(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 106953874 B
(45)授权公告日 2019.11.29

(21)申请号 201710268929.6

(22)申请日 2017.04.21

(65)同一申请的已公布的文献号
申请公布号 CN 106953874 A

(43)申请公布日 2017.07.14

(73)专利权人 深圳市科力锐科技有限公司
地址 518055 广东省深圳市南山区桃源街道丽山路大学城创业园1010

(72)发明人 张勇

(74)专利代理机构 深圳市恒程创新知识产权代理有限公司 44542
代理人 赵爱蓉

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 104156665 A,2014.11.19,
CN 105678193 A,2016.06.15,
CN 103150511 A,2013.06.12,
CN 105245550 A,2016.01.13,
CN 102546253 A,2012.07.04,
CN 105978908 A,2016.09.28,
CN 103605737 A,2014.02.26,
CN 103944757 A,2014.07.23,
CN 104967628 A,2015.10.07,

审查员 彭帜

权利要求书2页 说明书6页 附图2页

(54)发明名称

网站防篡改方法及装置

(57)摘要

本发明公开了一种网站防篡改方法，所述方法包括以下步骤：监控网站服务器的状态数据；将监控获得的状态数据发送至分析系统，以使所述分析系统根据接收到的状态数据分析是否出现网站篡改，并反馈分析结果；在所述分析结果为出现网站篡改时，从备份系统中获取安全的备份点；根据所述安全的备份点对所述网站服务器进行还原。本发明还公开了一种网站防篡改装置。本发明在检测到网站篡改时，根据安全的备份点对网站服务器进行还原，从而有效地实现了网站防篡改。

CN 106953874 B

1.一种网站防篡改方法,其特征在于,所述方法包括以下步骤:

监控网站服务器的状态数据;

将监控获得的状态数据发送至分析系统,以使所述分析系统根据接收到的状态数据分析是否出现网站篡改,并反馈分析结果;

在所述分析结果为出现网站篡改时,从备份系统中获取安全的备份点;

根据所述安全的备份点对所述网站服务器进行还原;

其中,所述监控网站服务器的状态数据,具体包括:

爬取所述网站服务器的网站的单个或多个页面数据,将爬取的页面数据作为状态数据;

和/或,

获取所述网站服务器中操作系统的当前数据变化,并将所述当前数据变化作为状态数据;

和/或,

检测所述网站服务器中带有修改网站的文件操作行为以及出现的异常进程,将所述文件操作行为及异常进程作为状态数据。

2.如权利要求1所述的方法,其特征在于,所述从备份系统中获取安全备份点之前,所述方法还包括:

将所述当前数据变化发送至所述备份系统,以使所述备份系统根据预存的操作系统及接收到的当前数据变化生成备份点。

3.如权利要求1～2中任一项所述的方法,其特征在于,所述根据所述安全的备份点对所述网站服务器进行还原之后,所述方法还包括:

根据所述分析系统反馈的补丁文件对所述网站服务器进行修复,所述补丁文件由所述分析系统从漏洞管理平台中获取。

4.如权利要求3所述的方法,其特征在于,所述补丁文件由所述分析系统根据目标漏洞从漏洞管理平台中获取,所述目标漏洞由所述分析系统根据接收到的状态数据确定。

5.一种网站防篡改装置,其特征在于,所述装置包括:

数据监控模块,用于监控网站服务器的状态数据;

数据发送模块,用于将监控获得的状态数据发送至分析系统,以使所述分析系统根据接收到的状态数据分析是否出现网站篡改,并反馈分析结果;

备份获取模块,用于在所述分析结果为出现网站篡改时,从备份系统中获取安全的备份点;

备份还原模块,用于根据所述安全的备份点对所述网站服务器进行还原;

其中,所述数据监控模块,具体用于爬取所述网站服务器的网站的单个或多个页面数据,将爬取的页面数据作为状态数据;和/或,获取所述网站服务器中操作系统的当前数据变化,并将所述当前数据变化作为状态数据;和/或,检测所述网站服务器中带有修改网站的文件操作行为以及出现的异常进程,将所述文件操作行为及异常进程作为状态数据。

6.如权利要求5所述的装置,其特征在于,所述装置还包括:

备份生成模块,用于将所述当前数据变化发送至所述备份系统,以使所述备份系统根据预存的操作系统及接收到的当前数据变化生成备份点。

7.如权利要求5～6中任一项所述的装置,其特征在于,所述装置还包括:

补丁修复模块,用于根据所述分析系统反馈的补丁文件对所述网站服务器进行修复,所述补丁文件由所述分析系统从漏洞管理平台中获取。

8.如权利要求7所述的装置,其特征在于,所述补丁文件由所述备份服务器根据目标漏洞从漏洞管理平台中获取,所述目标漏洞由所述分析系统根据接收到的状态数据确定。

网站防篡改方法及装置

技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种网站防篡改方法及装置。

背景技术

[0002] 近年来网站被黑的事件层出不穷，篡改网页是黑客们常用的手法。防止网站被黑的最直接手段就是限制黑客对网页文件的修改，或者利用程序监控网页文件的变化，发现网页被改了就立即把网页改回来。前者的技术原理是通过文件过滤驱动拦截网页文件的写操作，来实现对网页文件的保护，但是黑客可以绕开文件系统，直接解析和修改磁盘数据，以达到篡改网页的目的。后者是监控程序利用文件系统的事件通知，或者定时对比网页文件内容，发现文件被改了，就执行恢复操作，把文件改回来。

[0003] 这样会存在一个问题：如果黑客不停的篡改网页，监控程序不停的执行恢复，那么系统会变得很繁忙，导致网站不可访问。还有一个问题就是，不管是事前的“限制”还是事后的“恢复”，都无法避免一个事实：这台主机系统已经被黑客入侵和控制了。虽然网站是安全的，但是这个主机系统是不安全的了，网站被篡改随时都有可能发生。例如，黑客可以把网站指向其他目录的文件，或者安装新的Web服务器软件，再把网站指向其他的目录，进而实现篡改网站的目的。这些篡改网站的行为，传统的防护方法是阻止不了的。

[0004] 上述内容仅用于辅助理解本发明的技术方案，并不代表承认上述内容是现有技术。

发明内容

[0005] 本发明的主要目的在于提供一种网站防篡改方法及装置，旨在解决现有技术中无法有效实现网站防篡改的技术问题。

[0006] 为实现上述目的，本发明提供一种网站防篡改方法，所述方法包括以下步骤：

[0007] 监控网站服务器的状态数据；

[0008] 将监控获得的状态数据发送至分析系统，以使所述分析系统根据接收到的状态数据分析是否出现网站篡改，并反馈分析结果；

[0009] 在所述分析结果为出现网站篡改时，从备份系统中获取安全的备份点；

[0010] 根据所述安全的备份点对所述网站服务器进行还原。

[0011] 优选地，所述监控网站服务器的状态数据，具体包括：

[0012] 爬取所述网站服务器的网站的的单个或多个页面数据，将爬取的页面数据作为状态数据；

[0013] 和/或，

[0014] 获取所述网站服务器中操作系统的当前数据变化，并将所述当前数据变化作为状态数据；

[0015] 和/或，

[0016] 检测所述网站服务器中带有修改网站的文件操作行为以及出现的异常进程，将所

述文件操作行为及异常进程作为状态数据。

[0017] 优选地，所述从备份系统中获取安全备份点之前，所述方法还包括：

[0018] 将所述当前数据变化发送至所述备份系统，以使所述备份系统根据预存的操作系统及接收到的当前数据变化生成备份点。

[0019] 优选地，所述根据所述安全的备份点对所述网站服务器进行还原之后，所述方法还包括：

[0020] 根据所述分析系统反馈的补丁文件对所述网站服务器进行修复，所述补丁文件由所述分析系统从漏洞管理平台中获取。

[0021] 优选地，所述补丁文件由所述分析系统根据目标漏洞从漏洞管理平台中获取，所述目标漏洞由所述分析系统根据接收到的状态数据确定。

[0022] 为实现上述目的，本发明还提供了一种网站防篡改装置，所述装置包括：

[0023] 数据监控模块，用于监控网站服务器的状态数据；

[0024] 数据发送模块，用于将监控获得的状态数据发送至分析系统，以使所述分析系统根据接收到的状态数据分析是否出现网站篡改，并反馈分析结果；

[0025] 备份获取模块，用于在所述分析结果为出现网站篡改时，从备份系统中获取安全的备份点；

[0026] 备份还原模块，用于根据所述安全的备份点对所述网站服务器进行还原。

[0027] 优选地，所述数据监控模块，具体用于爬取所述网站服务器的网站的的单个或多个页面数据，将爬取的页面数据作为状态数据；和/或，获取所述网站服务器中操作系统的当前数据变化，并将所述当前数据变化作为状态数据；和/或，检测所述网站服务器中带有修改网站的文件操作行为以及出现的异常进程，将所述文件操作行为及异常进程作为状态数据。

[0028] 优选地，所述装置还包括：

[0029] 备份生成模块，用于将所述当前数据变化发送至所述备份系统，以使所述备份系统根据预存的操作系统及接收到的当前数据变化生成备份点。

[0030] 优选地，所述装置还包括：

[0031] 补丁修复模块，用于根据所述分析系统反馈的补丁文件对所述网站服务器进行修复，所述补丁文件由所述分析系统从漏洞管理平台中获取。

[0032] 优选地，所述补丁文件由所述备份服务器根据目标漏洞从漏洞管理平台中获取，所述目标漏洞由所述分析系统根据接收到的状态数据确定。

[0033] 本发明在检测到网站篡改时，根据安全的备份点对网站服务器进行还原，从而有效地实现了网站防篡改。

附图说明

[0034] 图1为本发明第一种实施例的网站防篡改方法的流程示意图；

[0035] 图2为本发明第二种实施例的网站防篡改方法的流程示意图；

[0036] 图3为本发明第一种实施例的网站防篡改装置的功能模块示意图；

[0037] 图4为本发明第二种实施例的网站防篡改装置的功能模块示意图。

[0038] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0039] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0040] 参照图1，本发明第一实施例提供一种网站防篡改方法，所述方法包括：

[0041] S10：监控网站服务器的状态数据；

[0042] 需要说明的是，本实施例的方法的执行主体为AIO Agent程序，其运行于所述网站服务器上的操作系统中。

[0043] 可理解的是，所述网站服务器的状态数据即为可反映所述网站服务器的网站是否被篡改的数据，为保证确定网站是否被篡改的准确率，本实施例中，步骤S10可包括：爬取所述网站服务器的网站的的单个或多个页面数据，将爬取的页面数据作为状态数据；步骤S10也可包括：获取所述网站服务器中操作系统的当前数据变化，并将所述当前数据变化作为状态数据；步骤S10还可包括：检测所述网站服务器中带有修改网站的文件操作行为以及出现的异常进程，将所述文件操作行为及异常进程作为状态数据。

[0044] 在具体实现中，所述网站服务器即Web服务器，其设有驻留于因特网上的某种类型计算机的程序，可以向浏览器等Web客户端提供文档，也可以放置网站文件，让用户浏览，还可以放置数据文件，让用户下载。

[0045] S20：将监控获得的状态数据发送至分析系统，以使所述分析系统根据接收到的状态数据分析是否出现网站篡改，并反馈分析结果；

[0046] 需要说明的是，所述网站篡改即为篡改网站里面的网页，植入恶意的页面、网址、图片、文字，或者修改系统的配置、数据库等，也就是通常人们所说的网站被黑客入侵。

[0047] 可理解的是，所述分析系统即为用于分析是否出现网站篡改的程序，其可运行于所述网站服务器上的操作系统中，也可运行于其他服务器中，本实施例对此不加以限制。

[0048] 在具体实现中，所述分析系统会根据接收到的状态数据分析是否出现网站篡改，为了保证分析结果的准确性，本实施例中，所述分析系统可根据接收到的页面数据、当前数据变化、文件操作行为及异常进程分析是否出现网站篡改。

[0049] 对于页面数据可包括：页面中文字、图片及音视频的修改信息，所述分析系统对文字的修改信息的分析可包括：敏感字识别与对比，对图片、音视频的修改为完整全匹配对比。

[0050] S30：在所述分析结果为出现网站篡改时，从备份系统中获取安全的备份点。

[0051] 可理解的是，所述备份系统即为用于备份的程序，其可运行于所述网站服务器的操作系统中，但考虑到安全性问题，其还可运行于备份服务器的操作系统中。

[0052] 在具体实现中，把操作系统恢复到以前的某一个状态，这些状态叫备份点。如果某个备份点还没有发生过网站篡改事件，那么这个备份点也叫安全的备份点，通常所述安全的备份点可由所述备份系统根据预存的操作系统直接生成，但这种实现方式，在对所述网站服务器进行还原时，非常容易导致安全的备份点与当前时间距离过远，引起网页展示问题，为避免该问题，本实施例中，可由所述备份系统根据预存的操作系统及接收到的当前数据变化生成备份点，从而选取距离网站被篡改时间最接近的安全的备份点，对于当前数据变化而言，可采用定时获取的方式，也可采用连续数据保护(Continual Data Protection，CDP)的方式，即实时获取的方式。

[0053] S40：根据所述安全的备份点对所述网站服务器进行还原。

[0054] 可理解的是，在根据所述安全的备份点对所述网站服务器进行还原之前，可将网站服务器的后台关闭，启动精简的网站服务器程序，并将网页切换到维护模式，从而防止网站服务器进行还原的过程中出现网站无法访问的情况。

[0055] 另外，在根据所述安全的备份点对所述网站服务器进行还原之前，还可通过电子邮件、短信、电话通知管理员。

[0056] 本实施例在检测到网站篡改时，根据安全的备份点对网站服务器进行还原，从而有效地实现了网站防篡改。

[0057] 参照图2，图2为本发明网站防篡改方法第二实施例的流程示意图，基于上述图1所示的实施例，提出本发明网站防篡改方法的第二实施例。

[0058] 本实施例中，步骤S40之后，所述方法还包括：

[0059] S50：根据所述分析系统反馈的补丁文件对所述网站服务器进行修复，所述补丁文件由所述分析系统从漏洞管理平台中获取。

[0060] 为准确确定所述网站服务器存在的漏洞，在具体实现中，所述补丁文件由所述分析系统根据目标漏洞从漏洞管理平台中获取，所述目标漏洞由所述分析系统根据接收到的状态数据确定。

[0061] 在具体实现中，所述分析系统根据目标漏洞从漏洞管理平台中获取补丁文件时，如果漏洞管理平台存在对应的补丁文件，则下载下来，推送给AIO Agent程序，由AIO Agent程序负责根据补丁文件给所述网站服务器上的操作系统进行修复，如果漏洞管理平台不存在对应的补丁文件，分析系统后面会定期查询。

[0062] 可理解的是，所述漏洞管理平台可接收分析系统上报上来的漏洞信息，由漏洞分析人员根据漏洞信息，制作漏洞补丁文件，还可提供补丁文件下载服务，使得分析系统能够根据漏洞信息到漏洞管理平台下载对应的补丁文件。

[0063] 参照图3，本发明第一实施例提供一种网站防篡改装置，所述装置包括：

[0064] 数据监控模块10，用于监控网站服务器的状态数据；

[0065] 需要说明的是，本实施例的装置为AIO Agent程序，其运行于所述网站服务器上的操作系统中。

[0066] 可理解的是，所述网站服务器的状态数据即为可反映所述网站服务器的网站是否被篡改的数据，为保证确定网站是否被篡改的准确率，本实施例中，数据监控模块10可用于爬取所述网站服务器的网站的的单个或多个页面数据，将爬取的页面数据作为状态数据；数据监控模块10也可用于获取所述网站服务器中操作系统的当前数据变化，并将所述当前数据变化作为状态数据；数据监控模块10还可用于检测所述网站服务器中带有修改网站的文件操作行为以及出现的异常进程，将所述文件操作行为及异常进程作为状态数据。

[0067] 在具体实现中，所述网站服务器即Web服务器，其设有驻留于因特网上的某种类型计算机的程序，可以向浏览器等Web客户端提供文档，也可以放置网站文件，让用户浏览，还可以放置数据文件，让用户下载。

[0068] 数据发送模块20，用于将监控获得的状态数据发送至分析系统，以使所述分析系统根据接收到的状态数据分析是否出现网站篡改，并反馈分析结果；

[0069] 需要说明的是，所述网站篡改即为篡改网站里面的网页，植入恶意的页面、网址、图片、文字，或者修改系统的配置、数据库等，也就是通常人们所说的网站被黑客入侵。

[0070] 可理解的是，所述分析系统即为用于分析是否出现网站篡改的程序，其可运行于所述网站服务器上的操作系统中，也可运行于其他服务器中，本实施例对此不加以限制。

[0071] 在具体实现中，所述分析系统会根据接收到的状态数据分析是否出现网站篡改，为了保证分析结果的准确性，本实施例中，所述分析系统可根据接收到的页面数据、当前数据变化、文件操作行为及异常进程分析是否出现网站篡改。

[0072] 对于页面数据可包括：页面中文字、图片及音视频的修改信息，所述分析系统对文字的修改信息的分析可包括：敏感字识别与对比，对图片、音视频的修改为完整全匹配对比。

[0073] 备份获取模块30，用于在所述分析结果为出现网站篡改时，从备份系统中获取安全的备份点；

[0074] 可理解的是，所述备份系统即为用于备份的程序，其可运行于所述网站服务器的操作系统中，但考虑到安全性问题，其还可运行于备份服务器的操作系统中。

[0075] 在具体实现中，把操作系统恢复到以前的某一个状态，这些状态叫备份点。如果某个备份点还没有发生过网站篡改事件，那么这个备份点也叫安全的备份点，通常所述安全的备份点可由所述备份系统根据预存的操作系统直接生成，但这种实现方式，在对所述网站服务器进行还原时，非常容易导致安全的备份点与当前时间距离过远，引起网页展示问题，为避免该问题，本实施例中，可由所述备份系统根据预存的操作系统及接收到的当前数据变化生成备份点，从而选取距离网站被篡改时间最接近的安全的备份点，对于当前数据变化而言，可采用定时获取的方式，也可采用连续数据保护(Continual Data Protection，CDP)的方式，即实时获取的方式。

[0076] 备份还原模块40，用于根据所述安全的备份点对所述网站服务器进行还原。

[0077] 可理解的是，在根据所述安全的备份点对所述网站服务器进行还原之前，可将网站服务器的后台关闭，启动精简的网站服务器程序，并将网页切换到维护模式，从而防止网站服务器进行还原的过程中出现网站无法访问的情况。

[0078] 另外，在根据所述安全的备份点对所述网站服务器进行还原之前，还可通过电子邮件、短信、电话通知管理员。

[0079] 本实施例在检测到网站篡改时，根据安全的备份点对网站服务器进行还原，从而有效地实现了网站防篡改。

[0080] 参照图4，图4为本发明网站防篡改装置第二实施例的功能模块示意图，基于上述图3所示的实施例，提出本发明网站防篡改装置的第二实施例。

[0081] 本实施例中，所述装置还包括：

[0082] 补丁修复模块50，用于根据所述分析系统反馈的补丁文件对所述网站服务器进行修复，所述补丁文件由所述分析系统从漏洞管理平台中获取。

[0083] 为准确确定所述网站服务器存在的漏洞，在具体实现中，所述补丁文件由所述分析系统根据目标漏洞从漏洞管理平台中获取，所述目标漏洞由所述分析系统根据接收到的状态数据确定。

[0084] 在具体实现中，所述分析系统根据目标漏洞从漏洞管理平台中获取补丁文件时，如果漏洞管理平台存在对应的补丁文件，则下载下来，推送给AIO Agent程序，由AIO Agent程序负责根据补丁文件给所述网站服务器上的操作系统进行修复，如果漏洞管理平台不存

在对应的补丁文件，分析系统后面会定期查询。

[0085] 可理解的是，所述漏洞管理平台可接收分析系统上报上来的漏洞信息，由漏洞分析人员根据漏洞信息，制作漏洞补丁文件，还可提供补丁文件下载服务，使得分析系统能够根据漏洞信息到漏洞管理平台下载对应的补丁文件。

[0086] 需要说明的是，在本文中，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、物品或者系统不仅包括那些要素，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、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0087] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0088] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0089] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

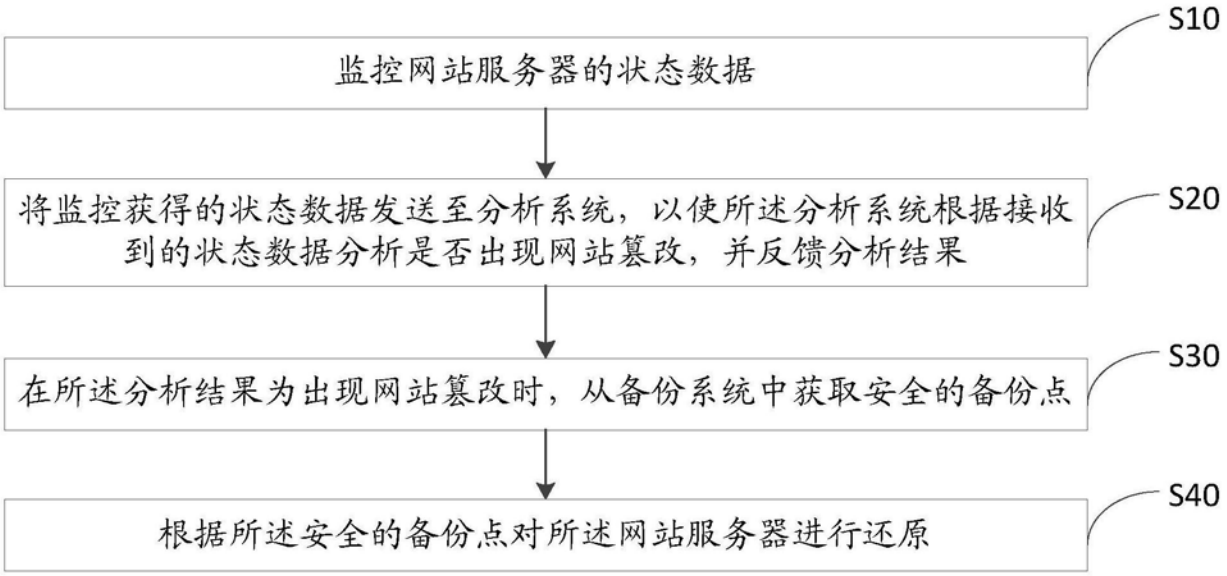
S10
监控网站服务器的状态数据
将监控获得的状态数据发送至分析系统，以使所述分析系统根据接收到的状态数据分析是否出现网站篡改，并反馈分析结果
S20
在所述分析结果为出现网站篡改时，从备份系统中获取安全的备份点
S30
根据所述安全的备份点对所述网站服务器进行还原
S40

图1

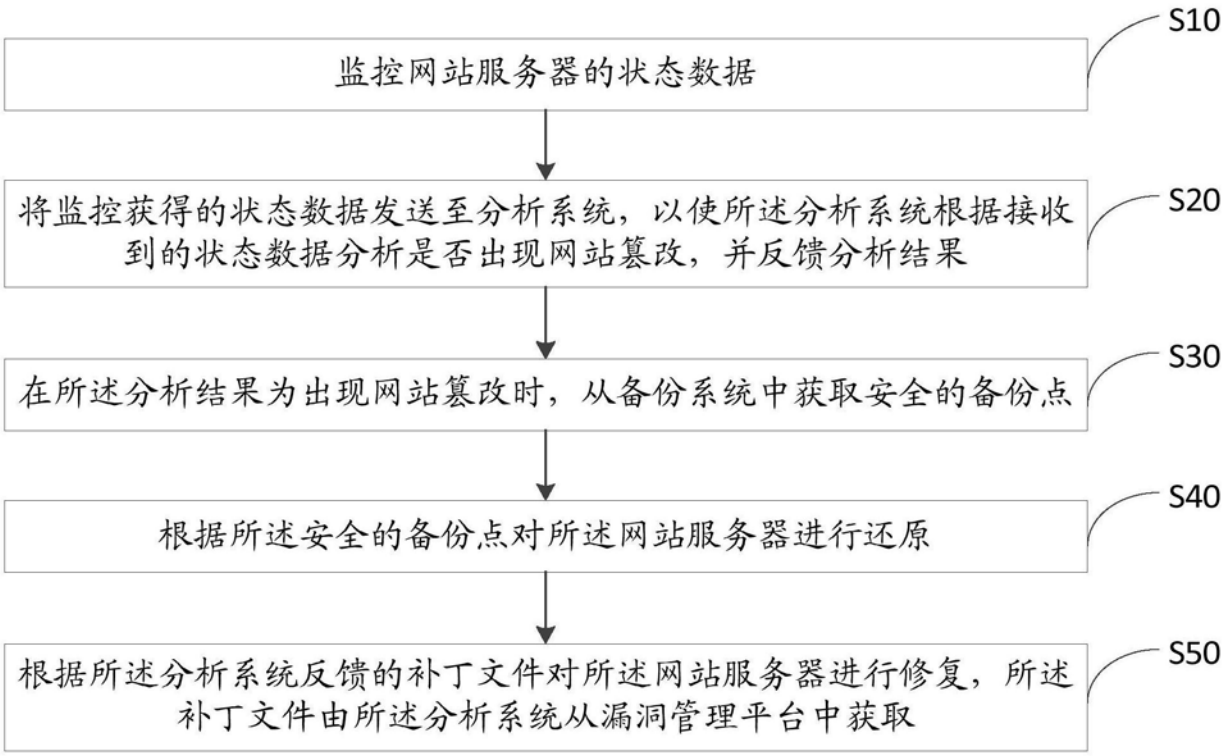
S10
监控网站服务器的状态数据
将监控获得的状态数据发送至分析系统，以使所述分析系统根据接收到的状态数据分析是否出现网站篡改，并反馈分析结果
S20
在所述分析结果为出现网站篡改时，从备份系统中获取安全的备份点
S30
根据所述安全的备份点对所述网站服务器进行还原
S40
根据所述分析系统反馈的补丁文件对所述网站服务器进行修复，所述补丁文件由所述分析系统从漏洞管理平台中获取
S50

图2

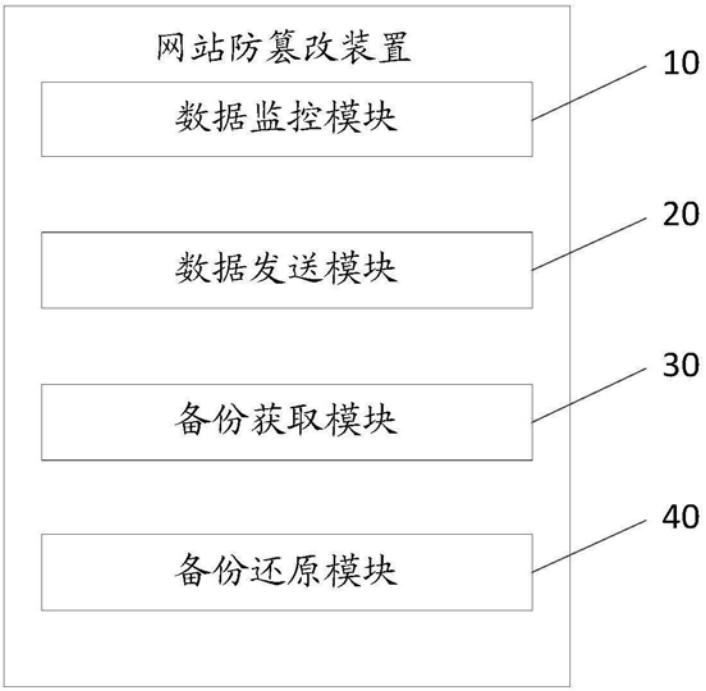
网站防篡改装置
数据监控模块
10
数据发送模块
20
备份获取模块
30
备份还原模块
40

图3

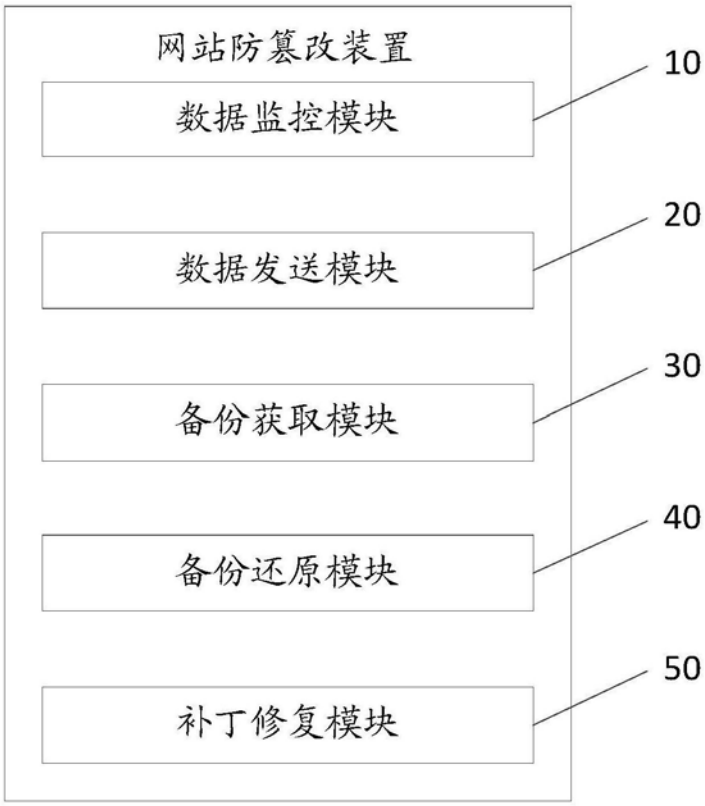
网站防篡改装置
数据监控模块
10
数据发送模块
20
备份获取模块
30
备份还原模块
40
补丁修复模块
50

图4