



(86) Date de dépôt PCT/PCT Filing Date: 2009/03/17
(87) Date publication PCT/PCT Publication Date: 2009/09/24
(85) Entrée phase nationale/National Entry: 2010/09/15
(86) N° demande PCT/PCT Application No.: US 2009/037436
(87) N° publication PCT/PCT Publication No.: 2009/117446
(30) Priorité/Priority: 2008/03/19 (US12/051,709)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01),
H04L 12/58 (2006.01)
(71) Demandeur/Applicant:
WEBSense, INC., US
(72) Inventeur/Inventor:
TROYANSKY, LIDROR, IL
(74) Agent: SMART & BIGGAR

(54) Titre : SYSTEME ET PROCEDE D'ANALYSE D'EVENEMENTS EN RAPPORT AVEC LA DISSEMINATION
D'INFORMATIONS ELECTRONIQUES

(54) Title: SYSTEM AND METHOD FOR ANALYSIS OF ELECTRONIC INFORMATION DISSEMINATION EVENTS

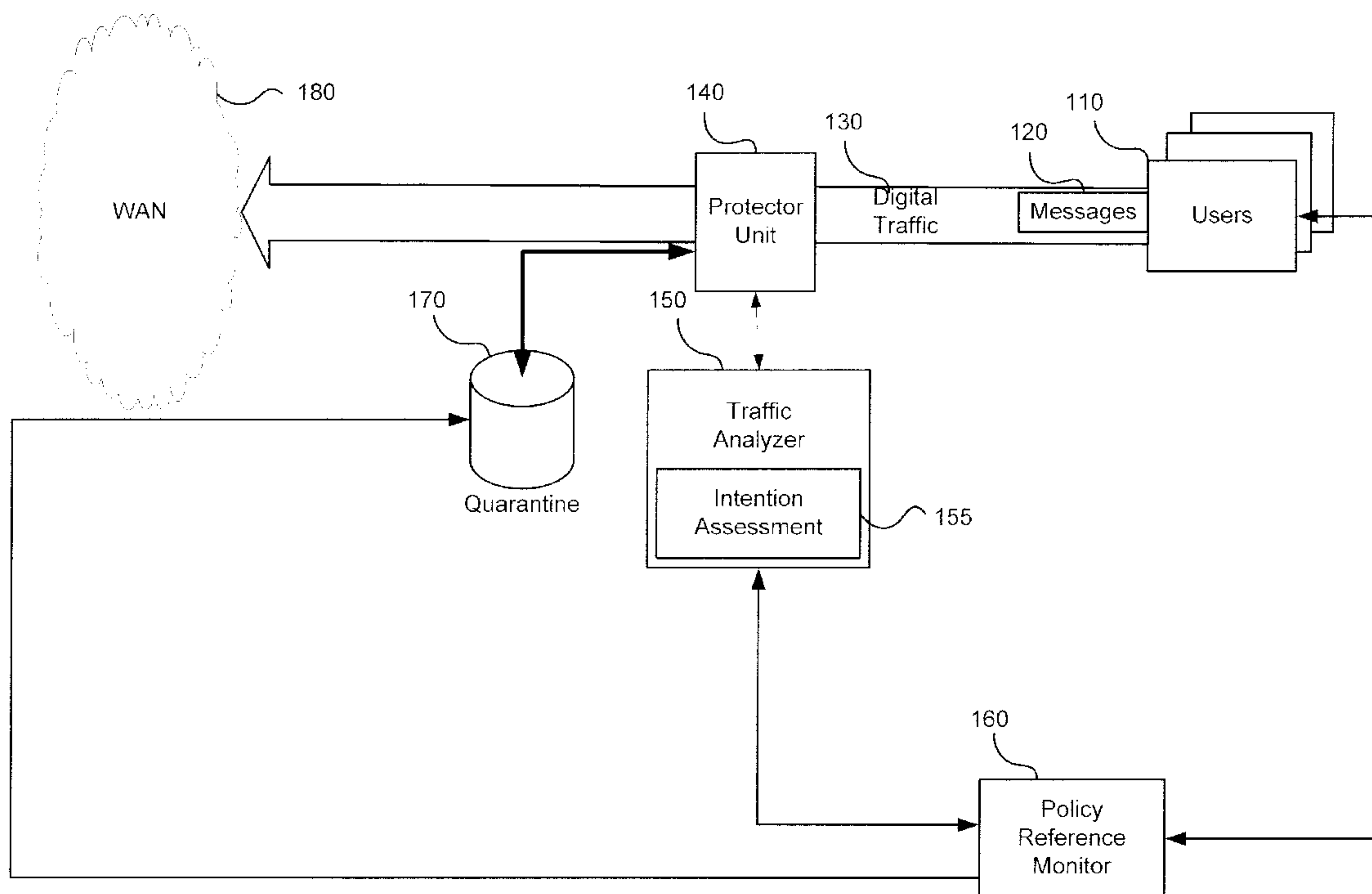


Fig. 1

(57) **Abrégé/Abstract:**

A system and method for determining an intent of a sender (110) in transmitting electronic information' (120) in order to prevent unauthorized dissemination of electronic information is disclosed. The system and method facilitate cost-effective handling of dissemination events and comprise a traffic analyzer (150) configured to analyze descriptors of the electronic information and parameters of the transmission of the electronic information in order to determine the intent of the sender. By determining the intent of the sender, it is possible to effectively quarantine- (170) the electronic information before it is disseminated.

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
24 September 2009 (24.09.2009)

(10) International Publication Number
WO 2009/117446 A3

(51) International Patent Classification:

H04L 29/06 (2006.01) *H04L 12/58* (2006.01)

(21) International Application Number:

PCT/US2009/037436

(22) International Filing Date:

17 March 2009 (17.03.2009)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

12/051,709 19 March 2008 (19.03.2008) US

(71) Applicant (for all designated States except US): **WEB-SENSE, INC.** [US/US]; 10240 Sorrento Valley Road, San Diego, CA 92121 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **TROYANSKY, Lidror** [IL/IL]; 18 Jobotinsky St., 53361 Givatayim (IL).

(74) Agent: **MALLON, Joseph, J.**; Knobbe Martens Olson & Bear LLP, 2040 Main Street, 14th Floor, Irvine, CA 92614 (US).

(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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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))

(88) Date of publication of the international search report:

3 December 2009

(54) Title: SYSTEM AND METHOD FOR ANALYSIS OF ELECTRONIC INFORMATION DISSEMINATION EVENTS

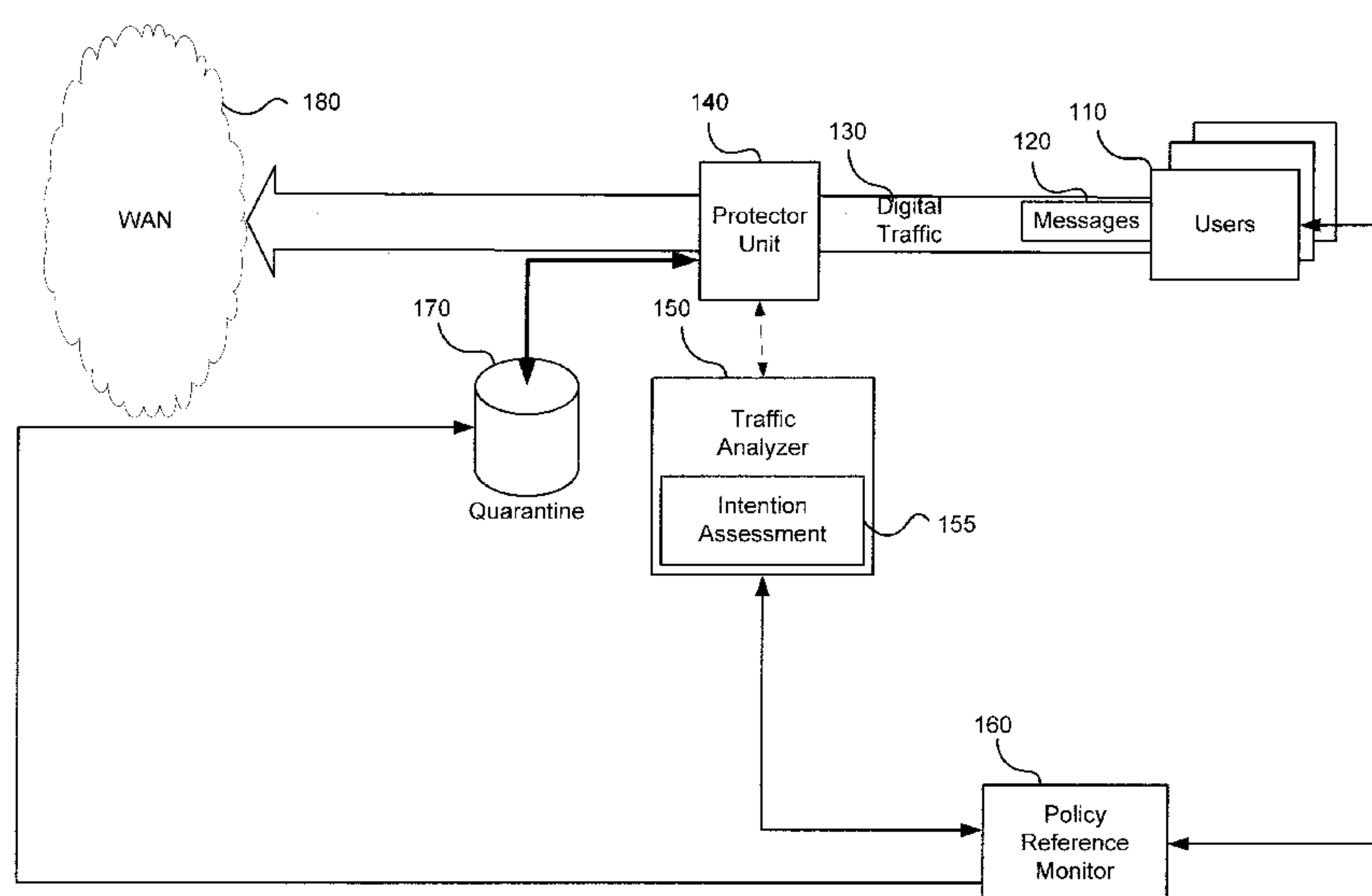


Fig. 1

(57) Abstract: A system and method for determining an intent of a sender (110) in transmitting electronic information' (120) in order to prevent unauthorized dissemination of electronic information is disclosed. The system and method facilitate cost-effective handling of dissemination events and comprise a traffic analyzer (150) configured to analyze descriptors of the electronic information and parameters of the transmission of the electronic information in order to determine the intent of the sender. By determining the intent of the sender, it is possible to effectively quarantine- (170) the electronic information before it is disseminated.

SYSTEM AND METHOD FOR ANALYSIS OF ELECTRONIC INFORMATION DISSEMINATION EVENTS

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates generally to the field of information leak prevention. More specifically but not exclusively, the present invention deals with methods for an efficient and accurate analysis of information dissemination events.

Description of the Related Technology

[0002] Information and knowledge created and accumulated by organizations and businesses are, in many cases, their most valuable assets. Unauthorized dissemination of intellectual property, financial information and other confidential or sensitive information can significantly damage a company's reputation and competitive advantage. In addition, private information of individuals inside organizations, as well as private information of clients, customers and business partners may include sensitive details that can be abused by a user with criminal intentions

[0003] Apart from the damage to both business secrecy and reputation, regulation within the US and abroad poses substantial legal liabilities for information leakage: Regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley act (GLBA) and the privacy-protecting laws of various states and nations imply that the information assets within organizations should be monitored and subjected to an information protection policy in order to protect client's privacy and to mitigate the risks of potential misuse and fraud.

[0004] One of the major challenges in preserving the confidentiality of information and knowledge in modern organizations and businesses is information leaks caused by an authorized user. It turns out that such events of unauthorized dissemination of information, especially via e-mail, are prevalent and happen in many large organizations almost on a daily basis.

[0005] An important aspect of information leakage events by authorized users is the variety of motives, intentions and disposition used in leakage of the electronic information. For example the leakage may be caused by an honest mistake (e.g., using the "reply to all" instead of the "reply" option in the email client may result in sending confidential information to an unauthorized recipient outside the organization), by an attempt to "bending the rules" (e.g., working on a confidential document at home) or from a malicious attempt of information dissemination motivated by greed or anger.

[0006] Handling events of unauthorized dissemination of electronic information in the business environment is extremely demanding because modern organizations produce immense amounts of electronic traffic and it is essential, on the one hand, to maintain the legitimate flow of electronic information undisturbed while, on the other hand, the confidentiality of the information must be maintained. In many cases, deciding whether the information in a particular case is indeed confidential is a difficult and subjective task, and the trade-offs between risking the confidentiality of the information versus disturbing an important business process are far from being clear. In this respect, the question of motivation of the information dissemination becomes important. If the dissemination event is either part of a legitimate (yet problematic) business process or an innocent mistake of the sender, it may be best handled by the sender himself. On the other hand, if the motive for the dissemination is malicious, it is probably better to block the dissemination without letting the sender know about it.

[0007] Current attempts to monitor and enforce policies with respect to electronic information dissemination are, in general, substantially agnostic to motives. This lack of understanding of motives induces less than optimal event handling.

SUMMARY

[0008] A system and method for an efficient and accurate analysis of events of electronic information dissemination is described. The method is based on analyzing and inferring the most probable motives of the dissemination event using various heuristics and/or by looking at various frequent scenarios and asserting the plausibility of each one of these scenarios. The scenarios include motives, intentions and disposition of the sender and

the recipients. The results of the heuristic and scenario-based analysis are preferably used thereafter by a decision system in order to provide the best event handling.

[0009] A system and method for determining an intent of a sender in transmitting electronic information in order to prevent unauthorized dissemination of electronic information is disclosed. The system and method facilitate cost-effective handling of dissemination events and comprise a traffic analyzer configured to analyze descriptors of the electronic information and parameters of the transmission of the electronic information in order to determine the intent of the sender. By determining the intent of the sender, it is possible to effectively quarantine the electronic information before it is disseminated. The descriptors describe at least the content of the message, the sender of the message, and the recipient of the message.

[0010] The traffic analyzer comprises an intention assessment unit for analyzing the descriptors and parameters of the electronic information and determines if the intent in sending the electronic information is malicious or a mistake. The intention assessment unit is configured to determine whether the electronic information should be disseminated based on the intent of the sender and also to determine whether the decision about dissemination should be made by the sender. The intention assessment unit also evaluates a confidence level and severity of the electronic information being disseminated in determining whether to disseminate the electronic information. Furthermore, the intention assessment unit can compare the descriptors and parameters of the electronic information to predefined scenarios in order to determine whether the electronic information should be disseminated. The predefined scenarios are generated from previous electronic information dissemination events and the comparison includes finding a nearest neighbor between the descriptors and parameters and the predefined scenarios. Additionally, it is possible to use heuristics based on the email addresses of the senders and the recipients to assess the intention of the sender.

[0011] A method for identifying a problematic business policy in the transmission of electronic messages is disclosed. The method includes determining the number of electronic messages that were transmitted that violated a prescribed business policy, determining the senders who sent the electronic messages and analyzing the recipients of the electronic messages. Then it is determined whether the business policy for the transmission

of the electronic message is problematic in response to the number of electronic messages, the senders of the electronic messages and the analysis of the recipients of the electronic messages. The step of analyzing the recipients of the electronic messages further comprises analyzing the recipient's addresses for positive and negative indicators that the recipient should be receiving the electronic message. The positive indicators of receipt comprise the recipient's affiliation and the negative indicators or receipt comprise the recipients address belonging to a domain of low reputation.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] For a better understanding of the invention and to show how the same may be carried into effect, reference will now be made, purely by way of example, to the accompanying drawings, in which:

[0013] FIG. 1 is an illustration of a system for information leak prevention that utilizes scenario analysis and assessing of motives.

[0014] FIG. 2 is flowchart illustrating a method for event handling that utilizes intention assessment.

[0015] FIG. 3 is flowchart illustrating a method for event handling using the severity of the event and the confidence level of the decision.

[0016] FIG. 4 is an illustration of a method for assessing the motives and the intentions utilizing the nearest neighbors' method.

[0017] Fig. 5 is an illustration of a method for assessing the motives and the intentions using heuristics based mainly on email address analysis.

[0018] Fig. 6 is an illustration of a method for assessing the plausibility of existence of a broken business process.

DETAILED DESCRIPTION OF CERTAIN INVENTIVE EMBODIMENTS

[0019] The inventors of the systems and methods described in this application have recognized a need for a method and system that includes the probable motives, intentions and disposition of electronic information dissemination events in determining how the dissemination should be handled. Disclosed herein is a method and system which

provides for efficient mitigation of hazards stemming from electronic information leakage, and is operable to mitigate information leakage which occurs when users inside a company breach and/or otherwise compromise confidential data, whether it is private employee or customer details, or the intellectual property of the company. These breaches can take the form of emails sent outside the company, uploading information to the web/Internet, instant messaging, printing, copying data to portable devices etc.

[0020] Before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and the arrangement of the components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments or of being practiced or carried out in various ways. In addition, it is to be understood that the phraseology and terminology employed herein is for the purpose of description and should not be regarded as limiting. Also, it will be recognized that the described components are illustrative and non-limiting and may be implemented solely in software, hardware or the combination of both.

[0021] There are several patterns where well-meaning users may leak electronic information unintentionally. The most common pattern is the simple mistake whereby, for example, electronic information is exposed to the wrong eyes by clicking "reply to all" instead of "reply" while answering a sensitive email, or trusting an email client's auto-complete feature and sending secrets to "John deCompetitor" instead of to "John deCoworker." In other cases, a distribution list is put in the "CC" field instead of the "BCC" field and reveals sensitive names and email addresses.

[0022] Another common pattern that is attributed to modern lifestyle is the "work at home" pattern where an industrious employee may send material containing confidential information to her home webmail account to continue working after work hours, thereby breaching the confidentiality of the materials and company policy.

[0023] Yet another pattern is "eagerness to please" which is the bread and butter of so-called "social engineers". Most people like to be helpful and may willingly disclose confidential information if the asker seems trustworthy and harmless enough. Social

engineers may be able to obtain even the most classified material, like source-code and passwords, simply by asking other people for help in a seemingly innocent manner.

[0024] On the other hand, malicious users who knowingly and deliberately breach security and confidentiality can cause considerable damage. Motivated by greed or discontent, malicious users are a less common source of breaches, but because their attempts are focused the average damage per incident may be greater. In organizations that do not adequately monitor their outgoing information, it is very easy for such a malicious user to successfully breach confidentiality by just sending out classified documents using web-mail. Indeed, it turns out that simple and conspicuous malicious leaks occur often. This can happen, for example, when employees intend to leave the company, and send themselves confidential information like customer portfolios, or technical drawings and source code.

[0025] Between the malicious and well intentioned are the misbehaved patterns. These are behaviors caused by users who do not fully appreciate the value of the company's assets and do not exercise proper caution. Common examples include gossiping, or sharing novel (and confidential) details with friends

[0026] An important aspect of the problem of information leakage stems from the inherent difficulty in defining confidential information. Apart from relatively prima facie cases, there is a wide "gray area" as to what should be classified as confidential. Assessing the level of confidentiality of the information at hand and defining its relevant distribution and usage policy may be subjective, as different people may have different opinions with respect to the confidentiality level and the impact of the distribution policy on business processes. In addition, any automatic system may suffer from false positives such that the system may mistakenly assign a more restrictive policy than it should. To that end, if it can be safely ascertained that a certain event stems from either a false positive of the decision system or an innocent mistake on behalf of the sender, the best mitigation and handling of the electronic information may be to return the message to the sender together with the findings of the decision system and let the sender decide about the desired action, taking into account the relevant trade-off between confidentiality and availability. Since in large organizations the amount of electronic traffic may be immense, and, consequently, the potential frequency of

confidential information dissemination events may be high, the cost reduction that can be achieved by distributing the event-handling may be substantial.

[0027] If, on the other hand, there are grounds to assume that the incident is malicious, the system shouldn't allow the sender to handle the event. Indeed, the sender himself should be "handled" by the authorities of the organization using the evidence gathered by the system. Without inferring to motives of the sender, it would be hard to provide an adequate resolution to the problem.

[0028] The following embodiments describe a system for an efficient assessment of motives and scenarios of electronic information leakage events. Along with the description, each scenario may refer to the entire context of an event of electronic information dissemination, which may include the following details:

- ☐ The source of the message (identity of the sender and the machine);
- ☐ The intention of sender ;
- ☐ The destination of the message;
- ☐ The disposition of the destination;
- ☐ Classification of the information in the message;
- ☐ Details regarding the content of the message;
- ☐ The channel of the electronic traffic; and
- ☐ The time of the transaction.

[0029] While some of the elements of a scenario can be extracted easily and unequivocally from the electronic message (e.g., channel, time and the addresses of the source and the destination) - other elements, such as the classification of the message and the identity and the disposition of the recipient, are, in many cases, harder to assess.

[0030] The most problematic element is the intention of the sender. Indeed, establishing intent is considered to be a difficult task even in other fields such as criminal and civil law. In an embodiment of the described system, the system attempts to establish intention using various heuristics and by considering the most common scenarios/patterns of electronic information leakage and assigning probabilities to each of the scenarios. The system is particularly useful when utilized within a system for information leak prevention

described more fully in the following patent applications, the contents of which are hereby incorporated herein by reference in their entirety:

□ "A System and a Method for Monitoring Unauthorized Transport of Digital Content", US patent application publication number 20020129140;

□ "A method and system for managing confidential information", US patent application publication number 20050288939;

□ "Apparatus and Method for Assuring Compliance with Distribution and Usage Policy", US patent application publication number 20040255147;

□ "Apparatus and Method for Electronic Mail Filtering", US patent application publication number 20040260924

□ "Apparatus and Method for Ensuring Compliance with a Distribution Policy" US patent application publication number 20050027980

□ "A Method and System for Information Distribution Management", US patent application publication number 20050025291

[0031] Referring now to FIG. 1, a system for information leak prevention 100 that utilizes scenario analysis and assessing of motives is shown. Users 110 send electronic information such as email messages 120 with digital traffic 130. A protector unit 140 intercepts the electronic message 120 and sends a copy of it to a traffic analyzer 150 that includes an intention assessment subunit 155. The traffic analyzer 150 and the intention assessment subunit 155 review the electronic message 120 and generate analysis results that are transmitted to a policy reference monitor 160 that determines required actions according to pre-defined policies and the analysis results. For example, one possible action is to send problematic electronic messages 120 to quarantine 170 where the message 120 is held. If the intention analysis from the assessment subunit 155 suggests that the most probable scenario is an innocent mistake than the user 110 can be notified that the message 120 is in quarantine. Preferably, the notification message will comprise a code that allows the user 110 to release the message 120 from the quarantine, using the method described in US patent application publication number 2005002529, "A Method and System for Information Distribution Management", the contents of which are hereby incorporated by reference herein in their entirety. The sender can then alter the message to omit (if required) confidential information

and/ or unauthorized recipients. The released message can then be directed to its destination via the WAN 180.

[0032] Assessing the intention of the user 110 by the intention assessment subunit 155 is far from trivial and can be a difficult task. In many cases, the intention can be assessed by inferring the probabilities of some common scenarios of mistakes and prima facie scenarios of malicious intent given the details of the transaction and the content of the message. Referring now to FIG. 2, a method for assessing these probabilities by looking at the descriptors of the transaction and applying heuristics in order to determine the most probable intention is illustrated. At stage A 210, descriptors of the message 120 (such as source of the message, destination of the message, content of the message, etc...) and parameters of the transaction (such as channel of the message, time of the transaction, etc...) are inputted into the intention assessment subunit 155. At stage B 220, the subunit 155 assesses whether the event is a prima facie malicious event (e.g. sending details of a large number of credit cards together with the name and the social security numbers of the owners to a dubious address) or not. If the event is a prima facie malicious event, the subunit 155 proceeds to step 230 whereby the event is handled as a malicious event and the desired action is commenced. If the event is not a prima facie malicious case, the subunit 155 proceeds to stage C 240 to decide whether the event is a prima facie mistake (e.g. using heuristics such as: "if a confidential document was sent to several internal email addresses together with one external email addresses – define the event as mistake). If it is a prima facie mistake, the subunit 155 proceeds to step 250 whereby the sender can handle the event preferably using the method described in US patent application number 20050025291 "A Method and System for Information Distribution Management", the contents of which are hereby incorporated by reference herein in its entirety. After allowing the sender to handle the event, the subunit 155 logs the details of the event in step 260. If the subunit 155 determines it is not a prima facie mistake in step 240, the subunit assigns an administrator to handle the case in step 270 and logs the event and details in step 260.

[0033] Generally, the method for handling events depends on many factors such as the severity level of the breach, the confidence level of the decision system regarding the fact that the event indeed constitutes a breach and the sensitivity of the organization to

information leakage. FIG. 3 illustrates a method substantially similar to the method of FIG. 2, and includes allowing the tuning of the maximum severity and confidence level in which the event will be handled by the sender.

[0034] More specifically, at stage A 310, descriptors and parameters of the electronic message 120 are inputted into the subunit 155. Next, at stage B 320, the subunit 155 assesses whether the event is a prima facie malicious event. If the event is malicious, the process proceeds to step 330 to be handled accordingly. If the event is not malicious, then the process proceeds to stage C 340 whereby the subunit 155 determines whether the event is a prima facie mistake. If the event is a prima facie mistake, the process proceeds to step 350 whereby the sender can handle the event and step 360 where the event and details are logged. However, if the event is not a prima facie mistake, the process proceeds to stage D 362 whereby the confidence level of the decision (e.g., based on the level of similarity to previously defined confidential information, preferably using the methods described in US patent application number 20020129140: "A System and a Method for Monitoring Unauthorized Transport of Digital Content", and US patent application number 20050288939: "A method and system for managing confidential information", the contents of which are hereby incorporated herein by reference in their entirety) and the severity of the event (based, e.g. on the sensitivity level of the disseminated information and the potential damage that can happen if this information will arrived to a malicious recipient) are evaluated and a numerical value is preferably assigned to each of them. Next at stage E 364, the numerical values assigned to the confidence level and severity are compared to predefined thresholds in order to decide if handling the event should be left to the user or to an assigned administrator. The threshold can be defined by the administrator or a security officer in the organization, in a manner that reflects the organizational policies and procedures with respect to confidential and proprietary information. If the confidence level and severity are higher than the threshold, this indicates that dissemination of the electronic information might not be advisable such that an administrator should be notified in step 370 and the information not transmitted. However, if the confidence level and severity are lower than the predefined threshold, then the process proceeds to step 350 whereby the sender can handle the event and the details are logged in step 360.

[0035] For events which are not clear-cut, it might be preferable to look at similar scenarios from the past in order to assess the sender's intention. FIG. 4 illustrates a method that utilizes a "nearest neighbor classification" for assessing the intention. At stage A 410, the subunit 155 obtains descriptors of the message and parameters of the transaction as previously described for FIG. 2. At stage B 420, similarities are evaluated between various scenarios stored in the database 430 and the descriptors of the message and the parameters of the transaction inputted from stage A 410. The scenarios in database 430 can be from previously logged and analyzed events together with the most probable intentions. At stage C 440, the most similar scenarios are considered wherein the similarity is based upon the similarities of the descriptors described above. In this respect, the process determines the "nearest neighbor" of the event by comparing the event to predefined scenarios. Next, at stage D 450, the subunit 155 decides about the most probable intention of the sender based upon the nearest neighbor found from stage C 440. Additionally, the subunit 155 may also assign a confidence level to the decision – based on the similarity levels to the nearest neighbors. Once the most probable intention is obtained at stage D 450, the subunit can determine the most appropriate actions such as either transmit the message, quarantine the message and inform the sender, or inform an administrator. Preferably, informing the sender should also include the details of the breach and the action needed to make sending the message allowable (e.g., "Please omit confidential information and/or unauthorized recipients")

[0036] Also, the system may utilize some of the following heuristics, based on an analysis of the email addresses within the headers and the body of the message, in order to determine the intention of the user:

[0037] 1. In cases where the message includes several authorized addresses and one or more unauthorized addresses, the event is, with a high probability, non-malicious.

[0038] 2. In cases where the message is sent to an internal unauthorized address, which is very similar to another, authorized address, such that, with a high probability, the auto-complete feature of the mail client causes the event, the event is most probably non-malicious.

[0039] 3. In cases where the user replies to a message using the "reply to all" feature, and the original sender of the replied message is authorized, the event is most probably non-malicious

[0040] The system can also look for events in which the sender is attempting to send information to his or her web-based mail, by looking for similarities between the name of the sender and the webmail address (e.g., Jerald Regan sends a message to JRegan@webbasedmail.com). The system can assess such similarities using, e.g., the measure of similarity known as the "edit distance" between the string of characters in the name and the string of characters in the prefix of the email address. Such attempts may stem from two basic scenarios:

[0041] 1. Attempts to "bend the rules" in order to work at home – this is basically a non-malicious scenario, although it should not be considered as an innocent mistake.

[0042] 2. Attempts to disseminate information for future use when the person involved intends to leave the company (or thinks that he is going to be fired soon) – a malicious event.

[0043] As both events cannot be considered as mistake, both of them should preferably be handled by the administrator. However, the severity level of the two events is different. There are several parameters that can be used in order to determine the likelihood of each of the two scenarios:

[0044] a. The ownership of the confidential information: in case in which the sender is also the owner of the information.

[0045] b. The amount of information: a large number of attached files made the malicious scenario more likely.

[0046] c. The diversity of the information: an intention to work at home will be characterized by documents that pertain to a single topic. High diversity of the information (e.g., topics that represents different types of information – e.g., customer's data and R&D documents) are more likely to stem from a malicious intent. The diversity of the information can be assessed using content classification methods, such as described, e.g., in US patent application publication number 20050288939, "A method and system for managing

confidential information", the contents of which are hereby incorporated herein by reference in their entirety.

[0047] d. The job title and the level of the sender – In most organizations, it will be reasonable to assign a lower level of severity to information dissemination events conducted by top-tier management. (e.g., top-level management in large organizations are less likely to conduct a scam based on identity theft than a low-tier sender).

[0048] Reference is now made to figure 5, which illustrates a method for assessing the intension of the user based on various heuristics as described above. More specifically, at stage A 510, the subunit 155 obtains descriptors and parameters of the electronic message that is suspected as unauthorized. Next, at stage B 520, the email addresses of the message are analyzed, e.g., according to the heuristics described above, in order to assess whether the event is, most likely, a result of a mistake (stage C, 530). If there are positive indications for mistake, then, at stage D 540, the subunit 155 assess the severity level of the event (e.g., based on the potential damage of the unauthorized dissemination). At stage E 542, the subunit 155 compares the severity to a predefined threshold: If the severity is lower than a predefined threshold, then the sender is allowed to handle the event at stage F 544 and the details of the event and the actions of the sender are logged at stage G 546. Otherwise, a message is sent to the assigned administrator at stage H 548 who handles the event according to the applicable policies and procedures. Again, the details of the event and the actions taken are logged at stage G 546. If there are no positive indications for mistake at stage C 530, the subunit 155 further looks for evidence that the information was sent to the private address of the sender at stage H 550. If there are positive indicators for such scenario at stage I 552, then a message is sent to the assigned administrator at stage H 548 who then handles the event according to the applicable policies and procedures. The details of the event and the actions taken are logged at stage G 546. If there are no such indicators, the message may continue for further analysis at stage K 560.

[0049] The system can also look at attempts to conceal the outgoing message as an indicator of malicious intent. Such attempts can be based on replacing characters with other characters (e.g., p@tent instead of "patent", "\$3cr3t" instead of "Secret" etc.) Methods for detection of such manipulations are described in US patent application publication

number 20050288939, "A method and system for managing confidential information", the contents of which are hereby incorporated herein by reference in their entirety.

[0050] Also, the system can infer recidivation patterns of the users and determine accordingly the disposition of the event taking into account the fact that the user was engaged in similar events in the past. Preferably, the system utilizes methods such as those described in US patent application publication number 20050027980, "Apparatus and method for ensuring compliance with a distribution policy", the contents of which are hereby incorporated herein by reference in their entirety, in order to handle recidivate patterns of the users.

[0051] The system can also identify problematic ("broken") business processes, where confidential or non-public information is sent in a manner that may expose it to unauthorized recipients (e.g., sending confidential information to another branch or a subsidiary of the company without any encryption). Such events are non-malicious and may stem from a malformed organizational policy or common mistakes. Identifying broken business processes can be based on the method illustrated in Figure 6 whereby messages that breach a certain policy P_i , preferably in a prescribed time frame (for example, during the last month) are counted as number N at stage A 610. Next, at stage B 620, N is compared with a predefined threshold N_0 in order to determine the frequency of such events. Broken business process are characterized, in general, by the fact that the same type of breach is repeated as part of a routine operation, so one can accept that N should be large enough. The level of the threshold, N_0 , will depend, in general, on the idiosyncratic characteristics of the organization or businesses and the volume of the traffic. If N is smaller or equal than N_0 , then it is, most probably, not a broken business process at stage 630. If N is larger than N_0 , then the number of different senders, N_s , is compared with a threshold Θ_1 at stage C 640, and the number of unique items, that breached the Policy P_i , N_{P_i} , is compared with another threshold, Θ_2 at stage D 650. Again, if $N_s \leq \Theta_1$ or $N_{P_i} \leq \Theta_2$, then it is, most probably, not a broken business process and the process proceeds to stage 630. If both $N_s > \Theta_1$ and $N_{P_i} > \Theta_2$ then the likelihood of a broken business process is further assessed at stage E1 660 whereby the recipients addresses are analyzed for positive indicators of a broken business process, such as:

- Are the recipients affiliated with the organization or its subsidiaries?
- Are the recipients business partners, customers or suppliers?
- Do several different senders send to the same recipient?

[0052] At stage E2 662, the recipient addresses and the methods of sending are analyzed for negative indicators, such as:

- Are the recipients belonging to domains of low reputation?
- Were the messages sent to or from webmail?

[0053] At stage E3 664, the positive and negative indications are combined in order to assess the likelihood of a broken business process. At stage F 670, the assessed likelihood is compared with a likelihood threshold Θ_3 . If the likelihood is greater than Θ_3 the decision is "broken business process" at stage G 680 and a message is preferably sent to the policy owner at stage H 690. Otherwise the decision is negative at stage 630.

[0054] The methods and apparatus disclosed herein address the shortcomings of the presently known configurations by providing a method and system to allow for an efficient handling of events of unauthorized dissemination of information in a digital traffic filtering system.

[0055] It is appreciated that one or more steps of any of the methods described herein may be implemented in a different order than that shown while not departing from the spirit and scope of the invention.

[0056] While the methods and apparatus disclosed herein may or may not have been described with reference to specific hardware or software, the methods and apparatus have been described in a manner sufficient to enable persons of ordinary skill in the art to readily adapt commercially available hardware and software as may be needed to reduce any of the embodiments of the present invention to practice without undue experimentation and using conventional techniques.

[0057] A number of features have been shown in various combinations in the above embodiments. A person skilled in the art can appreciate that the above combinations are not exhaustive and that all reasonable combinations of the above features are hereby included in the present disclosure.

WHAT IS CLAIMED IS:

1. A system for determining an intent of a sender in transmitting electronic information in order to prevent unauthorized dissemination of the electronic information and facilitate cost-effective handling of dissemination events, the system comprising a traffic analyzer configured to analyze descriptors of the electronic information and parameters of the transmission of the electronic information in order to determine the intent of the sender.
2. The system of claim 1, wherein the descriptors comprise at least one of the content of the message, the sender of the message, and the recipient of the message.
3. The system of claim 1, wherein the traffic analyzer comprises an intention assessment unit for analyzing the descriptors and parameters of the electronic information.
4. The system of claim 3, wherein the intention assessment unit determines if the intent in sending the electronic information is malicious or a mistake.
5. The system of claim 3, wherein the intention assessment unit is configured to determine whether the electronic information should be disseminated.
6. The system of claim 3, wherein the intention assessment unit is configured to determine whether the decision about dissemination of the information should be made by the sender.
7. The system of claim 6, wherein the intention assessment unit evaluates a confidence level and severity of the electronic information being disseminated in determining whether to disseminate the electronic information.
8. The system of claim 3, wherein the intention assessment unit compares the descriptors and parameters of the electronic information to predefined scenarios in order to determine whether the electronic information should be disseminated.

9. The system of claim 8, wherein the predefined scenarios are generated from previous electronic information dissemination events.

10. A computer-implemented method for determining an intent of a sender in transmitting electronic information in order to prevent unauthorized dissemination of the electronic information, the method comprising:

determining descriptors and parameters of the electronic information;
analyzing the descriptors and parameters of the electronic information; and
determining the intent of the sender from the analysis of the descriptors and parameters of the electronic information.

11. The method of claim 10, further comprising determining whether the intent of the sender is malicious.

12. The method of claim 10, further comprising determining whether the sender mistakenly transmitted the electronic information.

13. The method of claim 10, further comprising determining a confidence level and severity of the electronic information in deciding the intent of the sender.

14. The method of claim 13, further comprising using the intent of the sender in determining whether the electronic information should be quarantined.

15. The method of claim 14, further comprising using the intent of the sender in determining whether the decision about releasing the electronic information from the quarantine should be made by the sender.

16. The method of claim 10, further comprising comparing the descriptors and parameters of the electronic information to predefined scenarios in order to determine the intent of the sender.

17. The method of claim 16, wherein comparing the descriptors and parameters of the electronic information to predefined scenarios comprises finding a nearest neighbor between the descriptors and parameters and the predefined scenarios.

18. The method of claim 10, further comprising applying heuristics based on the email addresses of the senders and the recipients to assess the intention of the sender.

19. The method of claim 10, further comprising using the intent of the sender in determining whether the electronic information should be disseminated.

20. The method of claim 10, further comprising using the intent of the sender in determining whether the decision about dissemination of the information should be made by the sender.

21. The method of claim 14, further comprising informing the sender the actions required to release the message from quarantine.

22. A computer-implemented method for identifying a problematic business policy in the transmission of electronic messages, the method comprising:

determining the number of electronic messages that were transmitted that violated a prescribed business policy;

identifying the senders who sent the electronic messages;

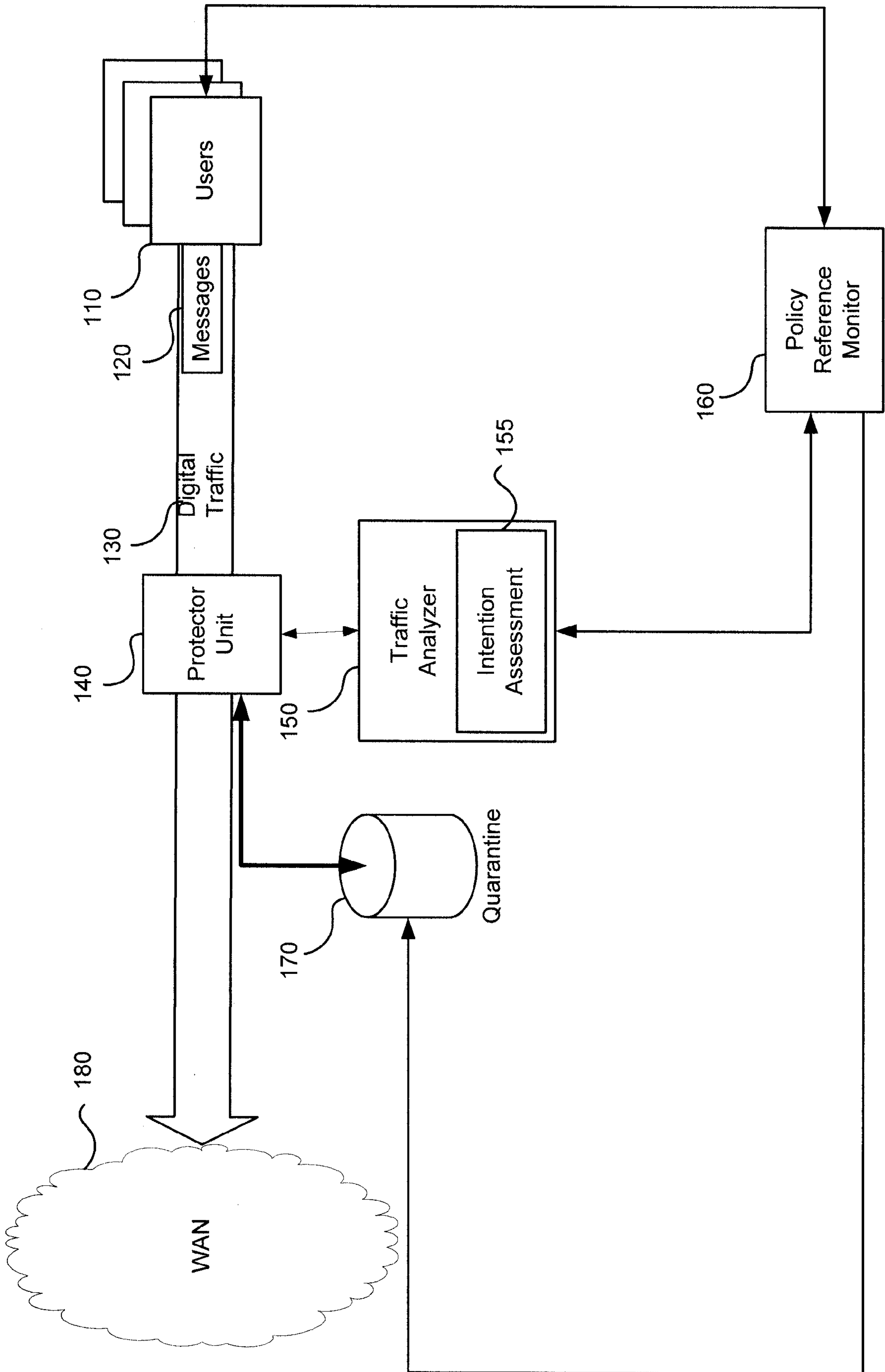
analyzing recipients of the electronic messages; and

determining whether the business policy for the transmission of the electronic message is problematic in response to the number of electronic messages, the senders of the electronic messages and the analysis of recipients of the electronic messages.

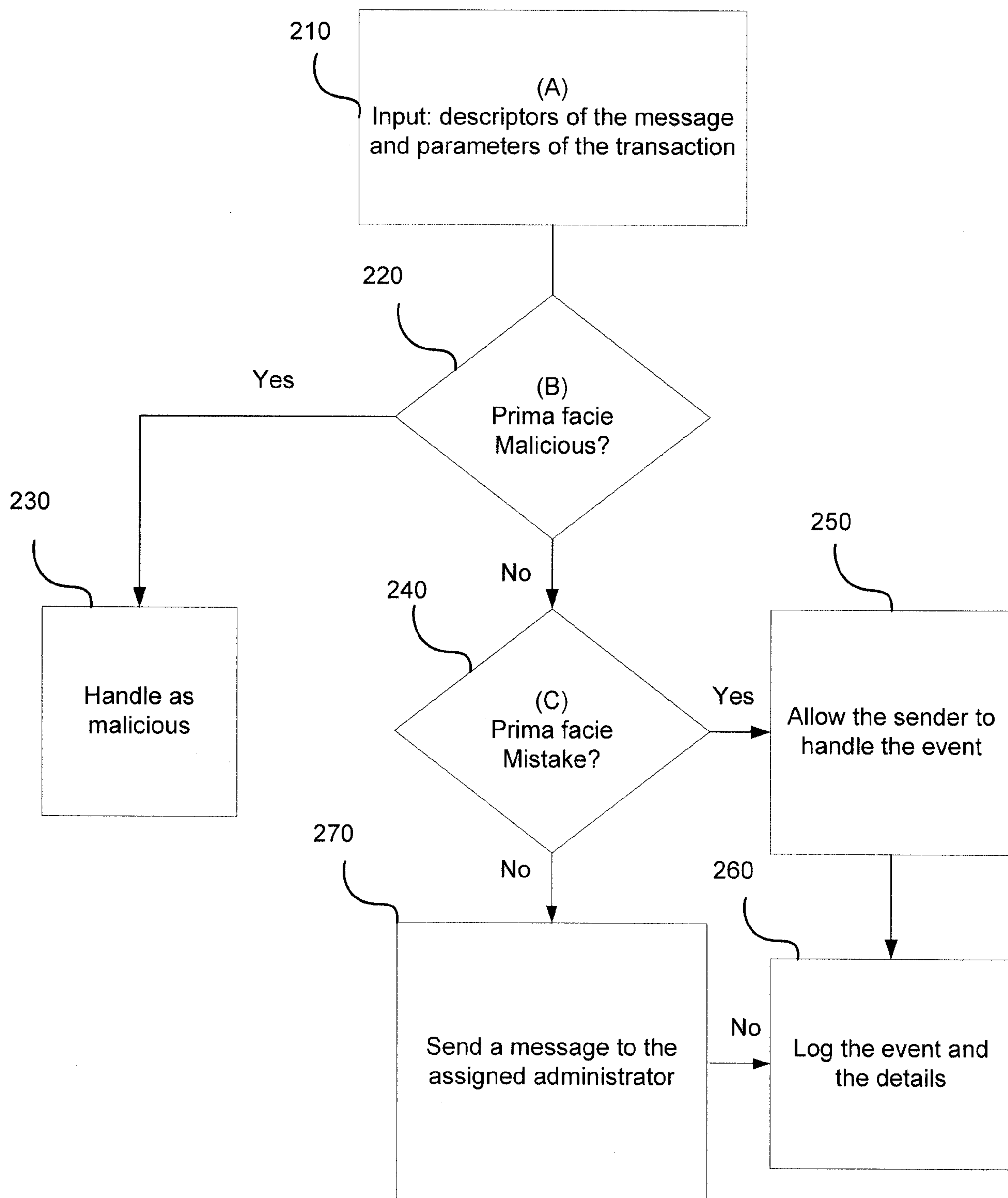
23. The method of claim 22, wherein analyzing recipients of the electronic messages further comprises analyzing the recipients addresses for positive and negative indicators that the recipient should be receiving the electronic message.

24. The method of claim 23, wherein positive indicators of receipt comprise the recipient's affiliation and negative indicators or receipt comprise the recipients address belongs to a domain of low reputation.

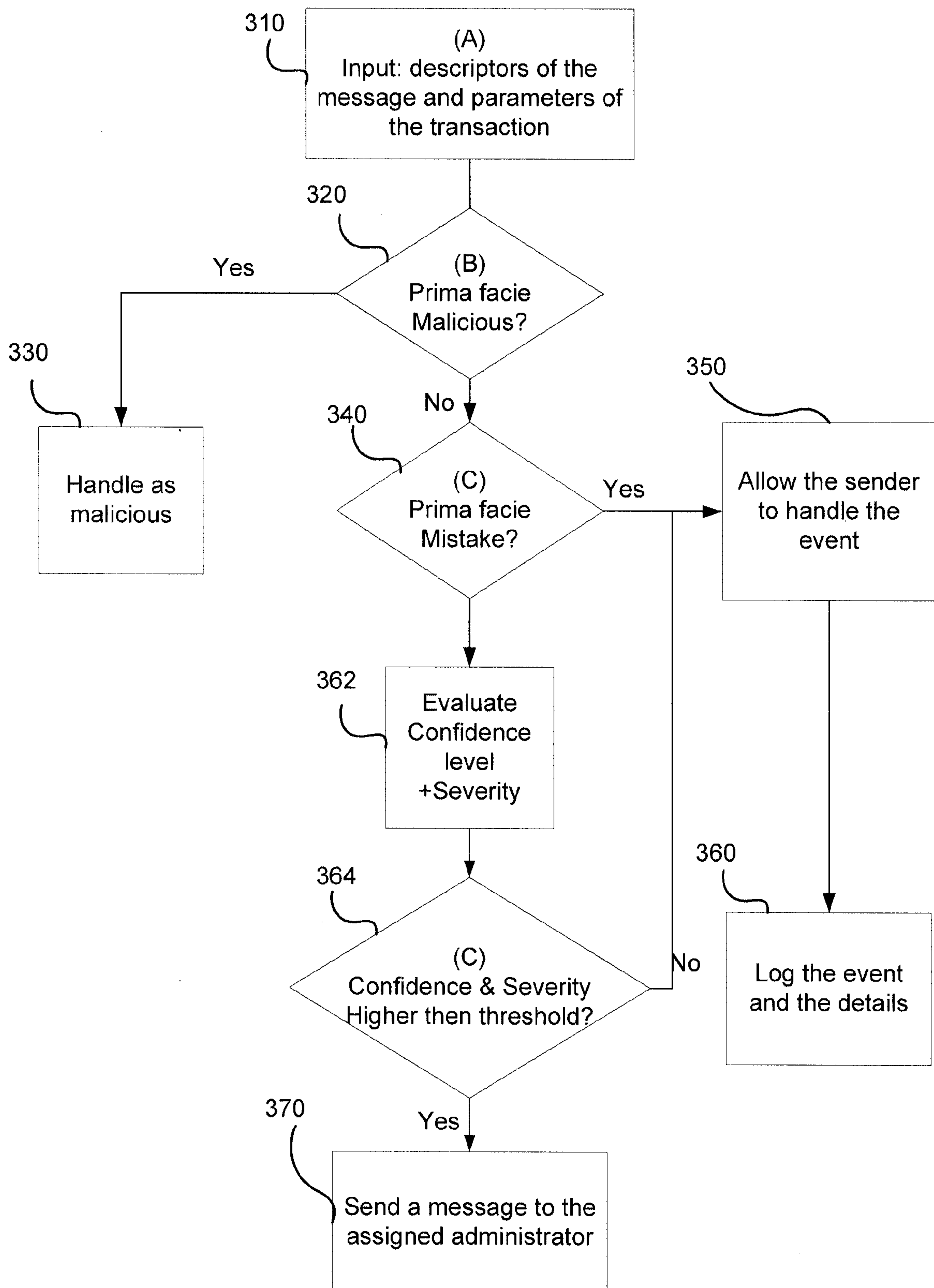
1/6

**Fig. 1**

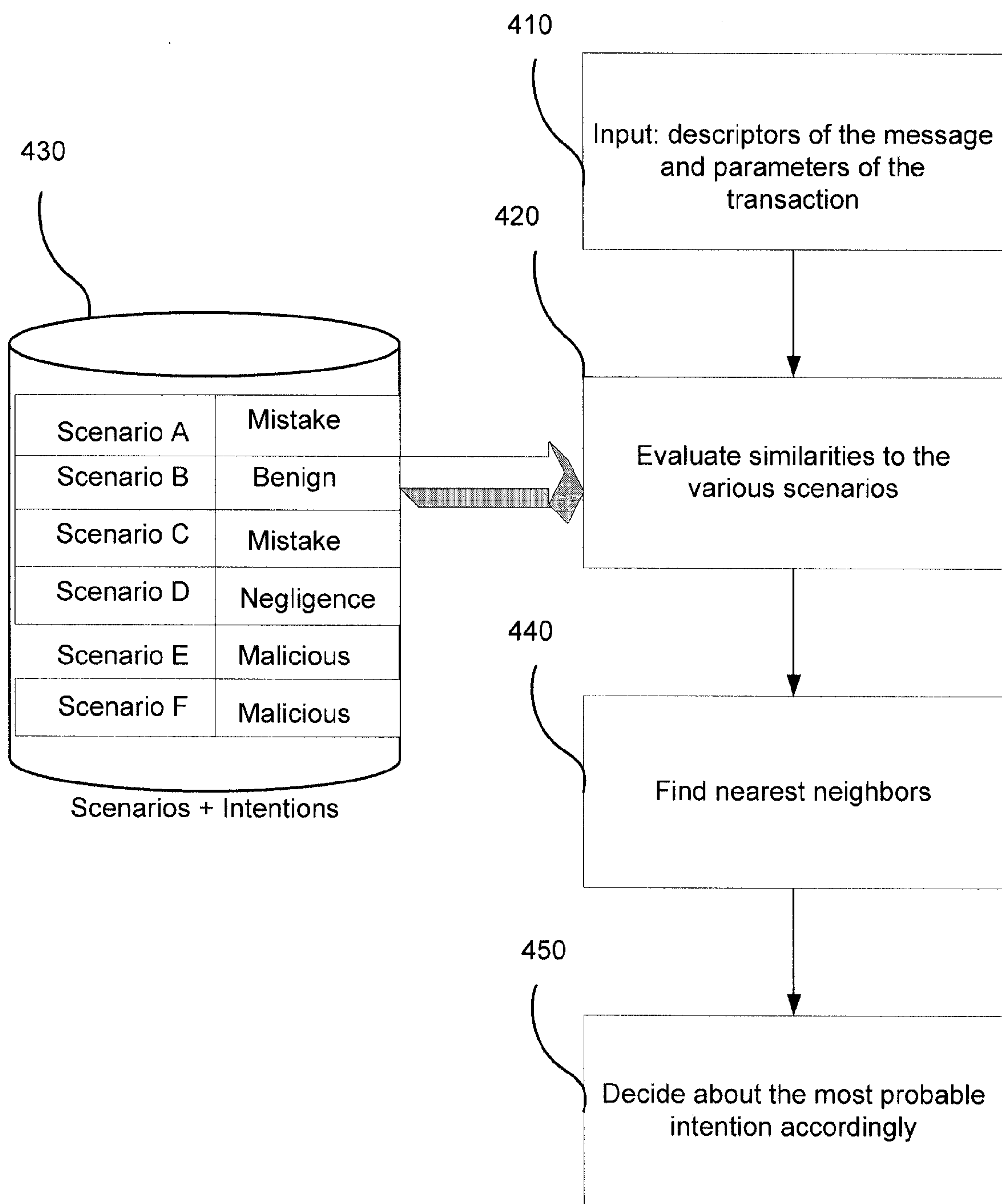
2/6

**Fig. 2**

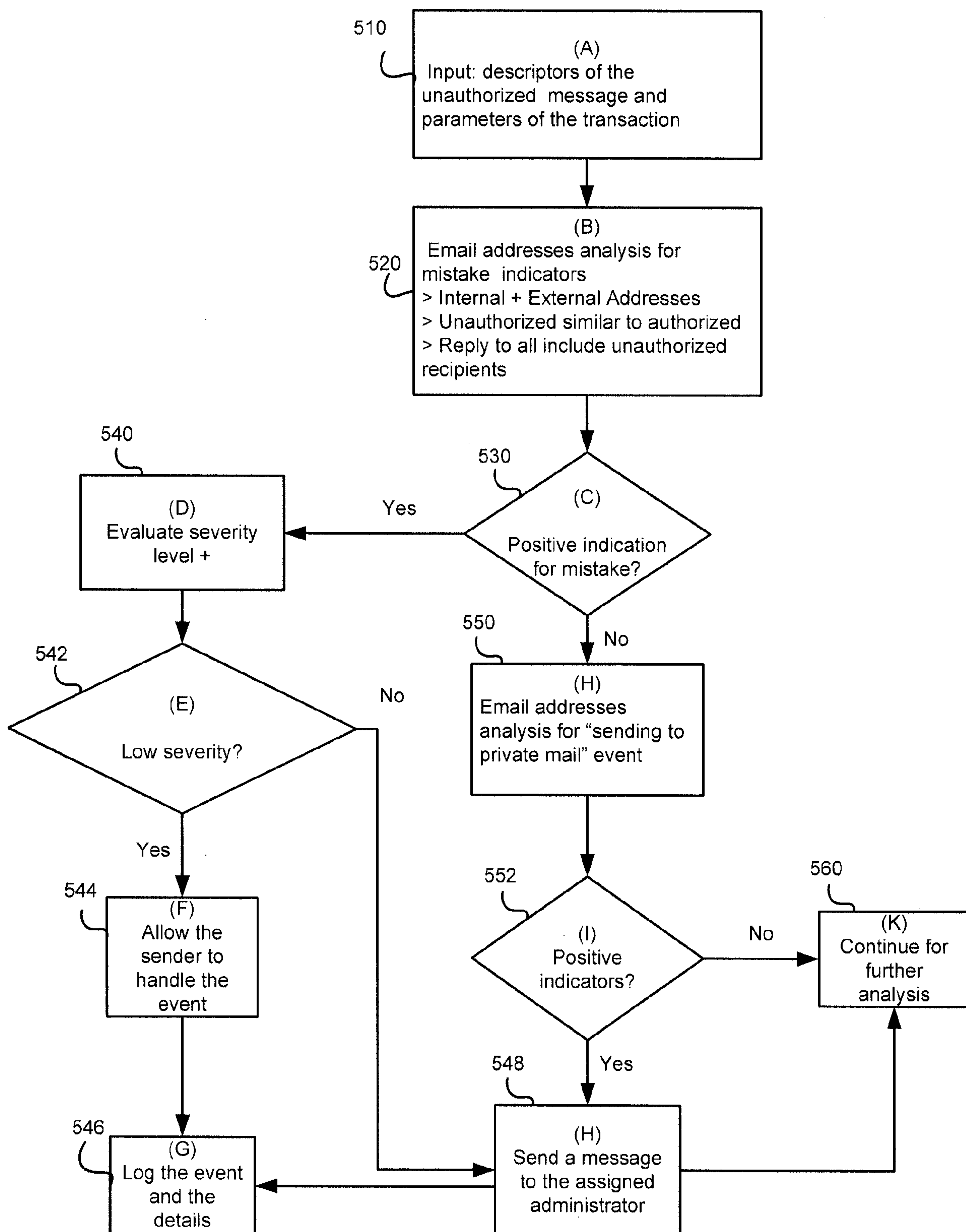
3/6

**Fig. 3**

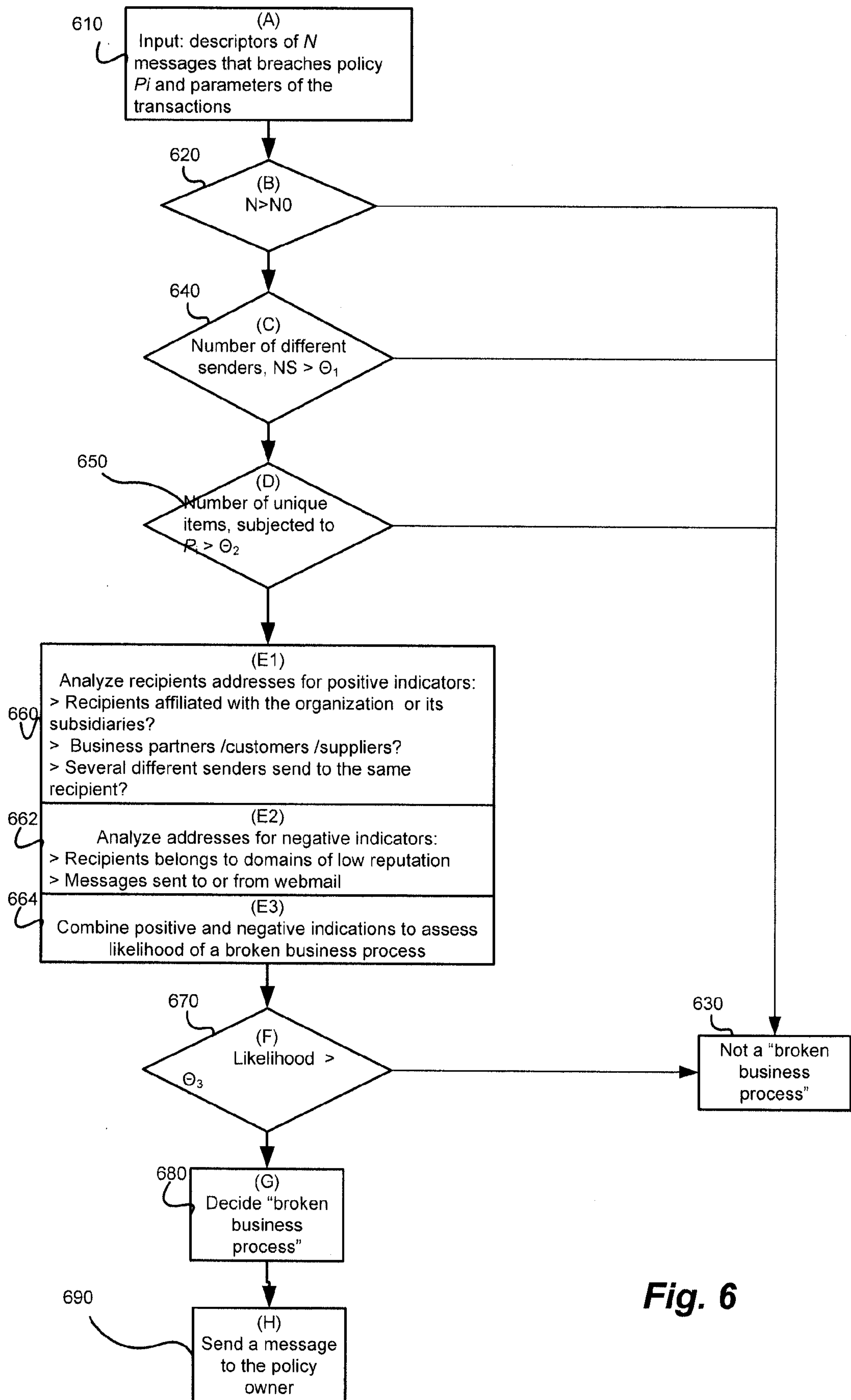
4/6

**Fig. 4**

5/6

**Fig. 5**

6/6

**Fig. 6**

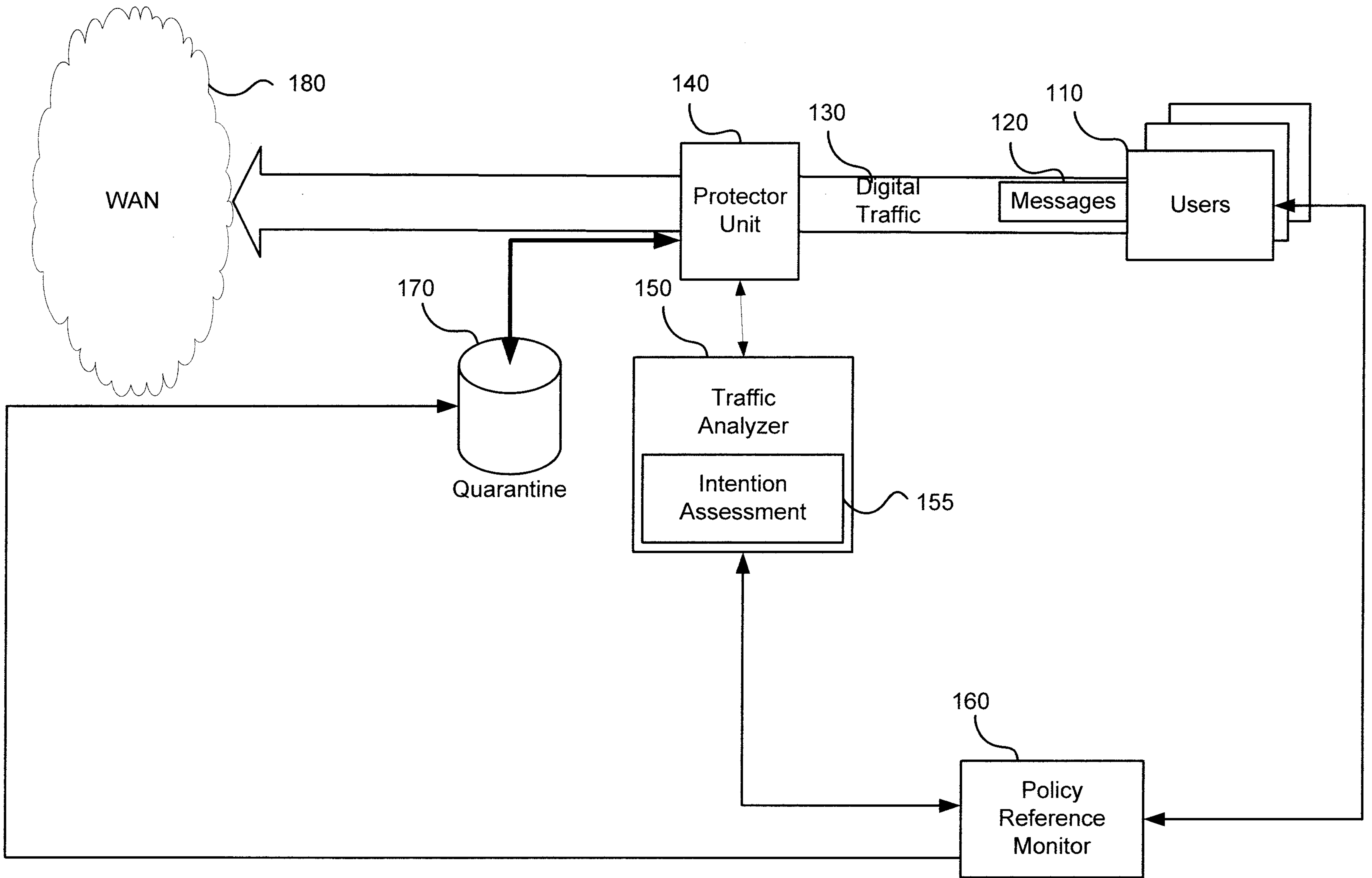


Fig. 1