(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2011 (06.01.2011)

PCT

(10) International Publication Number
WO 2011/001250 A1

(51) International Patent Classification:
G06Q 99/00 (2006.01)

(21) International Application Number:
PCT/IB2010/001578

(22) International Filing Date:
29 June 2010 (29.06.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1358/DEL/2009 1 July 2009 (01.07.2009) IN

(71) Applicant *(for all designated States except US)*: **HONEYWELL INTERNATIONAL INC** [US/US]; 101 Columbia Road, P.O. Box-2245, Morristown, NJ 07962-9806 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SAKET, Dwivedi** [IN/IN]; 25/26, Janta Quarters, Bangalore, Karnataka 560076 (IN). **HARSHA, Angeri** [IN/IN]; 402, Building 9, Shanti Apartments, Jayanagar 9th Block, Bangalore 560069 (IN). **CHANDANA, Kiran** [IN/IN]; 679, 6TH C Main, Bangalore, Karnataka 560 078 (IN). **SUBRAMANIAN, Krishnan** [IN/IN]; . (IN).

(74) Agent: **SANJAY, Kumar**; Remfry & Sagar, Remfry House at Millenium Plaza, Sector 27, Gurgaon-122022, New Delhi Capital Region (IN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: SECURITY MANAGEMENT USING SOCIAL NETWORKING

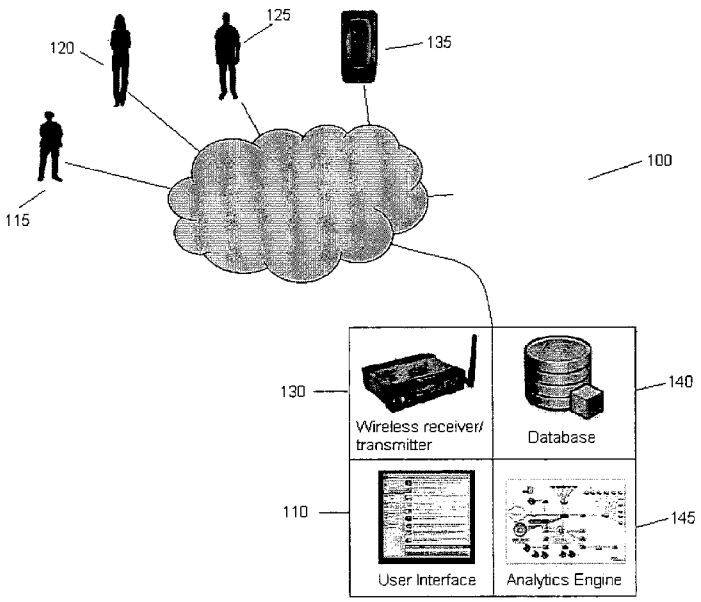


FIG. 1

(57) Abstract: A system includes a method, algorithms and apparatus to receive events being reported by various agents, analyze them, and actuate appropriate responses. Events which have the potential to adversely impact an organization's security situation impact several stakeholders. Many of these stakeholders, called agents, observe such events and hence possess the potential to prevent the adverse impact of such events; by reporting the observed events to a central decision making suite which includes a database, an analytics engine, and an actuation engine. The system includes a data receiver to receive communications regarding perceived security violations from the agents, thereby enabling the agents to report the observed events.

WO 2011/001250 A1

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

Security Management Using Social Networking

Background

[0001] Security breaches are among the most critical problems that entities such as software companies, manufacturers with physical/ intellectual assets, and in general all organizations face. Difficulties in security management could be attributed to multiple reasons such as lack of knowledge about security policies on part of actors [e.g., employees, contractors of an organization] who are supposed to adhere to such policies or inadvertent carelessness on their behalf. The said actors often circumvent security policies for the sake of convenience, viewing such violations as innocuous, and inadvertently generate loopholes in the overall security mechanism. For instance, an employee opens an access controlled door using his own access credential, for a stranger who poses to be another employee who forgot to carry his credential. Once the stranger has obtained physical access to the organization's premises, he is in a position to perform unauthorized actions. Such loopholes often lead to huge amounts of losses to organizations due to theft of information, physical devices such as laptops, intellectual property, real assets, and data assets.

[0002] Organizations deploy a variety of physical security systems [access control systems, video surveillance complemented by physical security guards] as well as network security systems but such systems do not prevent security breaches (leading to deterioration of organizational value) from taking place. For e.g., the most sophisticated firewall is of little use if an intruder can gain physical access inside the premises of an organization and find an unlocked computer to work on. The frequency of security incidents has therefore not decreased. One reason security systems fail is that systems and policies are designed to work together. If people don't comply with policies; even the best of systems are rendered less effective. For example,

doors with access control can only work if "no tailgating or anti-pass back" policies are implemented perfectly. However, tailgating is a very common practice. Again, in countries with empathetic cultures, it is common for people to use their cards to allow people who don't have access cards to allow passing through. Often, employees who forget to carry their access cards on a particular day keep the access controlled doors open to prevent discomfort to themselves during the day.

[0003] Organizations apply several policies but these policies are abused and ignored regularly. For example, there exist policies on password confidentiality, but passwords continue to be shared and dealt with casually. Whereas such policy abuses are addressable by better technological solutions, technology has certain limitations and it is not feasible to deploy technological solutions for every possible use case. For example, many organizations claim that use of turnstiles is a perfect solution to prevent tailgating [the practice of following someone through an open door without presenting an access credential oneself]. But turnstiles are an expensive solution, occupy precious space and they decrease company productivity by decreasing employee throughput as well. Apart from up front capital expenditure, they also necessitate recurring maintenance expenditure. Whereas more sophisticated mechanisms can be used to address several breach scenarios, they do not come without some caveats attached to them.

[0004] Security, however, is a social problem. Whereas security investments being made by organizations have increased in recent years, most organizations are averse to investing heavily on technology to prevent security breaches – nevertheless, security remains a major concern and focus on security has heightened during recent years. There is still significant likelihood of security breaches taking place. Such breaches have the potential to cause significant adverse impact to the organization.

[0005] Many security administrators mentioned that it is the inputs from observant/ informants that enable them to investigate certain events. An

online survey of several employees at various organizations was performed during Jan - May 2008 and it was realized that people do observe policy violations – and most of the common policy breaches are observed by them. Not only that, security awareness has heightened in recent years and people are also willing to report violations they observe – even without being incentivized for that. This provides the motivation for the proposed concept.

Brief Description of the Drawings

[0006] FIG. 1 is a simplified block diagram of a system to implement security management using social networking according to an example embodiment.

[0007] FIG. 2 is a workflow diagram of the system of FIG. 1.8 according to an example embodiment.

[0008] FIG. 3 is a screenshot illustrating communications in a social group according to an example embodiment.

[0009] FIG. 4 is a flowchart illustrating process flow according to an example embodiment.

[0010] FIG. 5 is a high level architecture diagram of a system according to an example embodiment.

[0011] FIG. 6 is table illustrating an example report.

[0012] FIG. 7 is a detailed block diagram of a security management system using social networking according to an example embodiment.

[0013] FIG. 8 is a flow diagram illustrating a method to determine who should be the right agents in a particular environment when there are deployment constraints.

[0014] FIG. 9 is a block diagram of a computer system for implementing methods and algorithms according to an example embodiment..

[0015] FIG. 10 is a diagram illustrating a typical security incident with analysis for root causes.

[0016] FIG. 11 illustrates a method to determine appropriate agents in a particular environment according to an example embodiment.

[0017] FIG. 12 illustrates yet another embodiment in a community which includes traffic management.

Detailed Description

[0018] In the following description, reference is made to the accompanying drawings that form a part hereof, and in which is shown by way of illustration specific embodiments which may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that structural, logical and electrical changes may be made without departing from the scope of the present invention. The following description of example embodiments is, therefore, not to be taken in a limited sense, and the scope of the present invention is defined by the appended claims.

[0019] The functions or algorithms described herein may be implemented in software or a combination of software and human implemented procedures in one embodiment. The software may consist of computer executable instructions stored on computer readable media such as memory or other type of storage devices. The term "computer readable media" is also used to represent any means by which the computer readable instructions may be received by the computer, such as by different forms of wired or wireless transmissions. Further, such functions correspond to modules, which are software, hardware, firmware or any combination thereof. Multiple functions may be performed in one or more modules as desired, and the embodiments described are merely examples. The software may be executed on a digital signal processor, ASIC, microprocessor, or other type of processor operating on a computer system, such as a personal computer, server or other computer system.

[0020] Social engineering is leveraged to complement technology solutions to observe and report security policy violations. A system includes a method, algorithms and apparatus to enable employees, and other stakeholders, including non human entities to report events, receive the reported events, analyze those events, corroborate those events, and actuate appropriate responses. Various embodiments of a system combine convergence of physical and information security devices with social computing to form a social network, intelligence. People in an environment to be monitored for security provide communications via many different communication mechanisms describing activity that they observe. Such people are referred to as agents. Now, these agents are to be identified keeping in mind the context of the environment in which security needs to be enhanced. For example, in a software company, the primary asset to be protected is data, and the primary mode of stealing data is USB devices. Now, the security guards who screen employees (software programmers) are generally not technology savvy, and cannot identify a USB device whose form factor is different from a usual one [e.g., USB device in the shape of a pen]. However, another programmer, who is savvy enough to realize the same may observe the misuse of the device and is in a position to report this violation. Hence, programmers are the appropriate stakeholders who can be identified as agents, along with some other stakeholders as well. In a manufacturing house, however, the primary asset to be protected are physical assets – machines, equipment, tools, and workers who spend almost their entire time dealing with those assets might be the right stakeholders to be identified as agents.

[0021] FIG. 8 illustrates a method to determine who should be the right agents in a particular environment when there are deployment constraints. In environments where there are no cost and scalability constraints, all or most stakeholders could be identified as agents. One of the advantages of the proposed system is that the cost of scaling it up is minimal; rather zero for certain thresholds, and hence it is more feasible to scale than

technological solutions. To that extent, this method is redundant in most environments. The communications received from agents may be monitored by security personnel and even security devices and appropriate actions taken as a measure of response.

[0022] The system may be deployed in varied environments like manufacturing houses, industrial plants, airports, public places, etc., which are fraught with security challenges. The system may trace and track several policy violations illustrated in a few use cases in this application. Such policy violations or events may not be detected by current systems and hence not responded to by the security administrators. For example, for some organizations, movement of unauthorized people [e.g., foreign nationals] is restricted. Technological solutions, unless very sophisticated like biometric access control systems, generally cannot restrict or identify such movements. The proposed system, however, may be utilized by several employees who may report independently that they observed an alien moving in the premises without an escort – this also serves to corroborate the events reported by one employee by providing supporting evidence in the form of more reported events. The system provides information to security administrators, who view all the content posted by the observers and users of the proposed system.

[0023] If any particular event, which an agent uploads, leads the agent to believe poses risk of significant loss to the organization, the agent may rate/tag such content as "high impact" - this would help administrators to respond faster to the threats. For instances when the security administrators may have too many events to deal with, they may be obligated to deal with the "high impact" and "very often" tagged events followed by "medium impact" and "often" events, etc. Again, in some embodiments, the system might use software analytical tools to prioritize the received events based on certain factors, such as the history of the correctness of reporting of one user with respect to that of another. In such embodiments, the system could also use a combination of system-prioritized and user-prioritized events.

Reference is cited to "Adaptive Learning for Enterprise Threat Management": USPTO Application No. 12/171231, Publication No. US 2010-0010776 A1 which discusses this subject matter in detail and is incorporated herewith in its entirety by reference.

[0024] In all embodiments, the system utilizes the fact that whereas security systems are limited in their ability to detect events which could lead to incidents of loss of physical assets or data to the organization, most of the time there are people around who observe events. The system seeks to leverage the observers to report the events through an easy to use interactive tool, which also serves to report back the response to such events by the administrators. The system may enable virtual collaboration by creating a network or communities of users in a forum via a cost effective portal. In some embodiments, the portal comprises a rich, user-friendly interface based on a rich media (hosted either on the internet or mobile or any hand held devices or any other devices) which allows easy user access and management of the data for detecting of an incident or condition reported by a single observer or multiple observers and an alerting mechanism to provide early notification via the portal. The reporting could be executed in multiple forms like uploading content having one or more of data, text, photo, video, and audio of the incidents of security violation using mobile or like devices.

[0025] The content may be transmitted via internet enabled technologies using mobile phones, hand held devices, over telephone wires, WiFi networks, Bluetooth, or any similar communications mechanisms. The system may utilize social computing methodologies, e.g., networking of people, resources, creating communities, user groups and forum for participants to generate information and transfer or partially transfer the responsibility of security management to other stakeholders. The same may translate to user generated policies and collective intelligence for the context.

[0026] Once a security breach has been reported, appropriate parties [security administrators] can connect and monitor the situation. If the

appropriateness of the notification has been established, the system may also publish the action and the response time along with more parameters. The validated notice or report may be collected to form intelligence. The intelligence may be edited, or modified to context and then published to create user generated intelligence. The system may create a chain of influence among the network of resources to form collective intelligence which can be termed a user generated policy for resources to comply with the policies they have generated adhering to the pre – determined policies.

[0027] A dynamic trust rating can be initially assigned to each person in an organization, based on designation, information flow control etiquette, etc. For example, a senior executive with a clean background and a good track record of not sharing sensitive documents or violating any security policy could be assigned a high trust rating of nine out of ten. On the other hand, a middle level executive with a track record of printing and losing several documents, and/or carrying USB drives in the company premises might be assigned a low trust rating of three out of ten. This trust rating of users [agents] changes as per their actions, their position, and their roles in the organization--this rating is stored in the Database, in the messaging backbone of the architecture of the system. In some embodiments, the dynamic trust rating of individuals is used, and it changes based on their behavior. As individuals report events regarding policy violations that they observe, the administrators respond to those events appropriately, depending on nature and severity. Once the administrators are done with their responses, they close the loop by acknowledging the reported event – this acknowledgement is used to alter the dynamic trust rating of the reporting individual. For every event an individual reports which is found to be true, his DTR increases and vice versa. Using this, in due course of time, the tool could also prioritize the incidents being reported by individuals – an incident reported by an individual with a higher trust rating may be given priority over an incident reported by an individual with a lower priority.

[0028] FIG. 1 is a simplified block diagram of a system 100 (referred to as "the system" here onwards) to implement security management using social networking. In one embodiment, a user interface 110 may be provided to facilitate generation of communications relating to perceived security violations. A wireless receiver/transmitter or hardwired network adapter 130 receives communications regarding perceived security violations from a group of users [agents] indicated at 115, 120 and 125, and also from stand alone edge devices such as 135. Many more users may be coupled to a network 135, such as an internal network of a company or other entity, or a public network, like the Internet. The received communications may be stored, such as in a database 140 coupled to the network adapter 130. In one embodiment, an analytics engine 145 is coupled to the database, and may be programmed to consolidate received communications, analyze them to provide insights and provide reports to security personnel regarding security violations.

[0029] In various embodiments, the users may be using hand held wireless devices, such as cellular phones, laptop computers, and other devices, or may be wired workstations or kiosks, or any other form of device that can provide a communication regarding a security violation. In one embodiment, electronic switches may be placed near controlled access doors, and simply pushed to report a violation, such as a person entering the door after an authorized user without entering a code or using a badge. This is referred to as tailgating. In other embodiments, tailgating may be reported by sending a text message or email with information about the event, including a picture if taken. Thus, the communications reporting perceived security violations may be content rich in various embodiments, and may even provide tags related to the frequency and/or seriousness of the violations. The user interface may provide a simple email address, or a graphical user interface with check boxes, drop down menus for entering tags, attachment capabilities and other interface constructs such as those associated with social based computing platforms. Further keys, such as

emergency keys may be provided that allow a user to anonymously report, or use an identification card or punch in an identification code to report emergencies or security violations.

[0030] Social computing platforms may be used in conjunction with security devices in one embodiment to create a mechanism which may sense, predict, and respond to most events which are observed by people within an organization. Events collected by the system might serve as sources of inputs into physical security systems such as access control systems, video analytics systems, etc. For example, events received by the data receiver may be sent to ProWatch access control system manufactured by Honeywell International, Morristown. The ProWatch access control system, in response may send instructions to lock a certain door, for example. Many such policy violations are not even detected by current physical security systems and hence not responded to.

[0031] FIG. 2 is a block flow chart illustrating an example workflow 200 in system 100. At 210, security threats [events] may be identified. Users of the system observe events around them – for example, an employee working in her cubicle may observe a stranger tail gating through the door right beside. Regarding security threats, several possible intrusion scenarios can emerge regarding how a physical security violation or, more generally, any policy violation could enable an intruder to gain unauthorized access to the company's physical/ information assets. It may or may not lead to an incident on every occasion, but does open up the possibility of the same. For example, a person may tailgate for innocuous reasons. The person may be an employee who forgot his/her access card. However, a security administrator needs to confirm this fact as an unauthorized person tailgating could create security loopholes.

[0032] Notification of security threats may be received by the system 100 at 220. The system enables virtual collaboration by creating a network / communities of users in a forum via a portal (hosted either on web or mobile/ hand held devices or any other devices which supports access to

the said network). The user interface enables the users to report a detected incident or noticed vulnerability in the security process in multiple forms - like uploading a data file / entering a text message / uploading photo / video clip / audio clip/ making a phone call to a voice analytics enabled receiver related to the detected incident or observed vulnerability. Once this data is entered into the system through the interface, it could be transmitted via IP network / cellular network / over telephone wires, cable, WiFi, or any similar communications system to the central database of the system.

[0033] Certain people may be designated as the administrators of the system. Such administrators possess administrative privileges and can view the reported incidents/ vulnerabilities through their respective user interfaces. The system may promote discussions among agents on possible security vulnerabilities and administrators may use the inputs from such discussions to frame the security policy of the company. FIG. 3 shows a user interface design in one embodiment with a few sample communications regarding some vulnerabilities displayed. A message by an agent "Chandana" address the need for enhancing the screening process of employees so that no employees bring in a USB drive or any other data storage device. Next, another agent, "Me", suggests that since most employees have laptops as well as remote connectivity to company servers, they could as well steal data from home – hence probably this policy [of not allowing USB drives at all] is redundant, and could be replaced with a policy of random checking of any employee's USB drive. Yet another agent [Aniruddh] concurs with "Me's". This might lead to a user generated policy. The interface provides a typing area, a pull down menu for selection of the recipient (currently set on Security), a list of groups the person is following, and different devices from which communications may be sent or read. Users of the systems may form groups, comprising individuals with some shared interest, to discuss specifically around that interest. In one embodiment, the system facilitates the partial transfer of the onus of

security management beyond the security personnel – to employees, contractors, trainees, workers, suppliers, et. al.

[0034] Returning to FIG. 2, validation and analysis occurs at 230. The relevant personnel – either the security personnel or any other designated personnel - can observe these incidents and investigate them. For example, in one implementation a security administrator may only sit in front of his desktop computer and view the reported violations – whenever the administrator feels the need, the administrator may assign a security guard the task of investigating a reported event. The administrator could send a text message to the security guard which the latter might receive on his mobile phone. The guard might then go, investigate the incident, and then acknowledge the response – "false alarm", or "caught the intruder". The acknowledgement message could be sent through his mobile phone. The system would wait for some time to allow the administrator to close the event, and once that threshold has passed, may record the security guard's acknowledgement – true event/ false event along with the action taken. Once the system does this, it also informs the reporting individual about the action taken by sending a message/ email. Again, the analytics engine 145 in Fig 1 queries the trust rating of the concerned individual from the database 140, and based on the security guard's acknowledgement – true event/ false event, the analytics engine 145 would compute the appropriate change to the dynamic trust rating of the individual. For example, if the reported event were true, the analytics engine 145 may increase the DTR of the individual from say 6.5 to 7.0. The analytics engine 145 possesses data analytics capability to analyze the events and categorize them based on several administrator defined parameters – such as time/ date, geographical location, reporting user, etc. Ontological dictionaries capture concepts and relationships in a specific domain from human experts which are used by machine learning algorithms to analyze behaviors and suggest recommendations based on empirical data. The responses may also be analyzed and categorized in the same manner. Such responses can be

managed / edited / modified at 250 and published to create user generated intelligence. The categorization helps in report generation. For example, an auditor may query the system – "please show me all the events related to USB drives and the responses" – for which the system can pull out all events categorized under USB drives and generate the appropriate report.

[0035] FIG. 10 shows the root cause analysis of a common use case explaining why current security systems are unable to prevent such incidents, and also how system 100 is better positioned to do so. There exist three points in the value chain, as shown in the figure, where system 100 comes into play. The probability of an agent observing the event at 1, 2 or 3 is high and system 100 enables him to report this/these observed event[s]. If an agent reports any of these events, the security administrators could swing into action and prevent the security breach.

[0036] The administrator may wish to actuate some action based on the reported incident. For example, if an agent reports a terminated employee tailgating into a room where a significant amount of sensitive information is kept, the administrator might want to lock all the computers in this area immediately and send a security guard to investigate the same. The system provides the administrator an interface to send commands to other security systems – including physical security systems as well as information systems. An example of one such physical security system is the Pro-Watch® Enterprise Edition manufactured by Honeywell international, Morristown. Interfaces may be provided to each of these recipient systems so that the commands are understood by the recipient systems and acknowledgements sent by them are understood by the system. The administrator thus sends commands to each of those information systems [computers/ printers] located within that room. The system interface provides the administrator an easy drag and drop environment to choose the information systems to which the command needs to be sent.

[0037] Once the command is sent, each of the recipient information systems may send an acknowledgement packet, which informs the system about whether

the command was executed successfully or not, or if it was executed after some delay. In case the command could not be executed, the system logs the same in a failed commands log within the database for later review. It may also send an alarm, depending on the configuration, to one or more of the alarm monitoring clients. The administrator could manually send an acknowledgement to the reporting user about the response, or the latter could also receive an auto reply, thus closing the loop at 240.

[0038] To keep the users motivated to continue to report incidents, and also to ensure the sanctity of the incidents they report, a risk/ reward mechanism may be included. The concept of trust rating may also be used, which works in a dynamic manner, based on the content the users communication. The administrator closes all incidents by reporting a logical conclusion – "True", "False" or "Others" – the last may be used if the incident could not be investigated, for some reason.

[0039] If a user reports an incident which is verified to be true by the administrator, the system increases his current trust rating. If a user reports an incident which is verified to be false by the administrator, the system decreases his current trust rating. No change to the trust rating occurs if the administrator categorizes the incident in the "Others" category. At any point of time, since there might be multiple users reporting various incidents, the system provides the administrator the option to view the reported incidents either based on time or based on priority. In case the administrator wants to view the reported incidents based on priority [this would happen whenever the number of incidents being reported in real time are too high and it is difficult to manage them], the system prioritizes the reported incidents based on the trust rating of the reporting user. The user has the choice to remain anonymous, in which case his/her identity would not be revealed to the administrator, but depending on the implementation the system may either use his trust rating to prioritize the incident reported by him or, it may not consider the trust rating for this particular user and leave this incident un prioritized.

[0040] The system provides a paradigm shift in the way organizations manage security. Current access control systems only receive events which their respective sensors collect. For example, if an employee swipes his access card at a certain door and enters the same, the access control system understands that he is present in a certain region. But if the same employee now tailgates and moves on to another room, the access control system has no knowledge of this event – it still understands the employee to be present in the previous region. The system bridges this gap partially. If another person observes this employee tailgating and entering the second room, and reports the same in the system, now the system understands the change of state. The system may serve as a supplementary source of events to current physical security systems and information systems. In some embodiments, the system thus adds an extra degree of redundancy.

[0041] At 260, a user generated policy to manage similar incidents is created. Creation of this policy involves consideration of the suggestions provided by various users [agents] as explained in Fig 3. In the foregoing example – a new policy may be created – report the presence of all ex-employees inside the campus. Whenever an ex-employee (or any employee who has resigned/has been terminated and has completed his/her notice period) is observed by an agent inside the company premises, the agent would report this event. It is possible that the ex-employee has come for some genuine reason, such as for dues settlement/ return of blackberry, etc. To that extent the reporting could be redundant – but in the context of security, redundancy is better than ignorance of such high impact events.

[0042] At 270, administrators are in charge of sending the appropriate report outs for these systems – the system provides them with the options to run reports in conjunction with other systems. The implementations could be different – for example, since ProWatch access control system manufactured by Honeywell Inc. runs reports related to access control, the access control reports could be run from ProWatch using the extra events

reported by the system. In further embodiments, the system may independently generate reports for the events handled by it.

[0043] FIG. 4 illustrates a typical process flow 400 utilizing the system 100. Receipt of communications fed from users is indicated at 410. The same user and other users may add more data on top of existing data at 420. The data is consolidated, and at 425, the consolidated data is analyzed to determine if an action should be performed in response to the communications. The action 430 may be performed, and an administrator responds based on the data, updating a response to the data at 435. A report may be generated by the system at 440. Many different reports may be generated. A report is classified at 445, and the report may be used to alter an existing state at 450. If the state is altered, an alarm may be flagged at 455, in response to which appropriate actions may be taken. The report is archived at 460 with all the data related to a chain of events corresponding to the report.

[0044] FIG. 5 is a block diagram of an example architecture 500 for implementing a security system. The system consists of a user interface 510, administrator interface 515, a data storage unit 520, a data warehouse 525, an analytics engine 530 to analyze the data stored, and an interfacing & actuating mechanism 540 with interfaces to other enterprise systems such as facility management systems, IT systems 550, etc. Facility management systems may include, for example, physical security systems 555, visitor management systems, third party applications 560, personal mobility equipment such as mobile phones or personal digital assistants, etc. The list mentioned here is representative and it would be apparent to those skilled in the art that the opportunities to integrate the tool with numerous other systems exist.

[0045] The user interface is a typical interface which permits easy entry of data, easy querying of data [for reports, for example], and viewing of data – a Web 2.0 portal is a simple example. The user interfaces may be located on a user's computer, mobile phone or any other device which could be used

to send data to the system/ view some data/ reports inside the system. The user interface may be generated by the system and sent to a user device for viewing via a web browsing application in one embodiment.

[0046] The administrator interfaces may be located on the administrator's computer, mobile phone or any other device which could be used to send, query, and modify data to/in the system, or even alter the system settings such as adding new users. The administrator interfaces need not be located distinct from the user's interfaces. For example, the administrator could access his interface from the same computer from which another user interfaces with the system, but log on with administrative rights which would enable him to perform additional functions, such as query the system for certain reports.

[0047] Once a certain user inputs some data into the system, the data analytics unit analyzes this data for any preset conditions and then classifies the data and presents it in a web browser form which other users can also view either from thin clients or even mobile phones. Other users can add some comments to this data, can respond with their own content, or perform some other actions [like rating or tagging content]. The data analytics unit can use such actions to perform more analysis based on such actions [like classifying similar rated content].

[0048] The administrator can also view content, just like other users do. But s/he has access to more details compared to normal systems. For example, certain applications may require users to mask their identities – which would not be visible when a normal user views uploaded data – but it may be visible when the administrators views the same data. Based on each uploaded content unit and other users' response to the same, the administrator may decide to take some action – for example, if the uploaded content is about a security incident and ratified by other users, the administrator may send some security personnel to investigate the event.

[0049] Once the response is performed, the administrator will "close" the current content chain by certifying – "true", "false" or "others" - which would be

archived in the data warehouse 525. The data warehouse 525 is also queried for the reports, which the administrator may require at a certain later time. The system allows for certain other services as well. The service bus contains several units which provide these services. The Integration Service unit helps integration with 3rd party applications 560 such as Enterprise Resource Planning systems.

[0050] A security services unit 570 helps in user enrollment, assigning privileges to a user, modifying or deleting user privileges or removing a user. It also takes care of authentication when a user tries to log on to the network. This would also include authenticating the administrator, for example, when he tries to log on to the network with administrative privileges. Device management services unit runs the routine functions to ping and verify the status of all other devices connected to the network. The diagnostic services unit is the heart of the system. The application specific data analytics algorithms are built in within this unit. Those well versed in the art would appreciate that the social networking platform may have several applications and collaborative security is just one indicative application. Different sets of algorithms could be built to enable different applications and accordingly, the form of the platform might be altered to accommodate the specific requirements of the application.

[0051] Event/ alert services unit provides alerts based on reported conditions or, whenever there is a change in the current state. The current state could be defined in terms of different parameters, such as time. So a condition could be defined as – "If time exceeds 8 pm, apply policy X else apply policy Y". As soon as the clocks ticks 8pm, the current state changes, and the event / alert services actuate a change in policy. A command is sent to the interfacing physical security systems/ information systems to execute the change in policy. The recipient system[s] sends an acknowledgement message for the receipt of the command. If the event/alert services unit does not receive an acknowledgement message, it records an error which is stored in the data warehouse. The reporting services unit collates are the

data from the user / administrator inputs and classifies and formats them for reporting purpose. For example, the various incidents reported by a single user could be classified together.

[0052] The following user table gives an indication of the way this information is tabulated and stored, in one possible implementation as shown in the table of FIG. 6. A user identification is provided at the top of table 600. Each row corresponds to columns that include a date, time, incident ID, administrator response and administrator comments.

[0053] FIG. 7 is a detailed block diagram of an example system 700 for implementing a security system. The top most layer depicts the kind of devices ranging from mobile phones to desktop and web based interfaces which may be used to access the applications and their data built on the platform. Some data like alerts may also be integrated with edge devices from Honeywell.

[0054] An Applications layer 720 enables various functions in the platform – the ability [for users/administrators] to search for text 722, the ability to generate and monitor alerts either through email, mobile phone message or RSS, the ability to interact with short messages 724, and the ability for agents to perform discussions within themselves and for administrators to be able to respond to the generated messages 726 e.g., the ability for an administrator to close a tailgating event reported by an employee. Third party applications 730 may be added such as to provide more analysis, workflow reporting and other functions.

[0055] An integration services layer 732 contains the following functionalities – adapters/ connectors 734 to different devices such as ProWatch or WinPak security access management control systems manufactured and marketed by Honeywell International; services 736 which enable the development of new applications 730 on top of the platform; web services for the applications to build data 738; security services 740 which govern the authentication of users/administrators and Native API 742 – which enables connecting the various databases 744. The LDAP 744, for example,

enables creation of user accounts, creation of groups, creation of roles for various users, creation and modification of policies – it keeps a record of all these parameters.

[0056] In an analytics engine layer 750, domain level ontological dictionaries 752 help in auto categorization of content – for example, four security incidents reported by different users at different points in time could be categorized as "Sunday afternoon shift events". Natural Language Processing Algorithms 754 may be written specific to the application/ intended end use of the product. For example, the collaborative security application may use prioritization of the various security incidents reported by various users, for the administrator to be able to optimize response [like sending the security guard to investigate], such algorithms may be written and would be different for different applications. There is a functionality [recommendation engine 756] to analyze the text and look out for specific keywords – for example, if a user reports – "a person without an access card followed another employee to gain entry into Jupiter building", the system could analyze this text and extract the words "without an access card" and "followed" to help tag this event as "tailgating". Users could add more tags to the same. The media indexing functionality 758 provides the implementation of the underlying search capability in the system. Machine learning algorithms also help to analyze behaviors and suggest recommendations based on empirical data. Learning models for constant learning and adaptability to new situations and behaviors.

[0057] A Distributed Computing/ Storage engine 760 governs the manner in which data is stored in the system and the way algorithms are executed and also offers a highly scalable framework for processing large set of data. A messaging backbone 770 is the back end infrastructure which enables data and message aggregation. Some of these messages need to be filtered at 772 [for example, if they contain inappropriate content]. Once the messages reach the designated inbox of an Outlook application, they are monitored. Messages may be queued and responded to and records kept for

the way the messages are handled. The backbone 770 performs all these functionalities. Data sources 780 explain the other possible ways in which data can be uploaded into the system – it could be obtained from other social networks, through files uploaded by users etc.

[0058] In one embodiment, many different case scenarios may be handled by the collaborative security approach of the system.

[0059] Scenario 1: Policy Violation. In this scenario, there are two possibilities – i] another stakeholder (maybe a cleaner, contractor, or another employee, for example) observes another employee opening the door and leaving it open _ in this case s/he may report the incident along with the name of the offender. This would result in the erring employee being warned, maybe in addition to some other form of punishment, on one side; and the person who reported the event being rewarded. Most importantly, the policy violation [the opened door] would be addressed quickly, hopefully before a potential intruder would have had the opportunity to exploit the same to his/her advantage ii] another stakeholder (maybe a cleaner, contractor, or another employee, for example) observes opened door but does not observe the erring person - in this case s/he may report the incident without with the name of the offender. This would result in the observer being rewarded.

[0060] The respective authorities may attempt to find out the erring person. Again, the policy violation [the opened door] would be addressed quickly, hopefully before a potential intruder would have had the opportunity to exploit the same to his/her advantage. In either case, the point is that the incident is reported at the earliest possible instance and a potential security loophole is addressed.

[0061] Scenario 2: Anomaly Check. In this scenario, the essential point is that, the contractor has normal permission to work on Weekdays. If s/he secures special permission to work on a weekend, a special badge may be assigning which s/he needs to wear all the time s/he is inside the campus. If s/he does not wear such a badge and is observed by another stakeholder roaming inside the campus, this could be reported duly, resulting in appropriate

rewards/ punishments. This increases the possibility of the policy violation being detected and reduces the chance of the contractor laying his/her hands on any assets _ since the possibility of someone observing him/her at the time of stealing an asset is very low in the first place.

[0062] Scenario 3: Policy Violation. In this scenario, the essential point is that, employee who works in a company where the usage of mobile phones with cameras is disallowed brings such a device to office regularly _ another employee who is probably part of the same team brings it to the notice of the authorities. This would result in the erring employee being warned, maybe in addition to some other form of punishment, on one side; and the person who reported the event being rewarded. Most importantly, the policy violation [the usage of unauthorized device] would be addressed quickly. Repeated violations can result in stern action being taken against the offender _ this can serve as a deterrent to other employees to violate policy.

[0063] Scenario 4: Duplication Check. If the company policy is such that sharing of desktop computers is not permitted, then the usage of any desktop computer is mutually exclusive _ in the absence of the designated user no one [exceptional cases like an administrative overhaul can be dealt with] is permitted to access this computer. If an intruder attempts to access this computer in such a scenario, it is quite likely to get noticed by some other stakeholder in the organization. Now, if that stakeholder reports the developments to the authorities, again whereas the appropriate reward/ punishment mechanisms are effected, the unauthorized access can be prevented.

[0064] In conclusion, reporting of policy violations and linking the same to individuals' privileges and incorporating suitable reward/ punishment mechanisms serves as a deterrent to individuals to violate policy and supplements the use of technology to detect incidents and prevent policy violations.

[0065] In the preceding discussion, organizations have been construed to be individual companies, with defined boundaries such as certain number of employees, walled within certain perimeters, etc. However, certain embodiments may involve the extension of this premise. For example, in one embodiment, an organization could comprise communities of agents, who belong to different walks of life, but come together for a shared purpose – such as residents securing the neighborhood in which they stay. FIGs. 10-11 illustrate few more embodiments of system 100. FIG. 10 illustrates an embodiment in a residential community. At 810, an informant in a residential neighborhood observes suspicious activity in another house. At 820, she logs on to the system via the web and reports the suspicious activity. The system analyzes the message, and by using natural language processing [NLP] techniques or using GPS functionality from the sender's transmitting device [such as GPS enabled mobile phone], or any related technology, determines the police station under whose jurisdiction the affected area falls – and routes the report to the concerned Station Head Officer at the identified local police station. The system also displays the nearest responder [such as police constable] on duty. At 830, the SHO receives this information, and routes the alert to the concerned responder. This could be in two forms – at 840, the responder receives this information displayed at an electronic display node which he visits frequently while on duty. Alternatively or in addition, at 850 the responder receives this information on his handheld device [such as Blackberry]. At 860, the responder goes to the affected area to check out the incident.

[0066] FIG. 12 illustrates yet another embodiment in a community which includes traffic management. At 910, an agent observes a car jumping a traffic signal/ being driven rashly. As a matter of fact, in this illustration there exists a CCTV camera with embedded video content analysis software which also detects the violation. While the camera may send this information to the data receiver via its own hard wired network, the agent may use her mobile phone to type in a text message and send the same to

the data receiver. The message received from the camera might serve to corroborate the message received by the agent. Alternatively, this embodiment illustrates that messages from agents could also be used to reduce the false alarms generated by technological solutions, by corroboration. Now, at 920 the system determines the nearest responder [such as traffic policeman] and re-routes the message to his mobile phone. At 930, the responder intercepts the offender. At 940, the feedback is complete with the agent sent a notification on the incident response. It will be apparent to those skilled in the art that the possible deployments are many – such as in airports or even at schools.

[0067] A block diagram of a computer system that executes programming for performing the above algorithm is shown in FIG. 9. A general computing device in the form of a computer 910, may include a processing unit 902, memory 904, removable storage 912, and non-removable storage 914. Memory 904 may include volatile memory 906 and non-volatile memory 908. Computer 910 may include – or have access to a computing environment that includes – a variety of computer-readable media, such as volatile memory 906 and non-volatile memory 908, removable storage 912 and non-removable storage 914. Computer storage includes random access memory (RAM), read only memory (ROM), erasable programmable read-only memory (EPROM) & electrically erasable programmable read-only memory (EEPROM), flash memory or other memory technologies, compact disc read-only memory (CD ROM), Digital Versatile Disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium capable of storing computer-readable instructions. Computer 910 may include or have access to a computing environment that includes input 916, output 918, and a communication connection 920. The computer may

operate in a networked environment using a communication connection to connect to one or more remote computers. The remote computer may include a personal computer (PC), server, router, network PC, a peer device or other common network node, or the like. The communication connection may include a Local Area Network (LAN), a Wide Area Network (WAN) or other networks.

[0068] Computer-readable instructions stored on a computer-readable medium are executable by the processing unit 902 of the computer 910. A hard drive, CD-ROM, and RAM are some examples of articles including a computer-readable medium.

[0069] The Abstract is provided to comply with 37 C.F.R. §1.72(b) is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims.

CLAIMS:

1. A system comprising:

a data receiver to receive communications regarding perceived security violations from a group of users;

a data base to store the received communications;

an analytics engine to consolidate received communications and provide reports to security personnel regarding security violations.

2. The system of claim 1 wherein the communications comprise a tag corresponding to user perceived severity of the perceived security violations.

3. The system of claim 1 wherein the communications comprise a tag corresponding to the user perceived frequency of the perceived security violations.

4. The system of claim 1 wherein the communications comprise multimedia content.

5. The system of claim 4 wherein the multimedia content comprises at least one of text, audio and video content.

6. The system of claim 1 wherein the communications are received via a network.

7. The system of claim 1 wherein the analytics engine generates a trust rating as a function of communications received.

8. The system of claim 7 wherein the trust rating is derived for the user providing a communication.

9. The system of claim 8 wherein communications are ranked by the trust ratings of the user providing the communications.

10. The system of claim 1 and further comprising a user interface generator to provide a social computing platform for authoring the communications.

11. A computer implemented method comprising:

providing a user interface to facilitate generation of communications relating to perceived security violations;

receiving the communications regarding perceived security violations from a group of users;

storing the received communications in a database;

consolidating received communications; and

providing reports to security personnel regarding security violations.

12. The method of claim 11 and further comprising alerting security personnel to a communication describing a security violation for which action should be immediately taken.

13. The method of claim 11 wherein the communications comprise a tag corresponding to user perceived severity of the perceived security violations.

14. The method of claim 11 wherein the communications comprise a tag corresponding to the user perceived frequency of the perceived security violations.

15. The method of claim 11 wherein the communications comprise multimedia content.

16. The method of claim 15 wherein the multimedia content comprises at least one of text, audio and video content.

17. The method of claim 11 and further comprising generating a trust rating for a user as a function of communications received from the user.

18. The method of claim 17 and further comprising ranking communications as a function of the trust ratings of the users providing the communications.

19. A computer readable storage device having instructions stored thereon for causing a computing platform to execute a method, the method comprising:

providing a user interface to facilitate generation of social based communications relating to perceived security violations;

receiving the communications regarding perceived security violations from a group of users;

storing the received communications in a database;

consolidating received communications; and

providing reports to security personnel regarding security violations.

20. The computer readable storage device of claim 19 wherein the method further comprises:

receiving a tag corresponding to user perceived severity of the perceived security violations;

receiving a tag corresponding to the user perceived frequency of the perceived security violations;

generating a trust rating for a user as a function of communications received from the user; and

ranking communications as a function of the trust ratings of the users providing the communications.

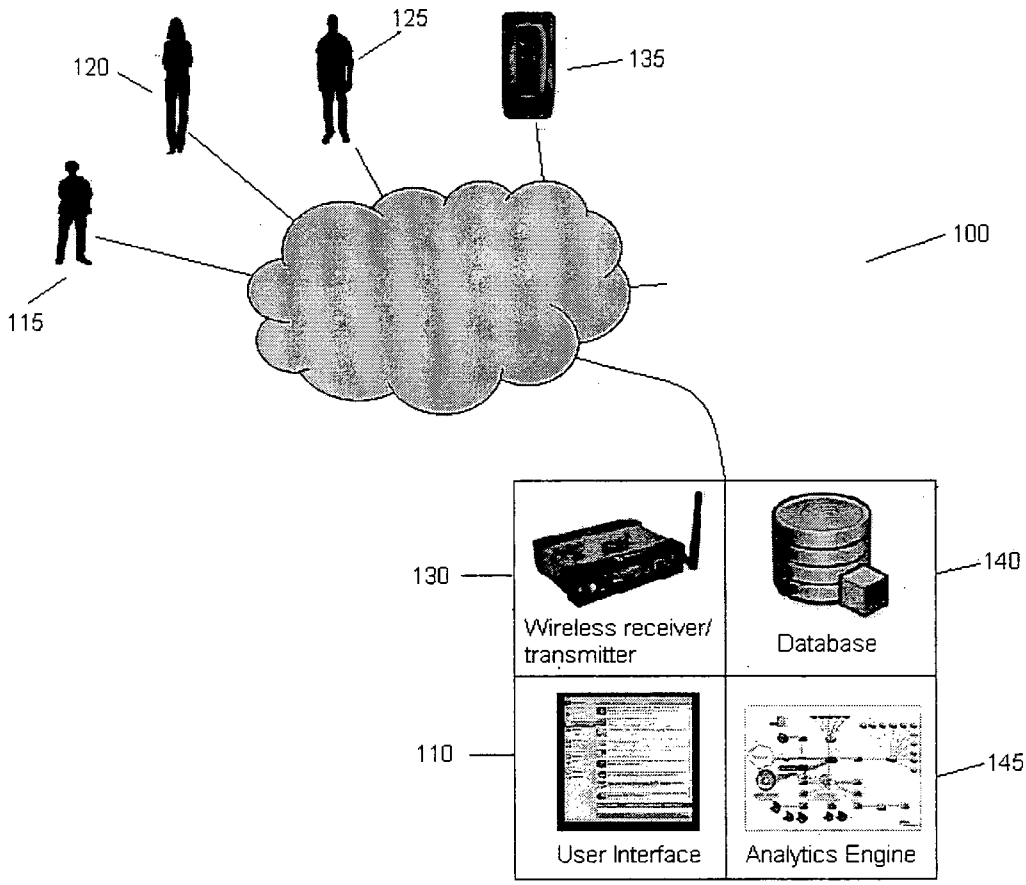

125
120
135
100
115
130
Wireless receiver/ transmitter
Database
140
110
User Interface
Analytics Engine
145

FIG. 1

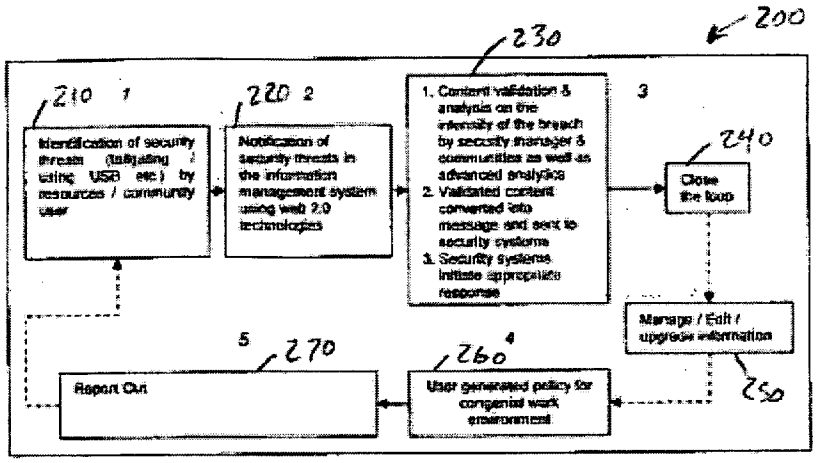

200
230
210 1
220 2
3
240
1. Content validation & analytics on the intensity of the breach by security manager & communities as well as advanced analytics
2. Validated content converted into message and sent to security systems
3. Security systems initiate appropriate response
Identification of security threats (mitigating / using USB etc.) by resources / community user
Notification of security threats in the information management system using web 2.0 technologies
Close the loop
Manage / Edit / upgrade information
250
5
270
260
4
Report Out
User generated policy for congenial work environment

FIG. 2

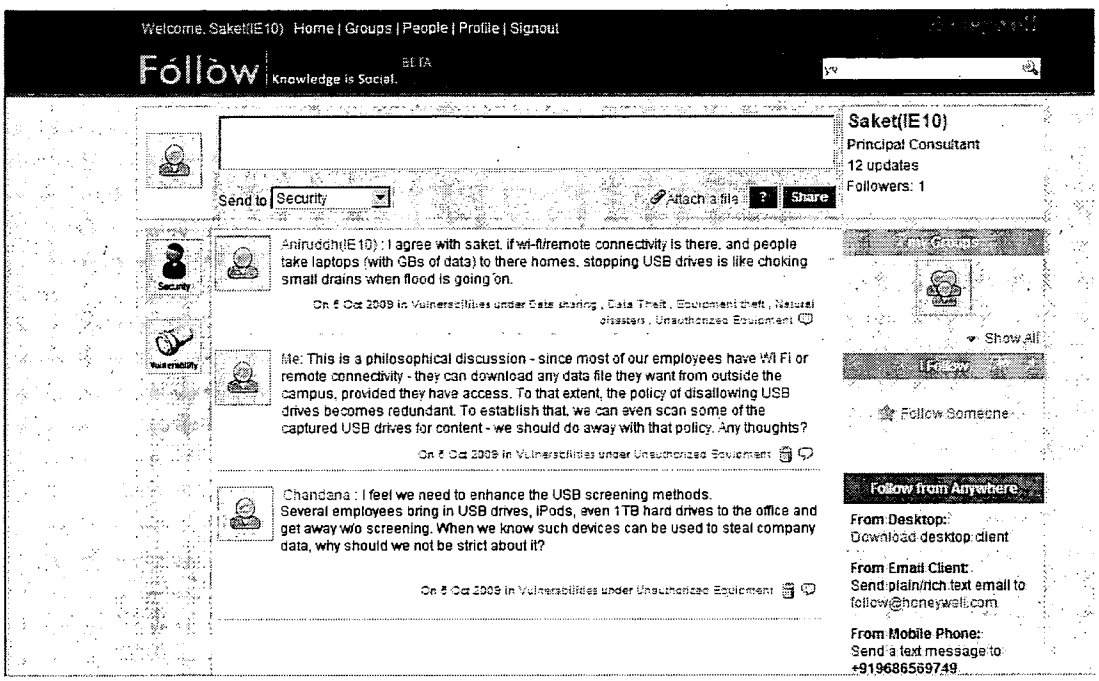

Welcome, Saket(IE10) Home | Groups | People | Profile | Signout
Follow
BETA
Knowledge is Social.
Saket(IE10)
Principal Consultant
12 updates
Followers: 1
Send to Security
Attach a file
Share
Aniruddh(IE10) : I agree with saket. if wi-fi/remote connectivity is there, and people take laptops (with GBs of data) to there homes, stopping USB drives is like choking small drains when flood is going on.
On 5 Oct 2009 in Vulnerabilities under Data sharing , Data Theft , Equipment theft , Natural disasters , Unauthorized Equipment
Me: This is a philosophical discussion - since most of our employees have Wi Fi or remote connectivity - they can download any data file they want from outside the campus, provided they have access. To that extent, the policy of disallowing USB drives becomes redundant. To establish that, we can even scan some of the captured USB drives for content - we should do away with that policy. Any thoughts?
On 5 Oct 2009 in Vulnerabilities under Unauthorized Equipment
Chandana : I feel we need to enhance the USB screening methods.
Several employees bring in USB drives, IPods, even 1TB hard drives to the office and get away w/o screening. When we know such devices can be used to steal company data, why should we not be strict about it?
On 5 Oct 2009 in Vulnerabilities under Unauthorized Equipment
Show All
Follow Someone
Follow from Anywhere
From Desktop:
Download desktop client
From Email Client:
Send plain/rich text email to follow@honeywell.com
From Mobile Phone:
Send a text message to +919686569749

FIG. 3

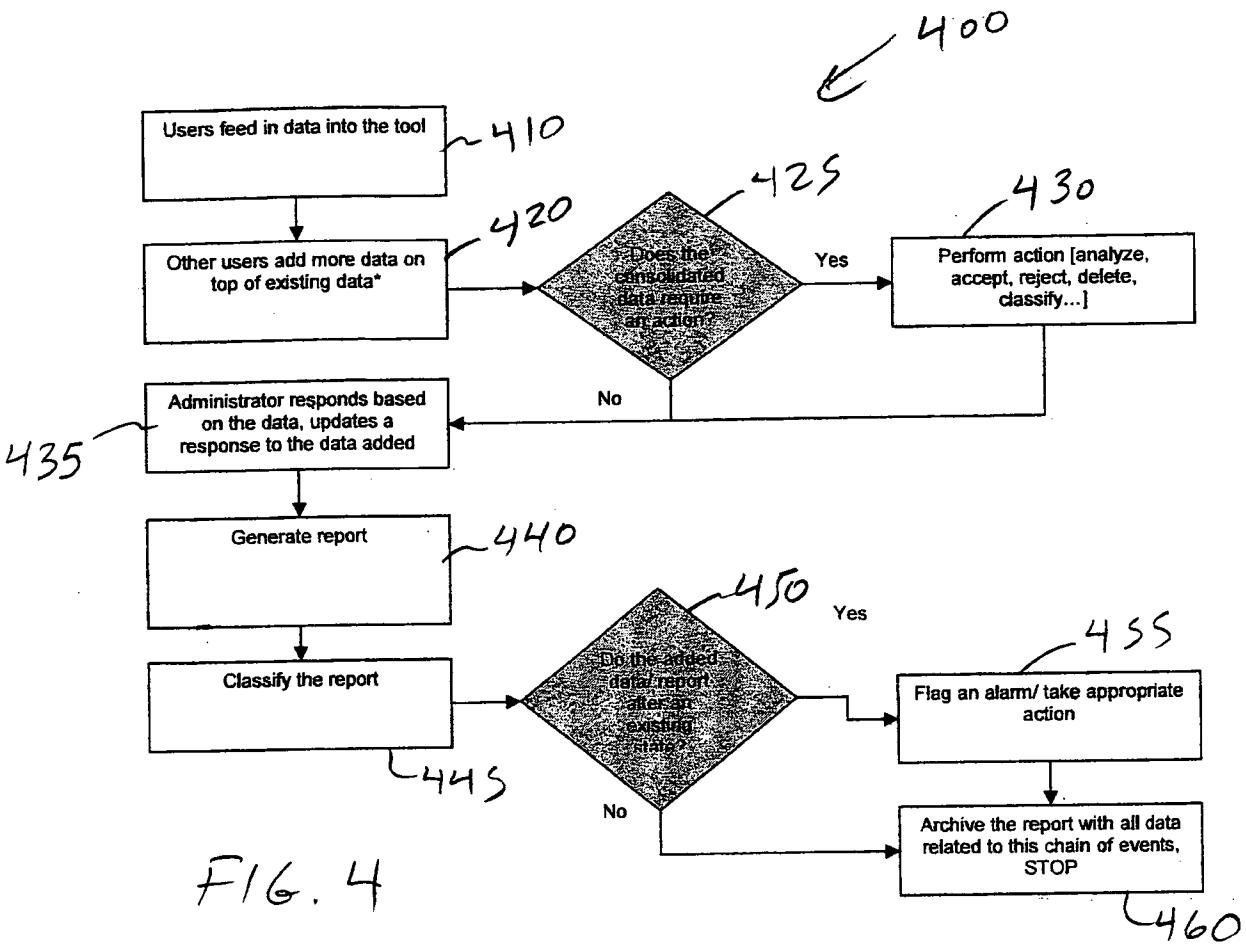

400
Users feed in data into the tool
410
Other users add more data on top of existing data*
420
Does the consolidated data require an action?
425
Yes
Perform action [analyze, accept, reject, delete, classify...]
430
No
Administrator responds based on the data, updates a response to the data added
435
Generate report
440
Classify the report
445
Do the added data/ report alter an existing state?
450
Yes
Flag an alarm/ take appropriate action
455
No
Archive the report with all data related to this chain of events, STOP
460

FIG. 4

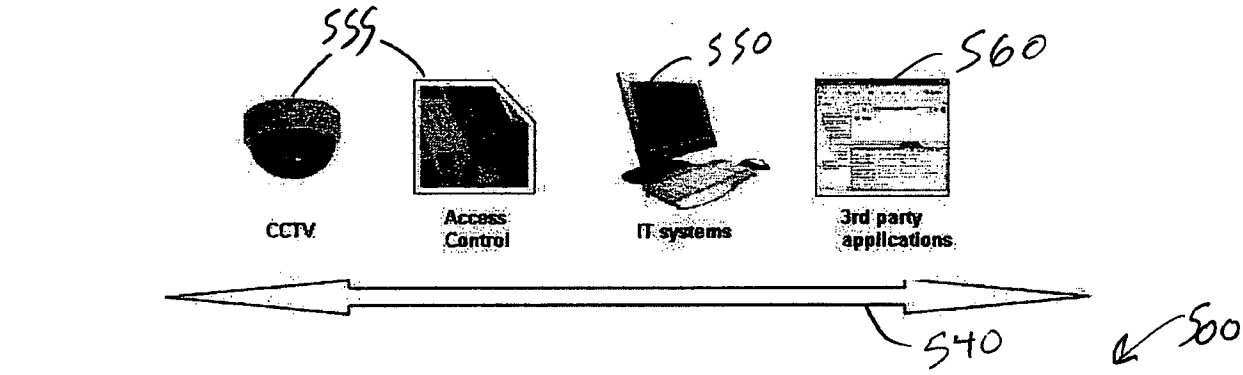
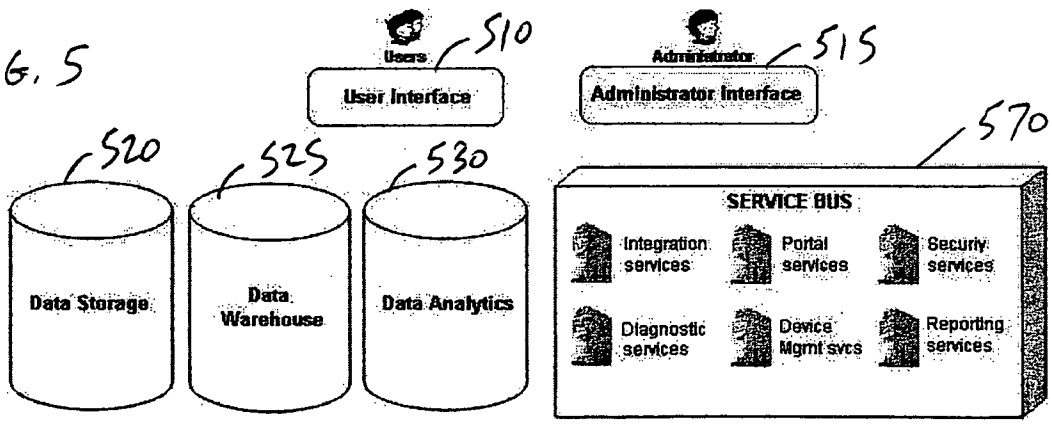

555
550
560
CCTV
Access Control
IT systems
3rd party applications
540
500

FIG. 5


Users
510
User Interface
Administrator
515
Administrator Interface
570
SERVICE BUS
Integration services
Portal services
Security services
Diagnostic services
Device Mgmt svcs
Reporting services
520
525
530
Data Storage
Data Warehouse
Data Analytics

User ID	1234			
Date	Time	Incident ID	Administrator response	Administrator comments
1-03-08	1243	0011223344	Observed to be false, overruled	This is the second time this user has reported a false incident in a week
3-03-08	1501	0011223345	Accepted, security guard sent for verification, USB drive recovered	USB drive will be reissued to violator after project manager approval
9-03-08	0756	0011223346		
2-04-08	1328	0011223347		
6-05-08	1442			
9-05-08	1523			
11-05-08	1641			
14-05-08	2032			

600

FIG. 6

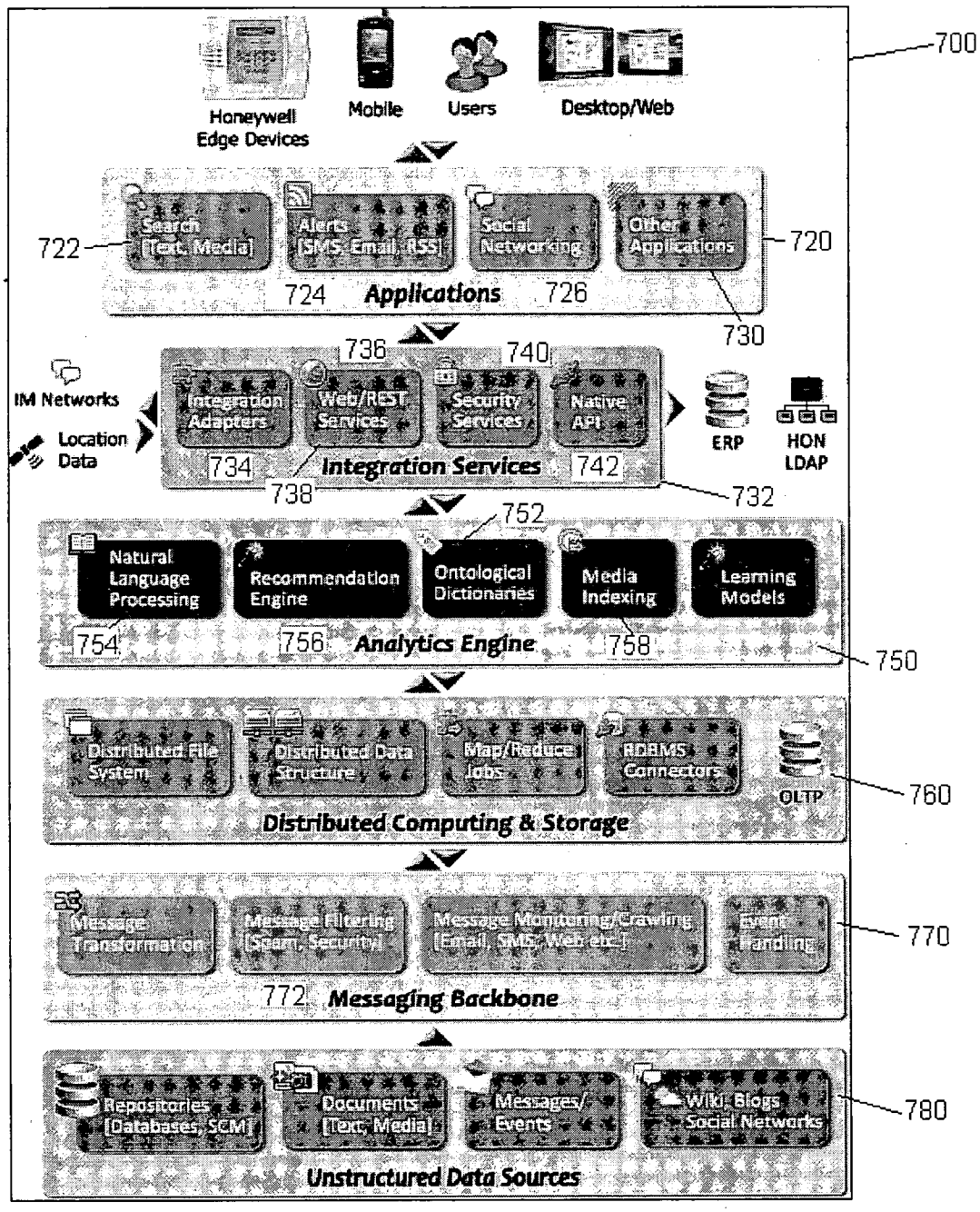

700
Honeywell Edge Devices
Mobile
Users
Desktop/Web
722
Search (Text, Media)
Alerts (SMS, Email, RSS)
Social Networking
Other Applications
720
724
Applications
726
730
736
740
IM Networks
Location Data
Integration Adapters
Web/REST Services
Security Services
Native API
ERP
HON LDAP
734
738
Integration Services
742
732
752
Natural Language Processing
Recommendation Engine
Ontological Dictionaries
Media Indexing
Learning Models
754
756
Analytics Engine
758
750
Distributed File System
Distributed Data Structure
Map/Reduce Jobs
RDBMS Connectors
OLTP
760
Distributed Computing & Storage
Message Transformation
Message Filtering (Spam, Security)
Message Monitoring/Crawling (Email, SMS, Web etc.)
Event Handling
770
772
Messaging Backbone
Repositories (Databases, SCM)
Documents (Text, Media)
Messages/ Events
Wiki, Blogs, Social Networks
780
Unstructured Data Sources

FIG. 7

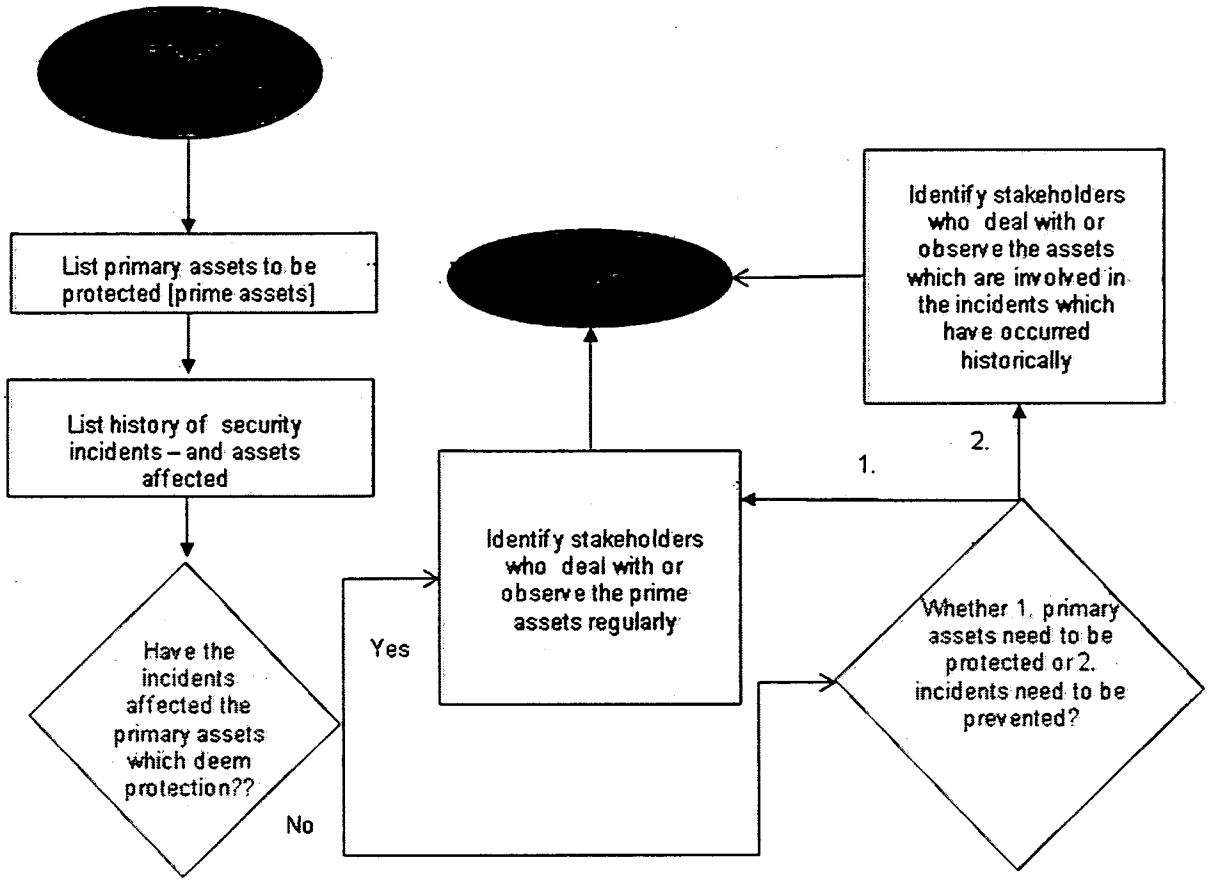

List primary assets to be protected [prime assets]
List history of security incidents – and assets affected
Have the incidents affected the primary assets which deem protection??
Yes
No
Identify stakeholders who deal with or observe the prime assets regularly
Identify stakeholders who deal with or observe the assets which are involved in the incidents which have occurred historically
1.
2.
Whether 1. primary assets need to be protected or 2. incidents need to be prevented?

FIG. 8

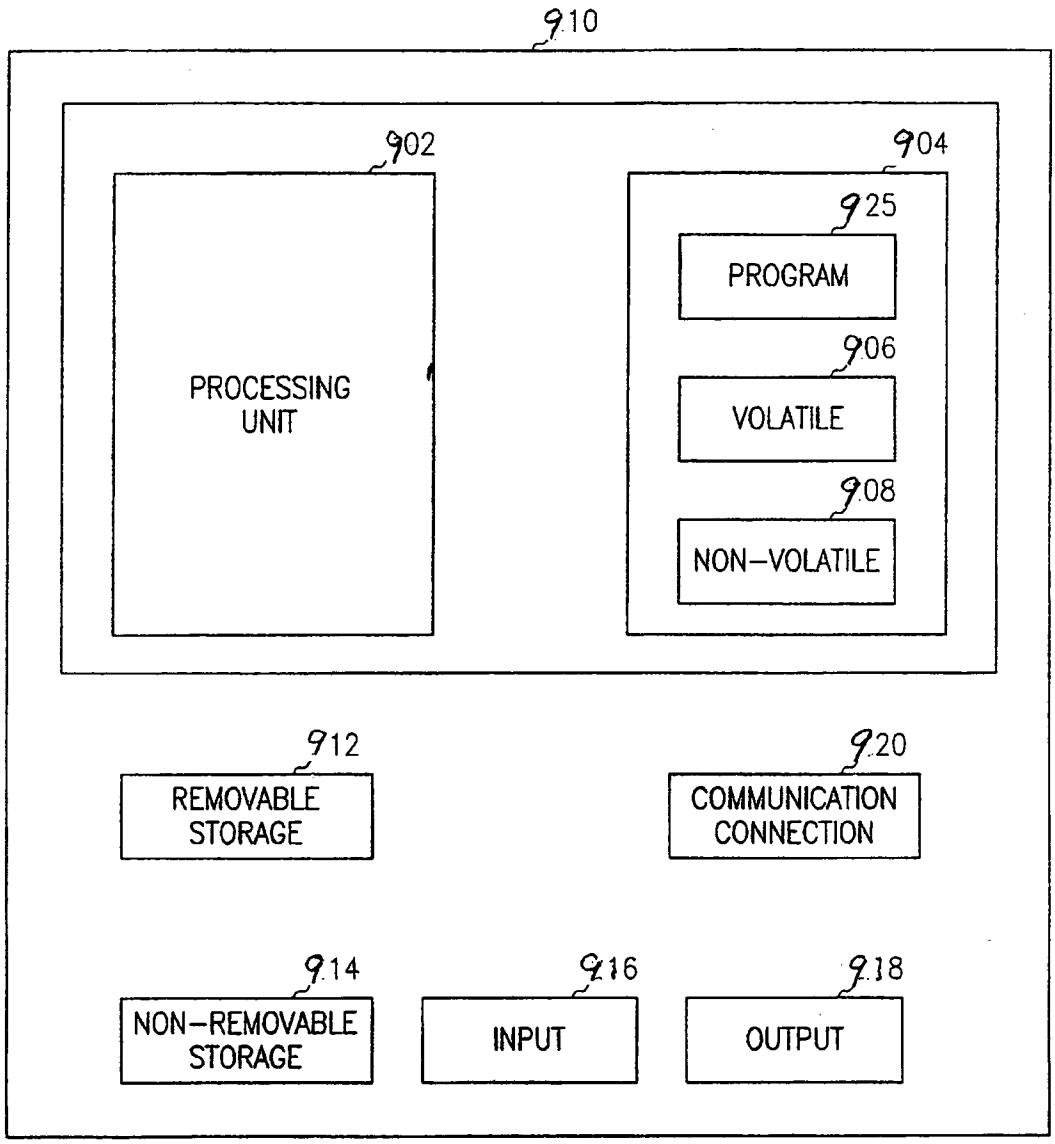

910
902
PROCESSING UNIT
904
925
PROGRAM
906
VOLATILE
908
NON-VOLATILE
912
REMOVABLE STORAGE
920
COMMUNICATION CONNECTION
914
NON-REMOVABLE STORAGE
916
INPUT
918
OUTPUT

FIG. 9

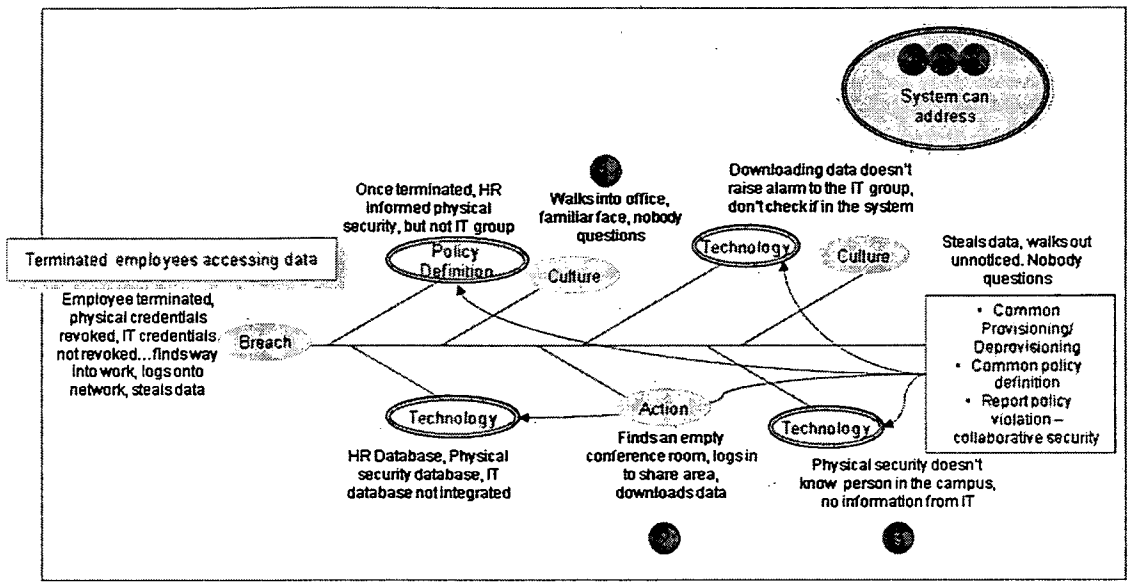

System can address
Once terminated, HR informed physical security, but not IT group
Walks into office, familiar face, nobody questions
Downloading data doesn't raise alarm to the IT group, don't check if in the system
Terminated employees accessing data
Policy Definition
Culture
Technology
Culture
Steals data, walks out unnoticed. Nobody questions
Employee terminated, physical credentials revoked, IT credentials not revoked...finds way into work, logs onto network, steals data
Breach
• Common Provisioning/ Deprovisioning
• Common policy definition
• Report policy violation – collaborative security
Technology
Action
Technology
HR Database, Physical security database, IT database not integrated
Finds an empty conference room, logs in to share area, downloads data
Physical security doesn't know person in the campus, no information from IT

FIG. 10

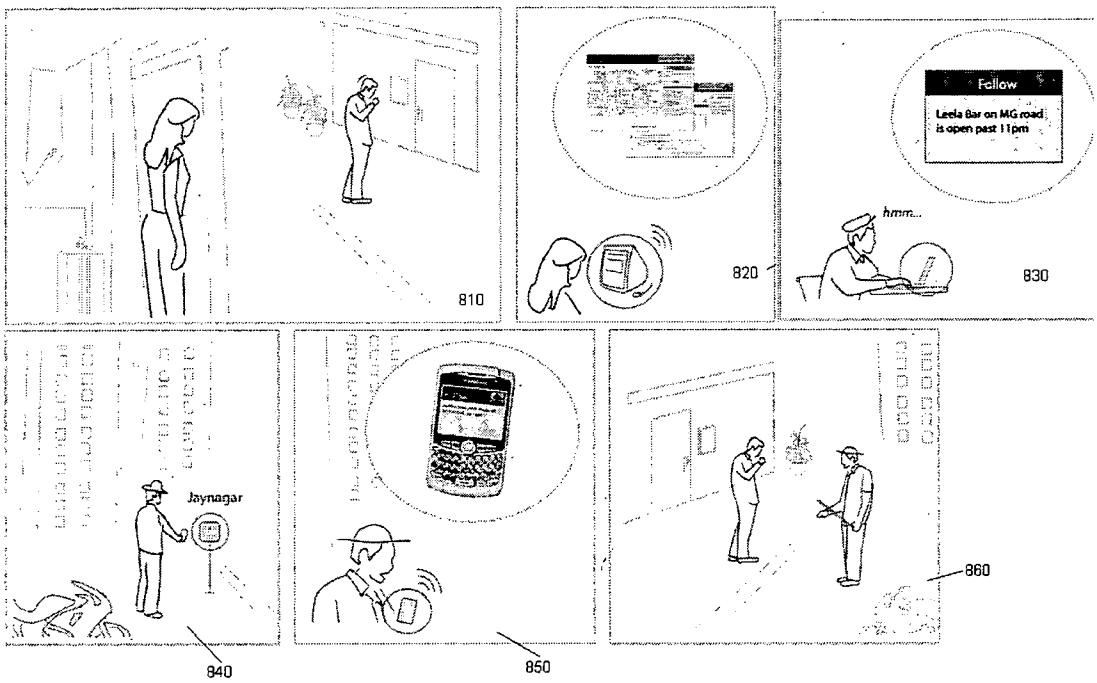

Follow
Leela Bar on MG road is open past 11pm
hmm...
Jaynagar
810
820
830
840
850
860

FIG. 11

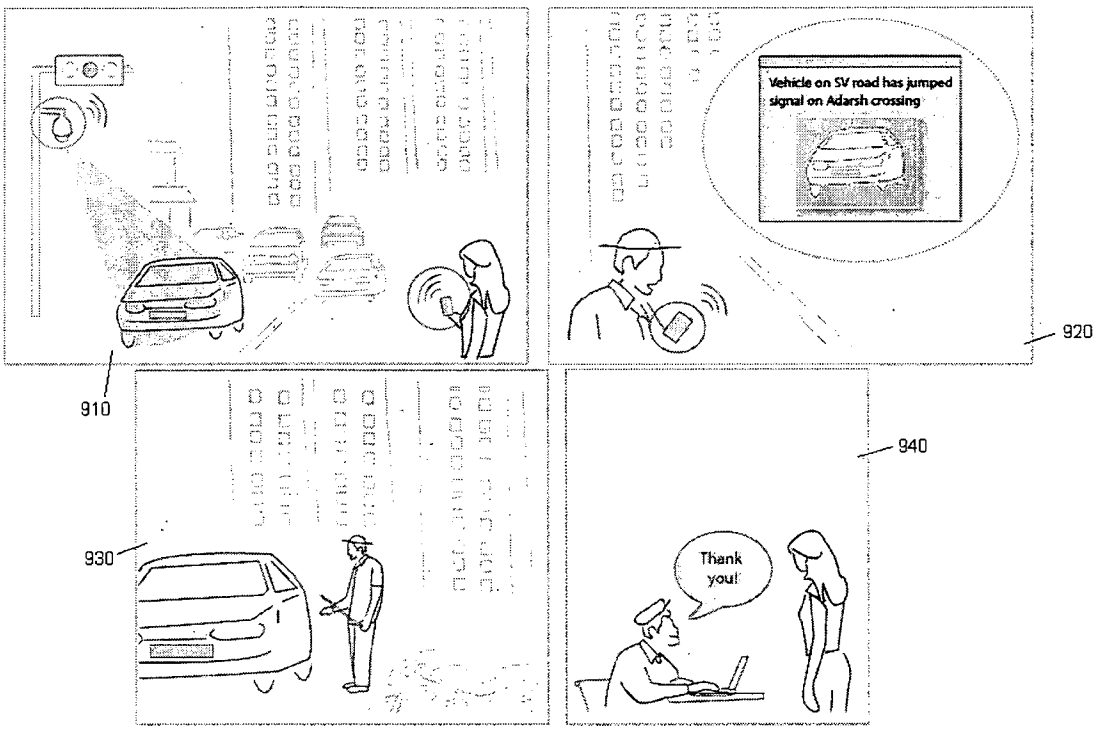

Vehicle on SV road has jumped signal on Adarsh crossing
910
920
930
940
Thank you!

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 10/01578

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 99/00 (2010.01)
USPC - 705/319
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC - 705/319

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 705/1.1, 2, 16, 18, 50, 64, 325; 715/700, 764, 767; 709/201, 203, 223, 224; 379/201.01; 370/431, 462 (keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Dialog; Google
Security, surveillance, threat, violation, intrud, tailgat, guard, user, report, generat, trust, reliability, credibility, enterprise, office, business, physical, building, dynamic, adaptive, learning, artificial, report, summary, evaluat, forum, social

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008/0278579 A1 (DONOVAN et al.) 13 November 2008 (13.11.2008) entire document, especially Abstract; Para [0017], [0019], [0020], [0022], [0023], [0025], [0026], [0029], [0031], [0032], [0089], [0104], [0105], [0108], [0110], [0119]	1 - 20
Y	US 7,158,022 B2 (FALLON) 02 January 2007 (02.01.2007) entire document, especially Abstract; Col 4, ln 40-41, 53-57; Col 5, ln 2-6	1 - 20
A	US 2005/0197847 A1 (SMITH) 08 September 2005 (08.09.2005) entire document	1 - 20
A	US 2007/0115108 A1 (MARTIN et al.) 24 May 2007 (24.05.2007) entire document	1 - 20
A	US 2007/0280462 A1 (NEECE) 06 December 2007 (06.12.2007) entire document	1 - 20
A	US 2008/0091681 A1 (DWIVEDI et al.) 17 April 2008 (17.04.2008) entire document	1 - 20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 November 2010 (11.11.2010)	22 NOV 2010
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774