401、通信接口(Communications Interface)402、存储器(memory)403和通信总线404，其中，处理器401，通信接口402，存储器403通过通信总线404完成相互间的通信。处理器401可以调用存储器403中的逻辑指令，以执行上述各实施例提供的基于农信系统的兼容性基线检测方法的步骤，例如包括：S1，将

农信系统的基础软件类型配置在检测程序的配置文件中;S2,设置不同基础软件类型对应的基线检测规则,并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中;S3,巡检服务器执行检测命令后,运行所述检测程序,从所述配置文件中获取被检服务器的基础软件类型;S4,根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。

[0073] 在一个实施例中,基于相同的构思,本发明实施例还提供一种非暂态计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现以执行上述各实施例提供的基于农信系统的兼容性基线检测方法的步骤,例如包括:S1,将农信系统的基础软件类型配置在检测程序的配置文件中;S2,设置不同基础软件类型对应的基线检测规则,并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中;S3,巡检服务器执行检测命令后,运行所述检测程序,从所述配置文件中获取被检服务器的基础软件类型;S4,根据所述基础软件类型匹配其对应的基线检测规则进行基线检测。

[0074] 需要说明的是,在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详细描述的部分,可以参见其它实施例的相关描述。

[0075] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0076] 本发明是参照根据本发明实施例的方法、设备(方法)、和计算机程序产品的流程图和/或方框图来描述。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式计算机或者其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的方法。

[0077] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令方法的制造品,该指令方法实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0078] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0079] 尽管已描述了本发明的优选实施例,但本领域内的技术人员一旦得知了基本创造概念,则可对这些实施例作出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0080] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包括这些改动和变型在内。

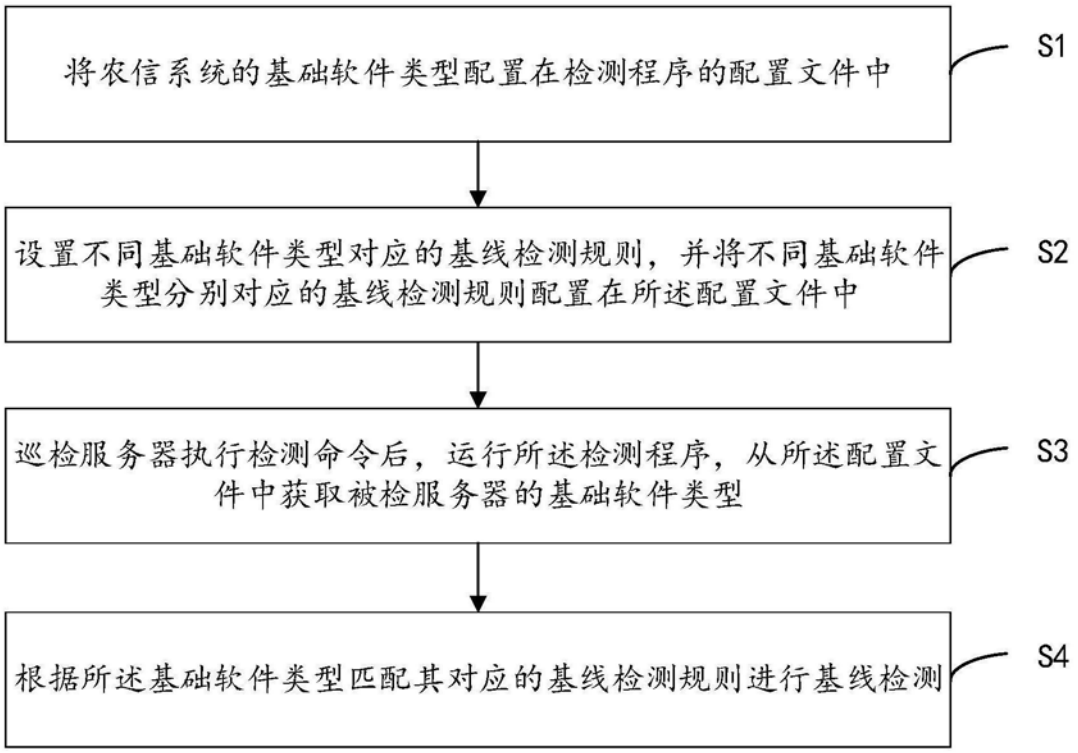

将农信系统的基础软件类型配置在检测程序的配置文件中
S1
设置不同基础软件类型对应的基线检测规则，并将不同基础软件类型分别对应的基线检测规则配置在所述配置文件中
S2
巡检服务器执行检测命令后，运行所述检测程序，从所述配置文件中获取被检服务器的基础软件类型
S3
根据所述基础软件类型匹配其对应的基线检测规则进行基线检测
S4

图1

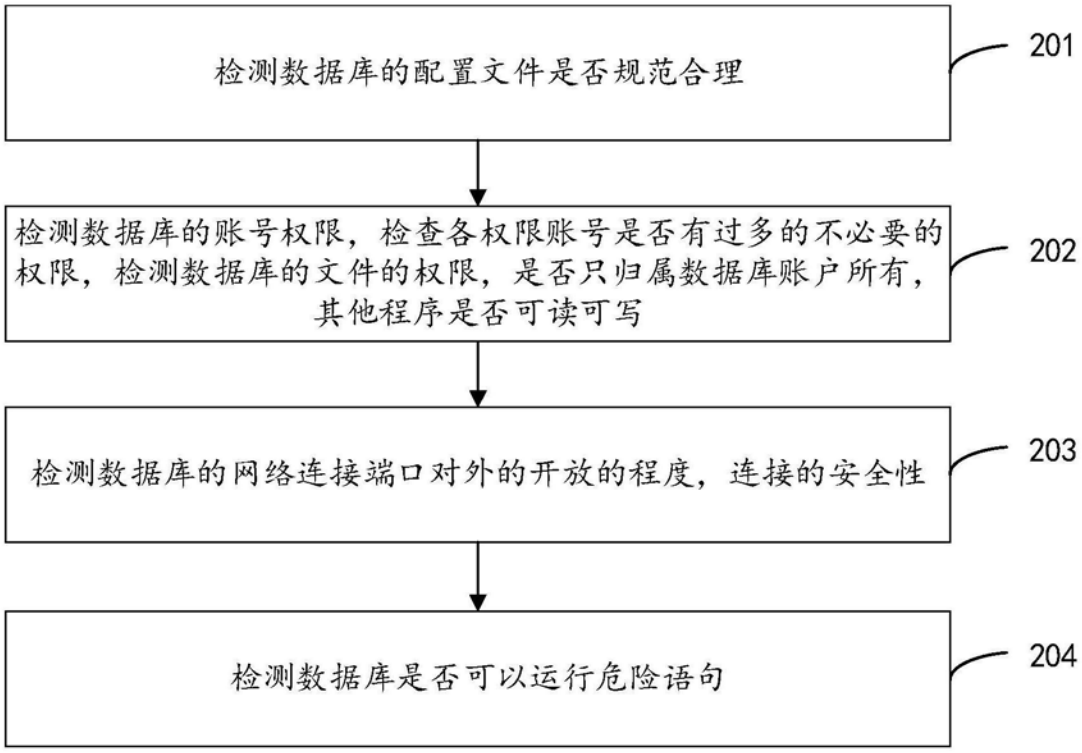

检测数据库的配置文件是否规范合理
201
检测数据库的账号权限，检查各权限账号是否有过多的不必要的权限，检测数据库的文件的权限，是否只归属数据库账户所有，其他程序是否可读可写
202
检测数据库的网络连接端口对外的开放的程度，连接的安全性
203
检测数据库是否可以运行危险语句
204

图2

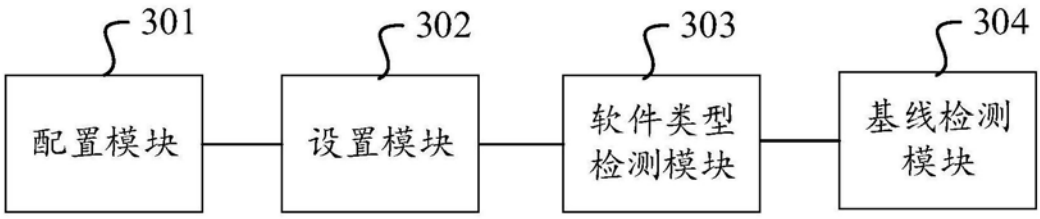

301
302
303
304
配置模块
设置模块
软件类型检测模块
基线检测模块

图3

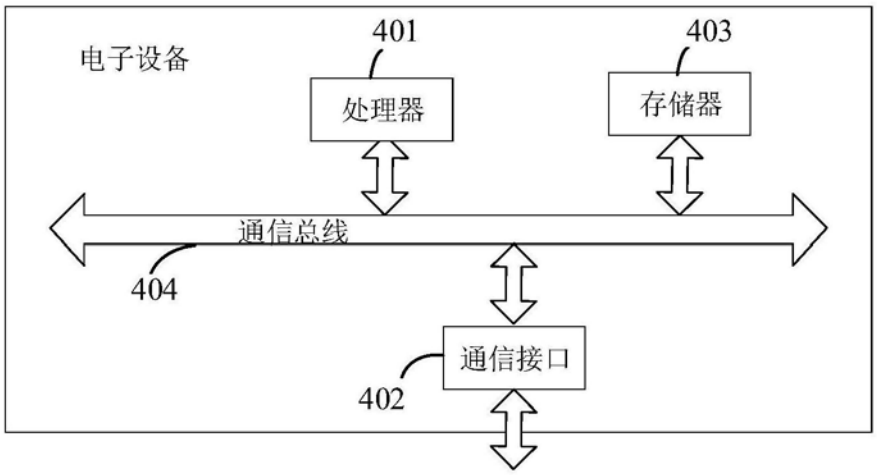

电子设备
401
处理器
403
存储器
通信总线
404
通信接口
402

图4