FORM 2

THE PATENTS ACT, 1970

(39 of 1970)

&

THE PATENTS RULES, 2003

COMPLETE SPECIFICATION

(See sections 10; rule 13)

TITLE OF THE INVENTION

SYSTEMS AND METHODS FOR DETECTION OF ANOMALIES IN CIVIL INFRASTRUCTURE USING CONTEXT AWARE SEMANTIC COMPUTER VISION TECHNIQUES

APPLICANT

NAME: DR. MANIK DESHMUKH, MRS. R. SELVAPRIYA, DR. D. JAYASUTHA, P. RAJ KUMAR, MANNE BHARADWAJ, ARYA SHAH, DR VINOTHINI V R, VENKATA SURYA PRABHATH.JAMILI, GATLA ANITHA, DR. DESHMUKH DILIP PANDURANG, MR. L. KARTHICK, DR. UJJAL ALOKE SARKAR

NATIONALITY: INDIAN

SYSTEMS AND METHODS FOR DETECTION OF ANOMALIES IN CIVIL INFRASTRUCTURE USING CONTEXT AWARE SEMANTIC COMPUTER VISION TECHNIQUES

BACKGROUND

Technical Field

[0001] The embodiments herein generally relate to a systems and methods for detection of anomalies in civil infrastructure using context aware semantic computer vision techniques.

Description of the Related Art

[0002] A method where the computer network administrators have placed a high importance on activity detection, both benign and malicious. Users of well-known public and private computer networks utilize gadgets like desktop computers, laptop computers, tablets, smart phones, browsers, etc. to communicate with one another through connected computers and servers. Anomaly detection is a broad objective that can be used to accomplish a variety of tasks, such as preventing actions taken by unintended threats or malevolent insiders and, more generally, managing operational and human risk. It is necessary to statistically convert the annual consumer use into monthly, weekly, or daily consumer profiles or to extrapolate individual random samples in order to simulate drinking water distribution networks and energy networks. These anomalies could be flaws like structural flaws brought on by wear and tear and severe use (such steel corrosion, cracks, concrete efflorescence, and concrete spalling), which could be brought on by or made worse by abnormalities in design or manufacture. Based on one or more pieces of contextual data related to the peer that are included in the CAID, the local peer may try to connect with the peer.

[0003] The system unauthorized access to and subsequent unauthorized use of network resources and data are examples of malicious actions. Network administrators look for patterns of behavior that are abnormal or otherwise deviate from the expected use pattern of a specific entity, such as an organization or subset thereof, an individual user, an IP address, a node or group of nodes in the network, etc. in order to identify such activities. Due to the static nature of the rules used to set them, one of their key drawbacks is that they cannot be utilized to cover the vast array of potentially harmful behaviors and acts that can occur in a large organization. The improvement strategies may be structural, legal, or financial in nature and geared towards overall goals such, for example, resource conservation or environmental protection. The ability to gather substantial amounts of visual data, including pictures, videos, and three-dimensional (3D) imaging, about civil infrastructure that can be used to assess the state of such systems has been made possible by advancements in the fields of remote sensing, robotics, and image capturing technologies. The method may also involve figuring out a first section of the CAID to identify the first piece of contextual data connected to the peer.

[0004] The method with the well-known systems, security appliances are utilized to offer network security. The appliance technique is placing security appliances—typically servers or computers outfitted with security measures—at one or more points throughout the network. After being set up, the device keeps track on network traffic. Since recent studies of espionage and IT sabotage cases have shown that nearly half of malicious insiders displayed some inappropriate, unusual, or concerning behavior prior to the incident but had no recorded incidents of violating organizational policies, it is a significant limitation in their detection capabilities. Since there aren't any extensive and continuous measurement data accessible for all domains of activity via sensors, video cameras, or similar devices, carrying out such data acquisition extensively over a whole city and over periods of several years, for example, might be highly expensive or even impractical. Since they do not take into account information in the context of the structure the way a human observer in the field naturally does, these images are fundamentally decontextualized. When a local service is found to be connected to CA Cat, a second portion of the CAID is decrypted based on the decision to keep processing the CAID and the peer's context data.

SUMMARY

[0005] In view of the foregoing, an embodiment herein provides a systems and methods for detection of anomalies in civil infrastructure using context aware semantic computer vision techniques. The appliance may perform a variety of tasks, such as detecting viruses, intrusions, unauthorized access, and unauthorized use of data. Unfortunately, scaling security appliances to address transient or long-term increases in network traffic is difficult. An increase in network traffic frequently necessitates an equipment switch or an equally time-consuming appliance upgrade from a security vendor. This disclosure is data-driven rather than solely rule-driven, allowing it to automatically adjust to changes in the environment or in the analyzed data, including when human behavior is changing. The installations are linked to a variety of infrastructures, and boundary conditions for models of various civil infrastructures are produced using the typification of the spatially distributed installations that have been mapped. The procedure includes applying an anomaly identification model to features taken from visual multimedia content showing at least a portion of civil infrastructure in order to identify at least one anomalous portion shown in the content, as well as the type and quantity of each anomalous portion. The radio transmit/receive unit (WTRU) may serve as an illustration of a peer device that is set up to contextually associate with one or more nearby WTRUs.

[0006] Another method of securing data networks is using installed software solutions as opposed to security hardware appliances. Anti-virus or anti-malware software is one of these items that is often installed on terminal devices. The installed products keep track of data travelling across the network between the terminal device to look for malware in either inbound or outbound data. Every risk-generating activity is accompanied by at least some change in behavior. Even malicious insiders who go to great lengths to evade detection mechanisms will leave some electronic footprint that will result in a departure from baseline behavior—whether from their own established baseline or that of their peer group—even when no rule has been broken and when the malicious activities in question do not fit any scenario known a priori. The spatially dispersed installations may be a structure, a piece of property, or a site for infrastructure. The machine learning model used to identify anomalies is chosen from a range of anomaly identification models based on the type of material used in at least some of the civil infrastructure. The integrated peer association mechanism sets up peer discovery parameters like channel sequences and scanning intervals, as well as peer access settings like duty-cycle schedules and channel switching. It can be applied to a variety of things, like.

[0007] The process of identifying anomalies with substantially similar profiles across time, the profiles being based on the underlying event data related to each anomaly. A novel blend of proactive and reactive anomaly detection mechanisms—this combination generates a consistent and easily understood stream of manageable notifications. A realistic deployment of an anomaly detection system such as the one described here would not be possible without the ability to limit the number of warnings and monitor their quality. A typification method for characterizing the geographically dispersed installations; and a determination method for figuring out the boundary conditions for at least one model using the stereotyped spatial distribution of installations. Each of the at least one anomalous portion's patterns are defined by the plurality of anomalous points. The WTRU may be set up to connect to a peer that corresponds to the CAID by utilizing orthogonal association messages that are sent nearly simultaneously with a number of other peers.

[0008] These and other aspects of the embodiments herein will be better appreciated and understood when considered in conjunction with the following description and the accompanying drawings. It should be understood, however, that the following descriptions, while indicating preferred embodiments and numerous specific details thereof, are given by way of illustration and not of limitation. Many changes and modifications may be made within the scope of the embodiments herein without departing from the spirit thereof, and the embodiments herein include all such modifications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The embodiments herein will be better understood from the following detailed description with reference to the drawings, in which:

[0010] FIG. 1 illustrates a method of a systems and methods for detection of anomalies in civil infrastructure using context aware semantic computer vision techniques according to certain embodiments herein; and

[0011] FIG. 2 illustrates a high-level view of an example of the processing within the security platform according to certain embodiments herein.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0012] The embodiments herein and the various features and advantageous details thereof are explained more fully with reference to the non-limiting embodiments that are illustrated in the accompanying drawings and detailed in the following description. Descriptions of well-known components and processing techniques are omitted so as to not unnecessarily obscure the embodiments herein. The examples used herein are intended merely to facilitate an understanding of ways in which the embodiments herein may be practiced and to further enable those of skill in the art to practice the embodiments herein. Accordingly, the examples should not be construed as limiting the scope of the embodiments herein.

[0013] FIG. 1 illustrates a method of a systems and methods for detection of anomalies in civil infrastructure using context aware semantic computer vision techniques according to certain embodiments herein. Indicative of the performance or operation of a computing system in an information technology environment, the data generated by such data sources can include, for instance, server log files, activity log files, configuration files, messages, network packet data, performance measurements, sensor measurements, etc. The animated actor graph visualizations, the social universe visualization, the stressful topics visualization, the temperature gauges visualization, the buck passing visualization, the pecking order visualization, and the love life visualization are just a few examples of the continuous visualizations that are available. The different boundary condition profiles and input data for each building type can be derived using defined models automatically and without requiring human participation. Preprocessing may be done on the visual multimedia content. Preprocessing may involve deleting visual multimedia information that is loud, distorted, zoomed out, fuzzy, or otherwise likely to lower the accuracy of anomaly recognition, but it is not limited to doing so. A locally distinctive identifier for identifying the connection ties established between peers may be referred to as the association identifier (ID). The peer association update technique also allows for updating the association ID, which may be assigned during peer association or peer reassociation. One or more modules that enable wireless communication between a user device and a wireless communication system, as well as between a user device and another user device, may be included in the wireless communication unit.

[0014] The system attackers can nearly always find a way to avoid classic security systems like rules-driven malware detection, malicious file signature comparison, and sandboxing since the patterns of these malicious activities fluctuate dynamically. Additionally, as the volume of data grows, utilizing human analysis to detect threats becomes more costly and time-consuming, and such human analysis prevents the threat from being addressed in a timely and efficient manner. Another kind of scope policy can remove data in accordance with a set of predicates. When resources are few, for instance, a predicate that says all emails from a particular group of actors should be the first to be deleted, or one that is based on a directive from a system user who is duly authorized ordering the deletion of specific sensitive material. The various boundary conditions for various civil facilities can be obtained from these occupancy profiles. For instance, a residential building's water usage will increase throughout the mornings and evenings. To identify the type of material exhibited in the visual multimedia content, the material identification machine learning model is used to the visual multimedia content. There might. Virtual readers and other group members may exchange applications and context-based services. Within a group, virtual readers may be dynamically selected and updated. The controller may allow the mobile communication module 111 access to a provider server or content server where it can download different rules for the context awareness service.

[0015] The security platform described here can explicitly do user behavioral analytics (UBA) or, more generally, user/entity behavioral analytics (UEBA) to find security-related abnormalities and dangers, whether they have been known about before or not. The security platform can also help network security administrators or analysts respond quickly to a discovered anomaly or threat by presenting analytical results rated with risk ratings and accompanying data. The remainder of this section describes several pruning techniques that can be used with the actor and communication graphs, the index, and item connections. The section on Collection management explains potential pruning techniques. Then, using statistical total values such as the population of the town or district, the demographic makeup, the number of vehicles, as well as a breakdown by type of vehicle, the total energy consumption, the total water consumption, etc., the individual profiles and input data must be itemized in absolute values of appropriate units. Deep Convolutional Neural Networks (CNNs), which are intended to capture fine-grained details, are used to extract a pattern of the discovered abnormalities from the visual multimedia information based on multi-class semantic segmentation. A peer designated to increase coverage using a multi-hop technique based on a physical or logical topology may be the sub-virtual reader. The sub-virtual reader may be set up to manage smaller groups of peers who use the same context-based services and/or applications and act as a virtual reader. Under the direction of the control unit, the wireless LAN module may transmit a result of action execution to at least one target user device.

[0016] FIG. 2 illustrates a high-level view of an example of the processing within the security platform according to certain embodiments herein. A personal computer, a smart phone, a computer server, a notebook computer, or any other type of computing system or device that enables a user to access the data in the environment can be considered among the computing devices displayed in the environment. Each of the aforementioned computer systems may contain one or more separate physical computers and other processing units.

When there are several units, they may be linked to one another over one or more wired and/or wireless networks. More generally, one of the key advantages of the system is that it is not necessary to exhaustively store all of the data that has been analyzed because, in most cases, the statistical patterns that emerge from that data analysis are sufficient to create a behavioral baseline and, consequently, to identify anomalies. For whatever time period needed, the data can be produced often. The extracted pattern may be rendered onto the visual multimedia material, a three-dimensional virtual model of the infrastructure, or both in a visually distinct manner. The TCP/IP Internet Protocol Suite, which includes the protocols Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Protocol (IP), is used by the interconnected computer network and device known as the Internet. may consist of the world system. In response to a user input, the user input unit creates input data for managing the operation of a user device. A keypad, a dome switch, a touch pad, a jog wheel, a jog switch, a sensor, an illuminance sensor, an acceleration sensor, a gyro sensor, etc. are all included in the user input unit.

[0017] The method where the security platform can be installed in a network environment at any number of different places. In the case of a private network, at least a portion of the security platform can be put into place at a key location such as a router or gateway connected to an administrator's computer console that can watch over and/or manage the network traffic within the private intranet. The system may, at its discretion, automatically prune the collection instances. This is accomplished by applying a pruning mode to any specific collection instance, and the scoping policies component enforces this mode. Across all forms of infrastructure, the data for the model remains consistent. The anomaly identification is context-aware, at least in the following two ways: the types of anomalies identified are context-sensitive with regard to the type of material of the civil infrastructure being analyzed; and the location, size, and pattern of the anomalies are reflected in context within the actual civil infrastructure. Transmitter/receiver, which is able to be coupled to transmit/receive element, may be connected to processor. It should be understood that the CPU and the transmitter/receiver may be combined together in an electronic package or chip, despite the fact that the figure shows them as separate components. In particular, the display unit may show several UIs and GUIs connected to the functioning of the context awareness service.

[0018] Machine learning and data science approaches are used to process the incoming data in order to extract knowledge from massive amounts of structured or unstructured data. Data mining and predictive analytics, also known as knowledge discovery and data mining (KDD), are broadened and continued in a broader sense by data science. The event passing infrastructure, which in the default embodiment of the current disclosure transmits data gathered by the data collection component from any other source of raw electronic events, is the provider of raw events that the continuous clustering component connects to. Dynamically assessing and modifying the interdependencies between the various infrastructure types is possible. The three-dimensional virtual models could be changed versions of models already established by the anomaly identifier, such as visually distinguishable projections of anomaly patterns on infrastructure, three-dimensional virtual models that the anomaly identifier will modify, or both. The transmit/receive element transmit/receive element may be designed to modulate the signal that will be transmitted by it and demodulate the signal that will be received by it. The WTRU may have multi-mode functionality, as was previously mentioned. The touch sensor has the ability to recognise user-generated touch events, produce a signal in accordance with those events, and send that signal to the control unit.

CLAIMS

I/We Claim:

1. A method for systems and methods for detection of anomalies in civil infrastructure using context aware semantic computer vision techniques, wherein the method comprises:

by processing the anomaly data using a variety of machine-learning threat indicator models, each of which is designed to examine relationships between anomalies detected across the computer network, the computer system can identify threat indicators;

creating in near-real time, predictive models of at least one of individual and group behavior for behavior and information analysis;

data structure mapping of spatially dispersed installations related to at least one civil infrastructure;

extracting from the visual multimedia content at least one pattern of the at least one anomalous portion, where each extracted pattern is collectively defined by a portion of a plurality of anomalous points;

receiving a discovery message from a peer device that has a frequency symbol displayed in front of it; the message contains group information, the peer device, and second context information; and

providing a user-selectable visual element for adding a rule to be displayed on a touch screen of an electronic device on the screen of an operating context-aware service application.

Dated 20th day of July 2023

Signature

ABSTRACT

SYSTEMS AND METHODS FOR DETECTION OF ANOMALIES IN CIVIL INFRASTRUCTURE USING CONTEXT AWARE SEMANTIC COMPUTER VISION TECHNIQUES

A method of treating together with single dose applicators, devices for delivering the drug formulations to the oral mucosa, and methods for using them

To identify security-related anomalies and risks in a computer network environment, a security platform uses a range of methodologies and procedures. The security platform uses machine learning and "big data" to do security analytics. A method entails gathering data, processing and categorizing a variety of events, continuously clustering the variety of events, continuously building a model for behavior and information analysis, analyzing behavior and information using a holistic model, detecting anomalies in the data, displaying an animated and interactive behavioral model visualization, and displaying an animated and interactive visualization of the detected anomalies. In order to identify at least one anomalous portion shown in the visual multimedia content showing civil infrastructure, as well as the type and quantification of each anomalous portion, a method is applied to features extracted from the visual content showing civil infrastructure. The current invention transforms the user's context information to the user or specified rule and performs context aware of the user in accordance with a rule defined by the user in a user device.

FIG.1