(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 107958322 A
(43)申请公布日 2018.04.24

(21)申请号 201710934868.2

(22)申请日 2017.10.09

(71)申请人 中国电子科技集团公司第二十八研究所
地址 210007 江苏省南京市秦淮区苜蓿园东街1号

(72)发明人 潘维 孙亭 李毅 丁杰 沈自然 叶云 周翠翠

(74)专利代理机构 北京中知法苑知识产权代理事务所(普通合伙) 11226
代理人 常玉明

(51)Int.Cl.
G06Q 10/06(2012.01)
G06Q 50/26(2012.01)
G06F 17/30(2006.01)
G06F 21/53(2013.01)
G06F 21/56(2013.01)
H04L 29/06(2006.01)
G06F 19/00(2018.01)

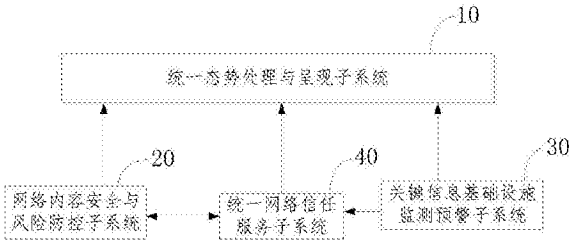
权利要求书4页 说明书11页 附图4页

(54)发明名称

一种城市网络空间综合治理系统

(57)摘要

本发明涉及一种城市网络空间综合治理系统，包括：统一态势处理与呈现子系统、网络内容安全与风险防控子系统、关键信息基础设施监测预警子系统和统一网络信任服务子系统；网络内容安全与风险管控子系统用于对城市网络空间媒体的信息进行实时采集，并进行提取和舆情分析；关键信息基础设施监测预警子系统用于对城市通信网络、联网工控识别及电磁环境进行监测；统一网络信任服务子系统用于对电子政务资源中心的现有身份信息进行汇聚，对实名用户进行管理；统一态势处理与呈现子系统用于对安全态势汇聚和处理。本发明的系统，能够实现对城市关键信息基础设施运行情况的网络内容安全综合监管，实现对城市网络空间安全统一态势和系统响应。



CN 107958322 A

1.一种城市网络空间综合治理系统，其特征在于，包括：统一态势处理与呈现子系统、网络内容安全与风险防控子系统、关键信息基础设施监测预警子系统和统一网络信任服务子系统；

其中，所述网络内容安全与风险管控子系统用于对城市网络空间媒体的信息进行实时采集，并对采集的内容进行提取和舆情分析；

所述关键信息基础设施监测预警子系统用于对城市通信网络、联网工控识别及电磁环境进行监测；

所述统一网络信任服务子系统用于对电子政务资源中心的现有身份信息进行汇聚，对实名用户进行管理、统一身份认证及信任评估；

统一态势处理与呈现子系统用于对网络空间综合治理分系统其他子系统的安全态势汇聚和处理，并结合GIS地理信息，反映城市整个网络空间所处的安全状况；

其中，所述内容安全与风险防控子系统向统一态势处理与呈现子系统提供安全态势及预警数据，向统一网络信任服务子系统提供网络行为日志及用户操作日志；关键信息基础设施监测预警子系统向统一态势处理与呈现子系统提供基础设施预警信息，向统一网络信任服务子系统提供网络行为日志及用户操作日志；统一网络信任服务子系统分别向内容安全与风险防控子系统及统一态势处理与呈现子系统提供用户实名信息。

2.根据权利要求1所述系统，其特征在于，所述统一态势处理与呈现子系统，具体包括：

事件采集单元，用于从高级威胁监测、工控威胁感知各分系统获取态势展现的事件数据；

格式检查单元，用于对获取的态势展现相关数据进行格式检查；对于格式符合的直接转入数据处理单元，格式不符合者，格式检查单元对其进行调整处理，然后再转入数据处理单元；

数据处理单元，用于按照系统数据标准，对获取的各分系统数据进行归一化、标准化的数据预处理；

基础资产态势单元，用于展示基础资产安全态势；

安全防护态势单元，用于展示网络空间当前安全防护态势，显示当前网络空间内各基础资源的安全级别；

安全危险态势单元，用于通过地图展示网络空间当前安全威胁态势。

3.根据权利要求2所述的系统，其特征在于，所述事件采集单元采集的事件数据包括网络入侵事件数据、工控系统威胁事件数据和网络舆情事件数据。

4.根据权利要求1所述的系统，其特征在于，所述网络内容安全与风险防控子系统，具体包括：

内容风险预警单元，用于按用户自定义类别对内容风险进行分类展示，对所有信息进行地域判断、敏感性判断、应急事件主题判断，对于判断为敏感、应急事件主题的信息，即时在页面上显示；

敏感事件跟踪单元，用于对内容风险预警单元判定的敏感事件进行全网监控以及跟踪分析，并识别重点网民和/或重点网站；

重点网民跟踪单元，用于对敏感事件跟踪单元识别的重点网民进行实施跟踪，并根据情况对所述重点网民的言论进行调控；

属地网站查询单元，用于对敏感事件跟踪单元识别的重点网站进行属地查询及管理。

5.根据权利要求4所述的系统，其特征在于，所述内容风险预警单元包括普通预警模式和应急预警模式，所述普通预警模式用于对敏感信息进行预警，所述应急预警模式用于对应急事件主题进行预警。

6.根据权利要求4所述的系统，其特征在于，所述敏感事件跟踪单元对敏感事件进行跟踪分析，具体包括：

对敏感事件进行热度评估、最新报道、网民观点、媒体传播途径以及事件进展趋势的跟踪和分析。

7.根据权利要求4所述的系统，其特征在于，所述敏感事件跟踪单元，具体地，通过对事件相关的所有信息内容的搜集，计算事件随时间变化的热度趋势，了解事件的最新报道，并对所采集的网民评论转发数据，基于情感分析技术，计算展示网络民众对事件的情感态度和主要观点，当发现重点网民时，则将信息推送至重点网民跟踪单元处理。

8.根据权利要求4所述的系统，其特征在于，所述重点网民跟踪单元，具体地用于，对重点人物聚焦，支持对监控对象的基本资料、最新发布信息的查看，识别监控对象发布的敏感和/或信息，分析监控对象言论兴趣及虚拟社会关系；识别网络上的与其关联的多个ID账号，并且当对重点网民跟踪时，对跟踪的重点网民的言论进行实时调控。

9.根据权利要求4所述的系统，其特征在于，所述属地网站查询单元，具体地用于，通过网页URL查询所示网站的网站备案地、接入地、联系人和联系方式，当网站不在辖属范围内时，查找其ICP备案号或IP地址所在属地，通过上级相关部门的协调实现对涉事网站的管理。

10.根据权利要求1所述的系统，其特征在于，所述关键信息基础设施监测预警子系统，具体包括：

APT威胁监测单元，用于通过入侵监测、反病毒和信誉检测识别已知威胁，同时开展针对大数据中心网络的异常分析，识别未知威胁；

城市联网工控威胁感知单元，用于深度识别工控设备信息，关联工控漏洞库，进行数据融合，对城市联网工控安全态势进行可视化呈现；

电磁污染监测单元，用于通过前端小型化的高性能电磁污染感应器及相应的传输技术，对电磁环境污染信息进行监测感知，并将监测系统得来的信息，为电磁辐射监测治理提供决策依据，再通过电磁环境评估污染治理系统对城市电磁环境进行集中整治，保障电磁环境空间的安全。

11.根据权利要求10所述的系统，其特征在于，所述APT威胁监测单元，具体地，用于在全网进行数据采集，识别应用协议，内容还原；对还原的样本文件反病毒检测，识别已知恶意代码；对还原的会话数据进行攻击特征检测；基于信誉检测，实时识别恶意的IP攻击和恶意网址访问；基于关联分析和机器学习挖掘网络异常行为。

12.根据权利要求10所述的系统，其特征在于，所述城市联网工控威胁感知单元，具体地，通过工业控制系统接入互联网威胁态势感知系统主动扫描、识别各区域范围内联网工控设备，直观呈现城市基础设施工控系统联网态势，感知并分析工业控制相关威胁，主动预警安全风险；指导企业及时修补安全漏洞，更新安全策略；形成城市联网工控系统主动威胁感知能力，使城市管理者掌握基础设施联网设备的信息安全态势和存在风险。

13.根据权利要求1所述的系统，其特征在于，所述APT高级威胁监测单元，具体包括：

采集探针，用于为所述APT高级威胁监测系统提供数据，具备高速网络数据采集、应用协议识别、协议内容还原和流量还原的功能；

静态特征监测子单元，用于基于信誉库和特征库进行静态检测；

沙箱动态分析子单元，用于实现对未知恶意代码的检测；

异常行为分析子单元，用于接收到采集探针、静态特征检测、沙箱动态分析的日志信息，进行预处理关联后，然后进行威胁场景分析和行为基线分析，最后根据日志的类型进行数据存储；

风险可视化展示子单元，用于实现攻击可视化呈现和可视化分析。

14.根据权利要求13所述的系统，其特征在于，所述采集探针，具体地，通过零拷贝技术的采集引擎实现实时网络数据采集，然后进行链路层、网络层、传输层的预处理解析，根据会话流哈希进行负载均衡分发；通过深度内容识别和深度协议识别引擎进行应用协议的识别，并通过特定的应用协议解析插件实现深度的内容还原。

15.根据权利要求13所述的系统，其特征在于，所述静态特征监测子单元基于信誉库和特征库进行静态检测，具体包括：反病毒检测、入侵检测、信誉库检测；

所述反病毒检测利用第三方病毒库，对网络流量中的样本文件进行特征检测，识别恶意代码程序；

所述入侵检测用于进行攻击特征检测，识别各种嗅探扫描和漏洞攻击等；

所述信誉库监测用于基于恶意IP、恶意网址和域名进行信誉检测，实时识别恶意的IP和恶意网址。

16.根据权利要求13所述的系统，其特征在于，所述沙箱动态分析子单元，具体地，通过虚拟化技术，对可疑样本进行行为仿真分析，通过行为分析和威胁评分的方法识别未知的恶意代码程序。

17.根据权利要求13所述的系统，其特征在于，所述风险可视化展示子单元，用于基于攻击图、攻击树的图谱分析技术，实现风险事件和主机的下钻分析和攻击路径回溯分析，并基于可视化图表实现高级威胁的可视化展现。

18.根据权利要求10所述的系统，其特征在于，所述城市联网工控威胁感知单元，具体地包括：

多维度检索子单元，用于对用户提交的关键字进行检索及数据的可视化展示；

实施扫描子单元，用于扫描任务的实时跟踪及展示，实时扫描模块由扫描引擎提供数据驱动，能够对城市联网工控的威胁感知过程进行可视化展示；

任务配置子单元，用于联网工控威胁感知任务的可视化配置和跟踪；

深度扫描分析子单元，用于探知联网工控的指纹信息并解析与威胁相关的关键参数，利用无状态探测技术感知联网工控的深度参数；

指纹字典库子单元，用于管理工控协议指纹和工控设备指纹及联网工控指纹的匹配和识别。

19.根据权利要求1所述的系统，其特征在于，所述电磁污染监测单元，具体包括：

电磁数据采集子单元，用于通过前端小型化电磁监测传感器采用宽频段感知技术和扫频式监测技术实现检测、分析电磁环境中各种复杂电磁辐射射频频率成分、电磁电场辐射

强度；

态势呈现子单元，用于使电磁环境的频谱态势通过预设的形式呈现；

业务辅助决策和综合展示，用于对电磁环境的频谱监测和管理的辅助决策，并结合关心的电磁频段、场强大小进行电磁监测数据的查询、统计；

电磁监测管理，用于通过电磁环境的频谱感知、呈现和展示，结合一定的决策依据，进行对电磁环境监测分析和管理的综合功能，保障电磁环境空间的安全。

20.根据权利要求1所述的系统，其特征在于，所述统一网络信任服务子系统，具体包括：

实名用户管理单元，用于对用户身份信息及属性日常的增加、删除、修改等集中管理，对实名信息发布访问控制，对用户实名服务；

统一身份认证单元，用于屏蔽底层认证基础设施的差异，以服务接口的方式对外提供统一认证服务，支持不同类型和强度的身份验证；

信任评估单元，用于采集、存储、分析、处理系统中各种用户操作和访问信息，对网络实体进行信任度评估，对网络中实体行为进行关联，对网络事件进行举证、对可疑行为进行评估。

一种城市网络空间综合治理系统

技术领域

[0001] 本发明涉及智慧城市技术领域，具体涉及一种城市网络空间综合治理系统。

背景技术

[0002] 当前，智慧城市建设已由物理空间向网络空间发展，智慧城市通过完善通信与信息基础设施，构建数据共享与整合平台，为城市提供包括市民管理与服务、企业管理与服务、城市管理与运营，是一个复杂的系统工程，其中既有政府和企业的业务信息系统，也有面向市民提供公共服务的市民服务系统。同时还面临着城市间信息化融合所带来的互信和安全等共性问题。

[0003] 就整个智慧城市的建设而言，安全问题尤为突出、严重，随着智慧城市快速发展和应用系统应用深化，对信息技术的依赖日趋严重，服务范围变广、应用交互增多、数据交换频繁、系统构建复杂度增大，城市信息安全问题已经成为事关城市经济和社会稳定的重大问题，成为了城市管理者重点关注的牵一发而动全身的问题。目前大部分城市在此方面的安全体系还不是很完善、安全措施还不是很到位、安全防护能力亟待提高。

发明内容

[0004] 针对现有技术存在的缺陷，本发明提供了一种城市网络空间综合治理系统，能够实现对城市关键信息基础设施运行情况的网络内容安全综合监管，实现对城市网络空间安全统一态势和系统响应。

[0005] 本发明的一个目的是提供了一种城市网络空间综合治理系统，包括：统一态势处理与呈现子系统、网络内容安全与风险防控子系统、关键信息基础设施监测预警子系统和统一网络信任服务子系统；

[0006] 其中，所述网络内容安全与风险管控子系统用于对城市网络空间媒体的信息进行实时采集，并对采集的内容进行提取和舆情分析；

[0007] 所述关键信息基础设施监测预警子系统用于对城市通信网络、联网工控识别及电磁环境进行监测；

[0008] 所述统一网络信任服务子系统用于对电子政务资源中心的现有身份信息进行汇聚，对实名用户进行管理、统一身份认证及信任评估；

[0009] 统一态势处理与呈现子系统用于对网络空间综合治理分系统其他子系统的安全态势汇聚和处理，并结合GIS地理信息，反映城市整个网络空间所处的安全状况；

[0010] 其中，所述内容安全与风险防控子系统向统一态势处理与呈现子系统提供安全态势及预警数据，向统一网络信任服务子系统提供网络行为日志及用户操作日志；关键信息基础设施监测预警子系统向统一态势处理与呈现子系统提供基础设施预警信息，向统一网络信任服务子系统提供网络行为日志及用户操作日志；统一网络信任服务子系统分别向内容安全与风险防控子系统及统一态势处理与呈现子系统提供用户实名信息。

[0011] 其中，所述统一态势处理与呈现子系统，具体包括：

[0012] 事件采集单元，用于从高级威胁监测、工控威胁感知各分系统获取态势展现的事件数据；

[0013] 格式检查单元，用于对获取的态势展现相关数据进行格式检查；对于格式符合的直接转入数据处理单元，格式不符合者，格式检查单元对其进行调整处理，然后再转入数据处理单元；

[0014] 数据处理单元，用于按照系统数据标准，对获取的各分系统数据进行归一化、标准化的数据预处理；

[0015] 基础资产态势单元，用于展示基础资产安全态势；

[0016] 安全防护态势单元，用于展示网络空间当前安全防护态势，显示当前网络空间内各基础资源的安全级别；

[0017] 安全危险态势单元，用于通过地图展示网络空间当前安全威胁态势。

[0018] 其中，所述事件采集单元采集的事件数据包括网络入侵事件数据、工控系统威胁事件数据和网络舆情事件数据。

[0019] 其中，所述网络内容安全与风险防控子系统，具体包括：

[0020] 内容风险预警单元，用于按用户自定义类别对内容风险进行分类展示，对所有信息进行地域判断、敏感性判断、应急事件主题判断，对于判断为敏感、应急事件主题的信息，即时在页面上显示；

[0021] 敏感事件跟踪单元，用于对内容风险预警单元判定的敏感事件进行全网监控以及跟踪分析，并识别重点网民和/或重点网站；

[0022] 重点网民跟踪单元，用于对敏感事件跟踪单元识别的重点网民进行实施跟踪，并根据情况对所述重点网民的言论进行调控；

[0023] 属地网站查询单元，用于对敏感事件跟踪单元识别的重点网站进行属地查询及管理。

[0024] 其中，所述内容风险预警单元包括普通预警模式和应急预警模式，所述普通预警模式用于对敏感信息进行预警，所述应急预警模式用于对应急事件主题进行预警。

[0025] 其中，所述敏感事件跟踪单元对敏感事件进行跟踪分析，具体包括：

[0026] 对敏感事件进行热度评估、最新报道、网民观点、媒体传播途径以及事件进展趋势的跟踪和分析。

[0027] 其中，所述敏感事件跟踪单元，具体地，通过对事件相关的所有信息内容的搜集，计算事件随时间变化的热度趋势，了解事件的最新报道，并对所采集的网民评论转发数据，基于情感分析技术，计算展示网络民众对事件的情感态度和主要观点，当发现重点网民时，则将信息推送至重点网民跟踪单元处理。

[0028] 其中，所述重点网民跟踪单元，具体地用于，对重点人物聚焦，支持对监控对象的基本资料、最新发布信息的查看，识别监控对象发布的敏感和/或信息，分析监控对象言论兴趣及虚拟社会关系；识别网络上的与其关联的多个ID账号，并且当对重点网民跟踪时，对跟踪的重点网民的言论进行实时调控。

[0029] 其中，所述属地网站查询单元，具体地用于，通过网页URL查询所示网站的网站备案地、接入地、联系人和联系方式，当网站不在辖属范围内时，查找其ICP备案号或IP地址所在属地，通过上级相关部门的协调实现对涉事网站的管理。

[0030] 其中，所述关键信息基础设施监测预警子系统，具体包括：

[0031] APT威胁监测单元，用于通过入侵监测、反病毒和信誉检测识别已知威胁，同时开展针对大数据中心网络的异常分析，识别未知威胁；

[0032] 城市联网工控威胁感知单元，用于深度识别工控设备信息，关联工控漏洞库，进行数据融合，对城市联网工控安全态势进行可视化呈现；

[0033] 电磁污染监测单元，用于通过前端小型化的高性能电磁污染感应器及相应的传输技术，对电磁环境污染信息进行监测感知，并将监测系统得来的信息，为电磁辐射监测治理提供决策依据，再通过电磁环境评估污染治理系统对城市电磁环境进行集中整治，保障电磁环境空间的安全。

[0034] 其中，所述APT威胁监测单元，具体地，用于在全网进行数据采集，识别应用协议，内容还原；对还原的样本文件反病毒检测，识别已知恶意代码；对还原的会话数据进行攻击特征检测；基于信誉检测，实时识别恶意的IP攻击和恶意网址访问；基于关联分析和机器学习挖掘网络异常行为。

[0035] 其中，所述城市联网工控威胁感知单元，具体地，通过工业控制系统接入互联网威胁态势感知系统主动扫描、识别各区域范围内联网工控设备，直观呈现城市基础设施工控系统联网态势，感知并分析工业控制相关威胁，主动预警安全风险；指导企业及时修补安全漏洞，更新安全策略；形成城市联网工控系统主动威胁感知能力，使城市管理者掌握基础设施联网设备的信息安全态势和存在风险。

[0036] 其中，所述APT高级威胁监测单元，具体包括：

[0037] 采集探针，用于为所述APT高级威胁监测系统提供数据，具备高速网络数据采集、应用协议识别、协议内容还原和流量还原的功能；

[0038] 静态特征监测子单元，用于基于信誉库和特征库进行静态检测；

[0039] 沙箱动态分析子单元，用于实现对未知恶意代码的检测；

[0040] 异常行为分析子单元，用于接收到采集探针、静态特征检测、沙箱动态分析的日志信息，进行预处理关联后，然后进行威胁场景分析和行为基线分析，最后根据日志的类型进行数据存储；

[0041] 风险可视化展示子单元，用于实现攻击可视化呈现和可视化分析。

[0042] 其中，所述采集探针，具体地，通过零拷贝技术的采集引擎实现实时网络数据采集，然后进行链路层、网络层、传输层的预处理解析，根据会话流哈希进行负载均衡分发；通过深度内容识别和深度协议识别引擎进行应用协议的识别，并通过特定的应用协议解析插件实现深度的内容还原。

[0043] 其中，所述静态特征监测子单元基于信誉库和特征库进行静态检测，具体包括：反病毒检测、入侵检测、信誉库检测；

[0044] 所述反病毒检测利用第三方病毒库，对网络流量中的样本文件进行特征检测，识别恶意代码程序；

[0045] 所述入侵检测用于进行攻击特征检测，识别各种嗅探扫描和漏洞攻击等；

[0046] 所述信誉库监测用于基于恶意IP、恶意网址和域名进行信誉检测，实时识别恶意的IP和恶意网址。

[0047] 其中，所述沙箱动态分析子单元，具体地，通过虚拟化技术，对可疑样本进行行为

仿真分析，通过行为分析和威胁评分的方法识别未知的恶意代码程序。

[0048] 其中，所述风险可视化展示子单元，用于基于攻击图、攻击树的图谱分析技术，实现风险事件和主机的下钻分析和攻击路径回溯分析，并基于可视化图表实现高级威胁的可视化展现。

[0049] 其中，所述城市联网工控威胁感知单元，具体地包括：

[0050] 多维度检索子单元，用于对用户提交的关键字进行检索及数据的可视化展示；

[0051] 实施扫描子单元，用于扫描任务的实时跟踪及展示，实时扫描模块由扫描引擎提供数据驱动，能够对城市联网工控的威胁感知过程进行可视化展示；

[0052] 任务配置子单元，用于联网工控威胁感知任务的可视化配置和跟踪；

[0053] 深度扫描分析子单元，用于探知联网工控的指纹信息并解析与威胁相关的关键参数，利用无状态探测技术感知联网工控的深度参数；

[0054] 指纹字典库子单元，用于管理工控协议指纹和工控设备指纹及联网工控指纹的匹配和识别。

[0055] 其中，所述电磁污染监测单元，具体包括：

[0056] 电磁数据采集子单元，用于通过前端小型化电磁监测传感器采用宽频段感知技术和扫频式监测技术实现检测、分析电磁环境中各种复杂电磁辐射射频频率成分、电磁电场辐射强度；

[0057] 态势呈现子单元，用于使电磁环境的频谱态势通过预设的形式呈现；

[0058] 业务辅助决策和综合展示，用于对电磁环境的频谱监测和管理的辅助决策，并结合关心的电磁频段、场强大小进行电磁监测数据的查询、统计；

[0059] 电磁监测管理，用于通过电磁环境的频谱感知、呈现和展示，结合一定的决策依据，进行对电磁环境监测分析和管理的综合功能，保障电磁环境空间的安全。

[0060] 其中，所述统一网络信任服务子系统，具体包括：

[0061] 实名用户管理单元，用于对用户身份信息及属性日常的增加、删除、修改等集中管理，对实名信息发布访问控制，对用户实名服务；

[0062] 统一身份认证单元，用于屏蔽底层认证基础设施的差异，以服务接口的方式对外提供统一认证服务，支持不同类型和强度的身份验证：

[0063] 信任评估单元，用于采集、存储、分析、处理系统中各种用户操作和访问信息，对网络实体进行信任度评估，对网络中实体行为进行关联，对网络事件进行举证、对可疑行为进行评估。

[0064] 本发明的城市网络空间综合治理系统，能够对网络空间进行全方位、立体化的监控，有效实现对城市网络空间安全统一态势和系统响应，实现对智慧城市健康度指数的动态量化评估。

附图说明

[0065] 图1示出了本发明的城市网络空间综合治理系统的结构框图。

[0066] 图2示出了本发明的统一态势处理与呈现子系统的软件架构图。

[0067] 图3示出了本发明的关键信息基础设施监测预警子系统中APT高级威胁监测单元的软件架构图。

[0068] 图4示出了本发明的关键信息基础设施监测预警子系统中城市联网工控威胁感知单元的软件架构图。

[0069] 图5示出了本发明的关键信息基础设施监测预警子系统中电磁污染监测单元的软件架构图。

[0070] 图6示出了本发明的统一网络信任服务子系统的软件架构图。

具体实施方式

[0071] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明，应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

[0072] 现在将详细参考本发明的实施例，这些实施例的示例在附图中示出。元件的后缀“模块”和“单元”在此用于方便描述，并且因此可以可交换地被使用，而且没有任何可区别的意义或功能。

[0073] 虽然构成本发明的实施例的所有元件或单元被描述为结合到单个元件中或被操作为单个元件或单元，但是本发明不一定局限于此种实施例。根据实施例，在本发明的目的和范围内所有的元件可以选择性地结合到一个或多个元件并且被操作为一个或多个元件。

[0074] 本发明的实施例的城市网络空间综合治理系统，通过数据资源采集接入、网络舆情监测预警、网络用户信任管理、关键信息基础设施监测预警以及全面态势呈现五个方面组成。

[0075] 本实施例中，数据资源采集接入，是系统通过Webserivice方式从第三方网络内容数据源搜集网络内容数据，比如微博、微信、门户网站、论坛等；通过Webservice方式从各级网信办处搜集网络舆情信息；通过Webservice方式或者Api方式从第三方病毒库获取病毒特征数据；以Webservice方式从电子政府资源中心、信息安全测评中心获取用户实名信息。

[0076] 网络舆情监测预警，是首先对网络内容风险进行预警，自动找出网络敏感事件，进而通过敏感事件跟踪单元对网络敏感事件进行追踪分析，在对事件追踪分析的过程中，当识别出重点网民时，则通过重点网民跟踪单元实时追踪重点人物，并根据情况对其言论进行调控；当识别出重点网站时，通过属地网站查询单元对涉事网站进行属地查询，如果属于管辖范围内，则进行本地管理，如果在管辖范围外，则通过上级相关部门的协调实现对涉事网站的管理。数据采集的网络爬虫采用Pyspider框架实现，第三方数据采用HTTP Get请求，以XML/JSON格式采集数据。实时分析系统基于大数据平台的实时计算框架storm集群实现，数据通信采用Kafka集群。离线分析采用基于大数据平台的MapReduce实现，分析数据直接从HDFS分布式文件中提取，分析结果首先存在Hive库，处理后采用MySQL存储。

[0077] 网络用户信任管理，是对采集到的用户信息，进行身份认证及实名服务。通过SOA的服务架构以及统一的服务协议规范，与各种认证基础设施进行交互，共同构建覆盖全市的统一网络信任服务体系，通过网络内容安全隔离技术进行受控的数据摆渡，防止用户信息泄露。安全服务层的实现采用基于Web Services框架的服务实现技术及规范。包含WS-Trust、WS-Secure Conversation、WS-Federation、WS-Policy、WS-Authorization等系列应用服务安全标准规范和SAML、XACML等断言及授权机制。

[0078] 关键信息基础设施监测预警，是基于采集到的网络关键信息基础设施数据，采用

深度内容检测DPI识别技术、基于流量特征DFI协议识别技术等实现应用协议的分析；采用反病毒检测、入侵检测、信誉库等技术实现静态特征检测，识别恶意程序；采用虚拟机仿真技术、API Hook技术对样本进行沙箱动态监测，包括进程行为、文件行为、注册表行为、内存行为等；采用指令跟踪技术；采用基于威胁场景的事件关联分析、基于自然语言处理和数据挖掘的随机域名DGA识别、利用通信行为特征等技术实现对命令控制通道的监测。采用Web可视化技术，实现对安全威胁可视化呈现。

[0079] 全面态势呈现，是基于网络舆情监测预警信息、网络用户信任管理信息、关键信息基础设施监测预警信息，首先利用统计学习方法对三类信息进行融合分析，对分析出来的信息利用WebGL技术进行可视化的展现，具体展示的信息包括基础资产态势、安全防护态势、安全威胁态势。

[0080] 基于上述框架，本发明的一个实施例中，如图1所示，提供一种城市网络空间综合治理系统，具体包括：统一态势处理与呈现子系统10、网络内容安全与风险防控子系统20、关键信息基础设施监测预警子系统30和统一网络信任服务子系统40；

[0081] 其中，统一态势处理与呈现子系统10用于对网络空间综合治理分系统其他子系统的安全态势汇聚和处理，并结合GIS地理信息，反映城市整个网络空间所处的安全状况；是用于提供城市网络空间整体安全态势呈现能力，汇聚网络空间综合治理各子系统的呈现内容，提供丰富直观的安全态势监控展示。

[0082] 网络内容安全与风险管控子系统20用于对城市网络空间媒体的信息进行实时采集，并对采集的内容进行提取和舆情分析。

[0083] 具体地，提供城市网络空间(新闻、论坛、博客/微博、微信、新闻客户端等)新媒体的信息发布、评论、回复、转发等信息的实时采集、内容提取和舆情分析能力，从意识形态、反恐维稳、国家安全、网络舆情等不同的维度展现城市网络空间内容态势。

[0084] 关键信息基础设施监测预警子系统30用于对城市通信网络、联网工控识别及电磁环境进行监测。具体地，提供城市网络空间面向高级持续性威胁的监测和分析能力，实现对已知威胁监测的同时，重点对未知漏洞、特种木马、APT高级攻击等未知威胁活动进行实时监测和响应。

[0085] 统一网络信任服务子系统40用于对电子政务资源中心的现有身份信息进行汇聚，对实名用户进行管理、统一身份认证及信任评估。即提供对用户实名信息、网络身份标识的集中管理，对用户实名信息的访问进行认证和授权。

[0086] 上述实施例中，网络内容安全与风险防控子系统20向统一态势处理与呈现子系统10提供安全态势及预警数据，向统一网络信任服务子系统提供网络行0为日志及用户操作日志；关键信息基础设施监测预警子系统30向统一态势处理与呈现子系统10提供基础设施预警信息，向统一网络信任服务子系统40提供网络行为日志及用户操作日志；统一网络信任服务子系统40分别向网络内容安全与风险防控子系统20及统一态势处理与呈现子系统10提供用户实名信息。

[0087] 在进一步的实施例中，统一态势处理与呈现子系统10具体包括：

[0088] 事件采集单元，用于从高级威胁监测、工控威胁感知等各分系统获取态势展现相关数据，如网络入侵事件、工控系统威胁事件、网络舆情事件等。

[0089] 格式检查单元，用于对获取的态势展现相关数据进行格式检查格式符合的直接转

入数据处理单元，格式不符合者，格式检查单元对其进行调整处理，然后再转入数据处理单元。

[0090] 数据处理单元，用于按照系统数据标准，对获取的各分系统数据进行归一化、标准化的数据预处理。

[0091] 基础资产态势单元，用于展示城市关键基础设施和重点制造企业工控系统等基础资产安全态势。

[0092] 安全防护态势单元，用于展示网络空间当前安全防护态势，显示当前网络空间内各基础资源的安全级别。

[0093] 安全危险态势单元，用于展示网络空间当前安全威胁态势，主要通过2D地图、3D地图方式展现。

[0094] 具体地，统一态势处理与呈现子系统10的软件架构如图2所示，分为数据接入层、数据处理层、业务逻辑层和应用展现层。数据采集支持多种数据采集方式，负责事件采集、格式检查和写入数据中心。综合态势来通过汇聚城市网络空间安全信息数据，并进行关联性融合分析，通过2D图形显示方式，结合GIS地理信息，反映整个网络空间所处的安全状况，综合安全态势包括：基础资产态势、安全防护态势、安全威胁态势。

[0095] 进一步地，网络内容安全与风险防控子系统20，首先对网络内容风险进行预警，自动找出网络敏感事件，进而通过敏感事件跟踪单元对网络敏感事件进行追踪分析，在对事件追踪分析的过程中，当识别出重点网民时，则通过重点网民跟踪单元实时追踪重点人物，并根据情况对其言论进行调控；当识别出重点网站时，通过属地网站查询单元对涉事网站进行属地查询，如果属于管辖范围内，则进行本地管理，如果在管辖范围外，则通过上级相关部门的协调实现对涉事网站的管理。

[0096] 基于上述，网络内容安全与风险防控子系统20，具体包括：

[0097] 内容风险预警单元，用于按用户自定义类别(政治、民生、安全、环境、经济、卫生)对内容风险进行分类展示，对所有信息进行地域判断、敏感性判断、应急事件主题判断，对于判断为敏感、应急事件主题的信息，即时在页面上显示。预警模式可选择普通或应急模式，普通模式对所有敏感信息预警，应急模式仅对应急事件主题进行预警。

[0098] 敏感事件跟踪单元，用于对指定敏感事件进行全网监控，可进行热度评估、最新报道、网民观点、媒体传播路径、事件进展趋势等方面进行分析，分析出某一事件的网上舆情动态。通过对事件相关的所有信息内容(新闻、论坛、微博、微信、移动端等)的搜集，计算事件随时间变化的热度趋势，此过程中可了解到事件的最新报道，进而对所采集的网民评论转发数据，基于情感分析技术，计算展示网络民众对事件的情感态度和主要观点，当发现重点网民时，则将信息推送至重点网民跟踪单元处理。

[0099] 重点网民跟踪单元，用于对重点人物聚焦，支持对监控对象的基本资料、最新发布信息的查看，识别监控对象发布的敏感(负面)信息；能够分析监控对象言论兴趣及虚拟社会关系；能够识别网络上的与其关联的多个ID账号。(重点网民即发布大量负面信息，且发布信息被其他网民多次转载)当对重点网民跟踪时，可对其言论进行实时调控。

[0100] 属地网站查询单元，用于通过网页URL查询所示网站的网站备案地、接入地、联系人和联系方式等信息。当网站不在辖属范围内时，查找其ICP备案号或IP地址所在属地，通过上级相关部门的协调实现对涉事网站的管理。

[0101] 进一步的实施例中，关键信息基础设施监测预警子系统30具体包括：

[0102] APT威胁监测单元，用于通过入侵监测、反病毒和信誉检测识别已知威胁，同时开展针对大数据中心网络的异常分析，识别未知威胁。全网数据采集，识别应用协议，内容还原；对还原的样本文件反病毒检测，识别已知恶意代码；对还原的会话数据进行攻击特征检测；基于信誉检测，实时识别恶意的IP攻击和恶意网址访问；基于关联分析和机器学习挖掘网络异常行为。

[0103] 城市联网工控威胁感知单元，用于深度识别工控设备信息，关联工控漏洞库，进行数据融合，对城市联网工控安全态势进行可视化呈现。工业控制系统接入互联网威胁态势感知系统主动扫描、识别各区域范围内联网工控设备，直观呈现城市基础设施工控系统联网态势，感知并分析工业控制相关威胁，主动预警安全风险；指导企业及时修补安全漏洞，更新安全策略；形成城市联网工控系统主动威胁感知能力，使城市管理者掌握基础设施联网设备的信息安全态势和存在风险。

[0104] 电磁污染监测单元，用于通过前端小型化的高性能电磁污染感应器及相应的传输技术，对电磁环境污染信息进行监测感知，并将监测系统得来的信息，为电磁辐射监测治理提供决策依据，再通过电磁环境评估污染治理系统对城市电磁环境进行集中整治，保障电磁环境空间的安全。

[0105] 进一步地，APT高级威胁监测单元，具体包括：

[0106] 采集探针，用于作为APT高级威胁监测系统的数据来源，具备高速网络数据采集、应用协议识别、协议内容还原和流量还原的功能。通过零拷贝技术的采集引擎实现实时网络数据采集，然后进行链路层、网络层、传输层的预处理解析，根据会话流哈希进行负载均衡分发。通过深度内容识别和深度协议识别引擎进行应用协议的识别，并通过特定的应用协议解析插件实现深度的内容还原。

[0107] 静态特征监测子单元，用于基于信誉库和特征库等进行静态检测，主要包括反病毒检测、入侵检测、信誉库检测等。反病毒检测主要利用第三方病毒库，对网络流量中的样本文件进行特征检测，识别病毒、木马、蠕虫、僵尸等恶意代码程序；入侵检测主要进行攻击特征检测，识别各种嗅探扫描和漏洞攻击等；信誉库监测主要基于恶意IP、恶意网址和域名进行信誉检测，实时识别恶意的IP和恶意网址。

[0108] 沙箱动态分析子单元，用于实现对未知恶意代码的检测。沙箱动态分析主要通过虚拟化技术，对可疑样本进行行为仿真分析，通过行为分析和威胁评分的方法识别未知的恶意代码程序。

[0109] 异常行为分析子单元，用于接收到采集探针、静态特征检测、沙箱动态分析的日志信息，首先进行资产、分组、地域等预处理关联后，然后进行威胁场景分析和行为基线分析，最后根据日志的类型进行数据存储。

[0110] 风险可视化展示子单元，用于实现攻击可视化呈现和可视化分析。基于攻击图、攻击树的图谱分析技术，实现风险事件和主机的下钻分析和攻击路径回溯分析等，基于各种饼图、柱图、地图等可视化图表实现高级威胁的可视化展现。

[0111] 又一个实施例中，城市联网工控威胁感知单元，具体地包括：

[0112] 多维度检索子单元，用于对用户提交的关键字进行检索及数据的可视化展示，实现按设备类型、厂商、型号、版本等关键字检索及多种关键字组合检索功能。

[0113] 实施扫描子单元，用于扫描任务的实时跟踪及展示，实时扫描模块由扫描引擎提供数据驱动，能够对城市联网工控的威胁感知过程进行可视化展示，包括设备的分布情况、威胁漏洞等信息。

[0114] 任务配置子单元，用于联网工控威胁感知任务的可视化配置和跟踪，可按工控协议、端口、自定义IP段等多种方式进行配置。

[0115] 深度扫描分析子单元，用于探知联网工控的指纹信息并解析与威胁相关的关键参数，利用无状态探测技术感知联网工控的开放端口、运行服务、安全信息等深度参数。

[0116] 指纹字典库子单元，用于管理工控协议指纹和工控设备指纹及联网工控指纹的匹配和识别。

[0117] 此外，电磁污染监测单元，具体包括：

[0118] 电磁数据采集子单元，用于通过前端小型化电磁监测传感器采用宽频段感知技术和扫频式监测技术实现检测、分析电磁环境中各种复杂电磁辐射射频频率成分、电磁电场辐射强度等；

[0119] 态势呈现子单元，用于使电磁环境的频谱态势呈现，主要让“看不见”的电磁频谱通过一定的方式呈现出来。

[0120] 业务辅助决策和综合展示，用于对电磁环境的频谱监测和管理的辅助决策，并结合关心的电磁频段、场强大小进行电磁监测数据的查询、统计。

[0121] 电磁监测管理，用于通过电磁环境的频谱感知、呈现和展示，结合一定的决策依据，进行对电磁环境监测分析和管理的综合功能，保障电磁环境空间的安全。

[0122] 本实施例中，如图3所示，APT高级威胁监测模块软件架构分为数据采集层、数据分析层及Web应用层，数据采集层利用采集探针进行数据采集，数据分析层提供静态检测、沙箱行为分析、异常行为挖掘，Web应用层提供态势呈现及配置管理功能。

[0123] 进一步地，如图4所示，城市联网工控威胁感知模块软件架构分为任务调度层、扫描引擎层、数据层、Web服务层及展示层，展示层是为内部应用搭建统一接口，实现数据、业务、应用集成的公共平台，提供对检索数据进行静态或动态的可视化展示功能。Web服务层主要是为上层的业务系统提供各类基础的服务，为展示层提供可视化组件模块。数据层提供数据的持久化存储服务，为可视化层提供数据驱动，实现对城市联网工控系统的威胁态势信息，工控漏洞知识库，联网工控系统深度信息等信息的存储。扫描引擎层负责感知接入互联网的工业控制系统和设备，实现联网工控系统和设备的辨识。任务调度层负责扫描任务的配置、分布式分发，以及扫描集群负载均衡、故障冗余、状态监控等；

[0124] 再一步地，如图5所示，电磁污染监测模块软件架构分为数据层、支撑层、服务层及应用层。数据层是监测信息感知和数据采集的基础，主要包括前端小型化电磁监测传感器及相应的传输途径。支撑层利用各软件技术，确保信息数据的高质量采。服务层将电磁环境安全监测系统中的监测与业务应用紧密结合起来，形成有机联动的整体。应用层将监测系统得来的信息，为电磁辐射监测治理提供决策依据，再通过电磁环境评估污染治理系统对城市电磁环境进行集中整治，保障电磁环境空间的安全。

[0125] 在进一步的实施例中，统一网络信任服务子系统，具体包括：

[0126] 实名用户管理单元，用于对用户身份信息及属性日常的增加、删除、修改等集中管理，对实名信息发布访问控制，对用户实名服务。

[0127] 统一身份认证单元，用于屏蔽底层认证基础设施的差异，以服务接口的方式对外提供统一认证服务，支持不同类型和强度的身份验证。

[0128] 信任评估单元，用于采集、存储、分析、处理系统中各种用户操作和访问信息，对网络实体进行信任度评估，对网络中实体行为进行关联，对网络事件进行举证、对可疑行为进行评估。

[0129] 本实施例中，如图6所示，统一网络信任服务子系统包括实名用户管理、统一身份认证及信任评估等模块，其软件架构分为数据层、认证层、服务层及应用层。应用层是统一网络信任服务子系统涉及的应用系统总和。在服务层屏蔽了网络应用与特定的认证基础设施联系，形成了覆盖全网的认证体系。系统支持不同认证模式、认证算法的用户在授权后合理访问业务系统。由于应用系统存储的是用户的电子身份标识而非用户实名信息，从而保护了用户的真实身份，起到了隐私保护的作用。服务层直接为应用系统提供公共服务。安全服务层根据安全协议对应用层的认证请求进行响应，为网络实体提供签名和认证等服务，为网络舆情监控系统提供责任认定等实名服务，支撑舆情监控系统将网络异常行为定位到具体的实名用户。安全服务层将底层基础设施实现的功能封装成为标准的服务接口统一发布。各类业务系统作为服务使用者，只需依据统一服务接口标准所定义的调用方法就能调用统一身份认证服务。基础设施层作为用户身份认证的基础功能设备，可包含多种形式的用户身份载体，为具体的用户身份认证提供实际操作运算。数据层作为用户电子信息数据以及用户网络操作行为日志存储、管理的基础设施，为统一网络信任服务提供数据存储服务。按照约定服务协议，将用户的电子身份与网络行为等信息进行存储，必要时为网络内容安全治理提供最原始的证据，使得网络内容安全事件有源可溯。为智慧城市提供不间断的数据存取，数据校验，以及数据备份保护等服务。标准规范体系用来约定统一网络信任服务子系统各服务层级之间/层内的通信协议、认证协议、访问接口等标准，是架构在安全标准之上的规范。安全保障体系是保障统一网络信任服务子系统自身的安全体系，包括访问控制、权限管理等。

[0130] 本发明的城市网络空间综合治理系统，能够对网络空间进行全方位、立体化的监控，有效实现对城市网络空间安全统一态势和系统响应，实现对智慧城市健康度指数的动态量化评估。

[0131] 应当理解，在本说明书中描述的功能单元或能力可被称为或标示为组件、模块或系统，以便更具体地强调它们的实现独立。例如，组件、模块或系统可被实现为硬件电路，其包括定制超大规模集成(VLSI)电路或门阵列、现成的半导体，诸如逻辑芯片、晶体管，或其他分立组件。组件或模块还可在可编程硬件设备中实现，诸如场可编程门阵列、可编程阵列逻辑、可编程逻辑设备等。组件或模块还可以在用于由各种类型的处理器执行的软件中实现。例如，可执行代码的识别的组件或模块可以包括一个或多个物理或逻辑的计算机指令，其可以，例如，被组织为对象、程序或功能。然而，所识别的组件或模块不必在物理上定位在一起，而是可以包含存储在不同位置的全异指令，其当逻辑上接合在一起时，包含组件或模块并实现对于组件或模块的规定目的。

[0132] 应该理解由本领域技术人员通过本发明能够实现的效果并不局限于在上文已特别描述的内容，并且本发明的其它优点从上面的详细描述中将更清楚地理解。

[0133] 对于本领域技术人员，显然可以在不脱离本发明的精神或范围的情况下在本发明

中做出各种修改和变型。因此，本发明旨在如果本发明的修改和变型落入附随权利要求和它们的等同形式的范围内，那么本发明覆盖这些修改和变型。

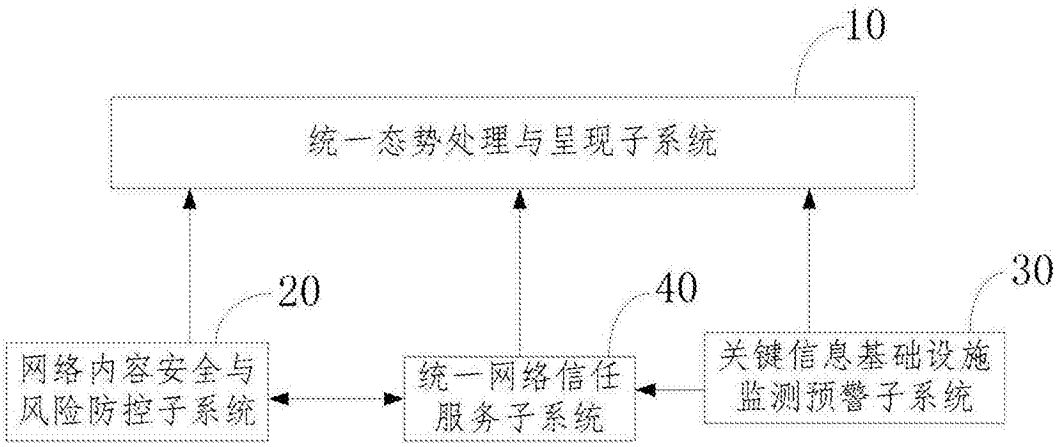

10
统一态势处理与呈现子系统
20
网络内容安全与风险防控子系统
40
统一网络信任服务子系统
30
关键信息基础设施监测预警子系统

图1

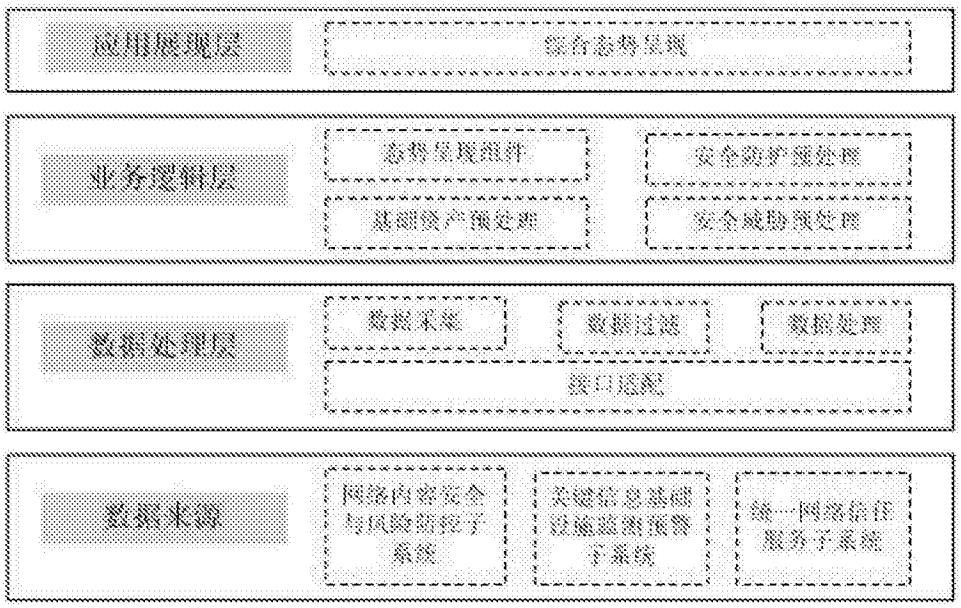

应用展现层
综合态势呈现
业务逻辑层
态势呈现组件
安全防护策处理
基础资产策处理
安全威胁策处理
数据处理层
数据采集
数据过滤
数据处理
接口适配
数据来源
网络内容安全与风险防控子系统
关键信息基础设施监测预警子系统
统一网络信任服务子系统

图2

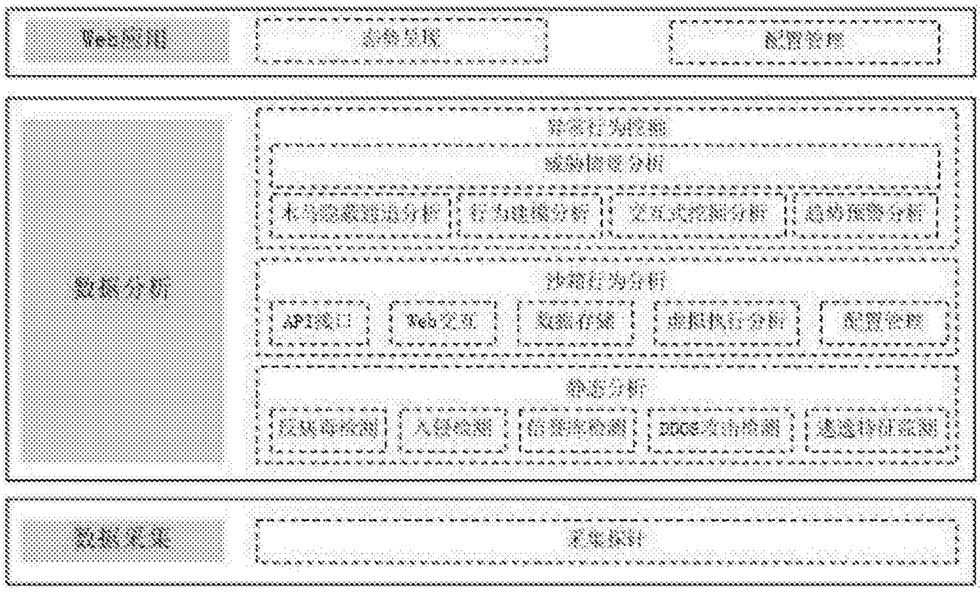

Web应用
态势呈现
配置管理
异常行为挖掘
威胁情报分析
木马隐蔽通道分析
行为建模分析
交互式挖掘分析
趋势预警分析
数据分析
沙箱行为分析
API接口
Web交互
数据存储
虚拟执行分析
配置管理
静态分析
反病毒检测
入侵检测
信誉库检测
逃逸特征检测
数据采集
采集探针

图3

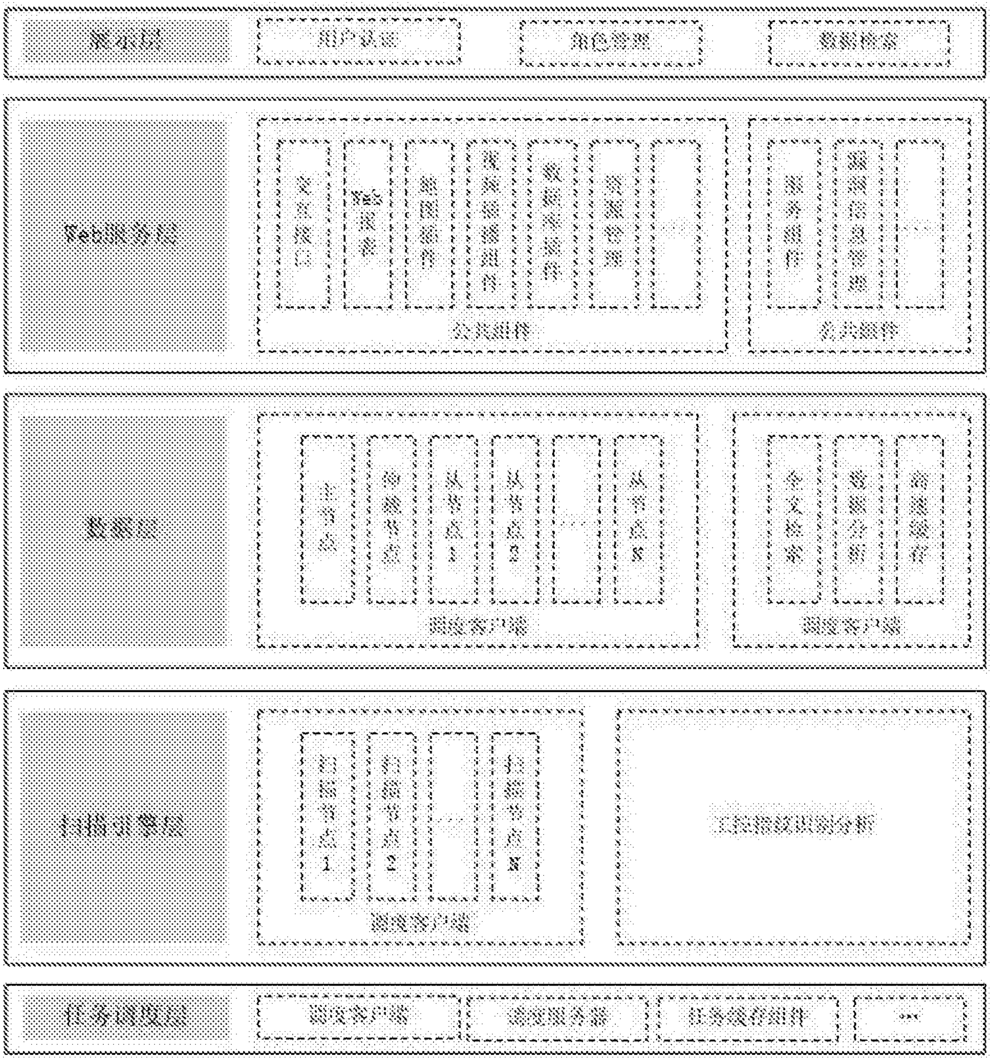

展示层
用户认证
角色管理
数据检索
Web服务层
公共组件
数据层
主节点
从节点1
从节点2
从节点N
全文检索
数据分析
高速缓存
调度客户端
调度客户端
扫描引擎层
扫描节点1
扫描节点2
扫描节点N
调度客户端
任务调度层
调度客户端
调度服务器
任务缓存组件
...

图4

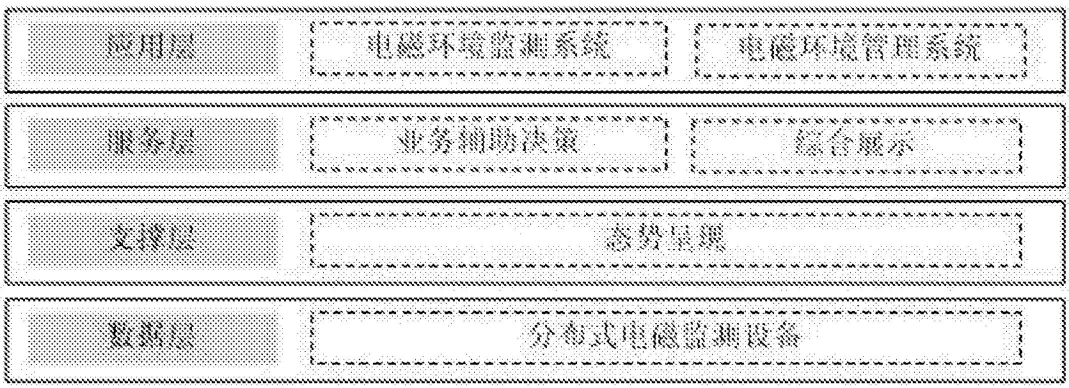

应用层
电磁环境监测系统
电磁环境管理系统
服务层
业务辅助决策
综合展示
支撑层
态势呈现
数据层
分布式电磁监测设备

图5

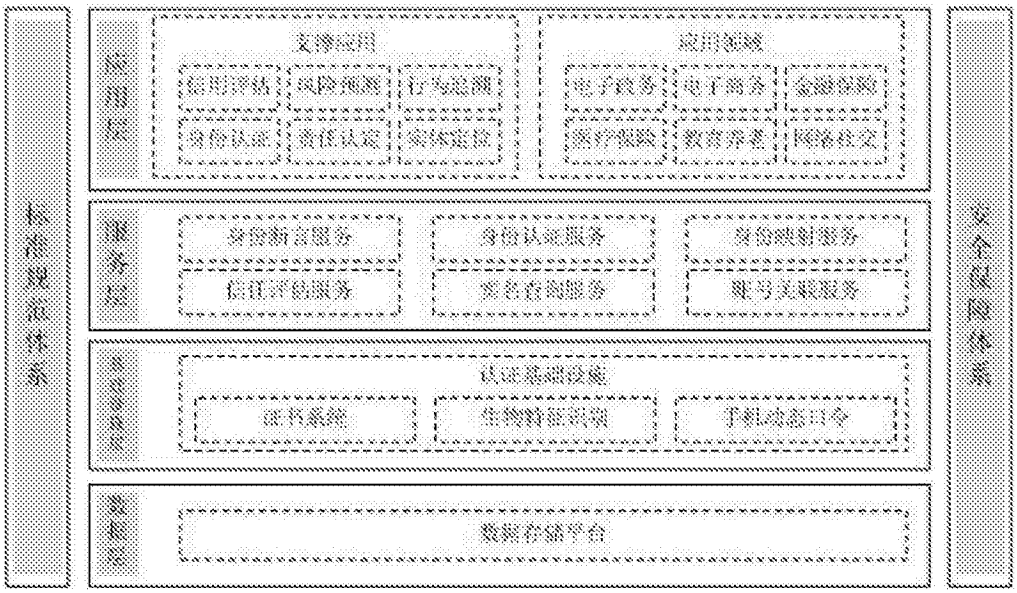

标准规范体系
支撑应用
应用评估
风险预测
行为监测
身份认证
责任认定
实体定位
应用领域
电子政务
电子商务
金融保险
医疗保险
教育养老
网络社交
服务层
身份断言服务
身份认证服务
身份映射服务
信任评估服务
实名查询服务
账号关联服务
认证基础设施
证书系统
生物特征识别
手机动态口令
数据存储平台
安全保障体系

图6