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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 May 2005 (12.05.2005)

PCT

(10) International Publication Number
WO 2005/043846 A1

(51) International Patent Classification[7]: H04L 12/58, G06F 17/60

(21) International Application Number:
PCT/RU2003/000476

(22) International Filing Date:
3 November 2003 (03.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **ADVA TECHNOLOGIES LTD** [GB/GB]; 259 Yorktown Road, College Town, Sandhurst, Berkshire GU47 0RT (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WALKER, Roy, Simon** [GB/GB]; 259 Yorktown Road, College Town, Sandhurst, Berkshire GU47 0QD (GB). **OPESKINE, Vadim, Borisovich** [RU/GB]; 259 Yorktown Road, College Town, Sandhurst, Berkshire GU47 0QD (GB). **SMIRNOV, Alexey, Anatolievich** [RU/RU]; 24/1 Odoevskogo ul., of. 917, St. Petersburg, 199155 (RU). **LEBEDEV, Andrey, Gennadievich** [RU/RU]; 24/1 Odoevskogo ul., of. 917, St. Petersburg, 199155 (RU).

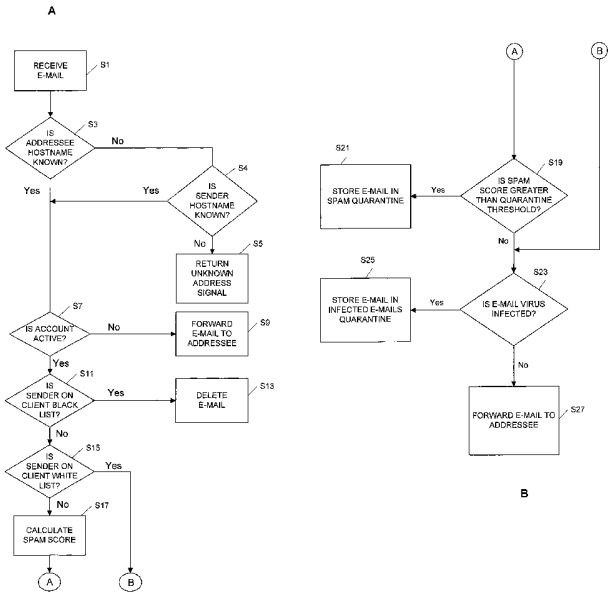
(74) Agent: **NILOVA, Maria, Innokentievna**; PATENTICA, 58 Moika Embankment, St. Petersburg, 190000 (RU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR FILTERING UNWANTED E-MAIL



(57) Abstract: There is described a method of filtering electronic messages transmitted over a communications network, in which a filtering apparatus analyses a received electronic message using predefined tests to derive a message score in dependence thereon, and filters the received electronic message in dependence upon the relationship between the message score and multiple threshold values. The multiple threshold values define at least three value ranges, and the received electronic message is processed in dependence upon which of the at least three value ranges the message score of the received electronic message falls within. In a preferred embodiment, the electronic messages are e-mails, the message score indicates the likelihood that the e-mail is wanted by the addressee, and the filter prevents transmission of e-mails which are unlikely to be wanted by the addressee. There is also described a method of archiving e-mails.

WO 2005/043846 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

APPARATUS AND METHOD FOR FILTERING UNWANTED E-MAIL

This invention relates to the processing of electronic messages. In one aspect, the present invention relates to the filtering of electronic messages. In another aspect, the present invention relates to the archiving of electronic messages.

Electronic mail, hereafter called e-mail, has become progressively more popular for sending messages as more and more people have access to the Internet. One of the main advantages associated with e-mails is negligible mailing cost. However, this negligible cost has resulted in the proliferation of unsolicited bulk e-mails, commonly referred to as spam e-mails. Typically, these spam e-mails are commercial in nature, although some spam e-mails are, for example, political or religious in nature.

For most computer users, spam e-mails are a nuisance because the user must take time to delete the spam e-mails while being careful not to delete any wanted e-mails. Further, many computer users pay a connection time charge for connection to the Internet, and therefore have to pay extra for the time taken to download spam e-mails. From a broader perspective, spam e-mails are a nuisance because they form a significant proportion of Internet data traffic, and therefore slow down the transfer of other Internet data traffic.

A variety of techniques have been developed for filtering out spam e-mails. All these e-mail filtering techniques have to address the problem of how to remove spam e-mails without removing e-mails which are wanted by

the addressee. Generally, it is considered more important that wanted e-mails are delivered than spam e-mails are removed, and therefore the filtering techniques are biased towards ensuring wanted e-mails are delivered.

An e-mail filter which is currently available is a computer program called SpamAssassin. SpamAssassin calculates a "spam score" for an e-mail by applying a plurality of tests to the content of the e-mail, with the likelihood that the e-mail is a spam e-mail increasing as the spam score becomes higher. These tests include tests on the header of a received e-mail, for example how long ago the e-mail was sent and the wording of the title, and the body of the received e-mail, for example testing for words and for syntax which are typically used in spam e-mail. SpamAssassin is also able to test a received e-mail using a Bayesian filtering module which compares the content of the received e-mail with the content of previously received wanted e-mails and previously received spam e-mails to derive a value indicative of the probability of the received e-mail being a spam e-mail. If SpamAssassin generates a spam score above a threshold value, then the corresponding e-mail is either deleted or flagged as potential spam to alert the addressee.

In order to reduce the chance of wanted e-mails being removed by content filters such as SpamAssassin, a preliminary filtering process can be applied in which if the sender of a received e-mail is on a "White List" of approved senders, then the e-mail is delivered directly to the addressee bypassing the content filter.

Similarly, in order to reduce the number of spam e-mails delivered, another preliminary filtering operation

can be applied in which if the sender of a received e-mail is on a "Black List" of prohibited senders, then the e-mail is automatically deleted or flagged as spam.

According to a first aspect of the present invention, electronic messages for an addressee are directed to a filtering station which tests at least part of the content (i.e. the header and the body) of a received electronic message for a plurality of criteria in order to derive a message score. This message score is compared with a plurality of different threshold values to determine how the electronic mail message is subsequently handled by the filtering station. Using plural threshold values enables greater flexibility as to how the electronic messages are processed by the filtering station.

In an embodiment, the multiple threshold values define three non-overlapping ranges of values. If the message score of a received electronic message falls within a first value range indicative of messages which are likely to be wanted by the addressee, than the filtering station automatically forwards the received electronic message to the addressee. If the message score of a received electronic message falls within a second, intermediate value range, then the filtering station stores the electronic message until instructions are received for handling the stored electronic message. If the message score of a received electronic message falls within a third value range indicative that the received electronic message is likely to be a spam e-mail, then the filtering station either deletes the received electronic message immediately or stores the received

electronic message for a limited period of time during which instructions for processing the stored electronic message may be received.

Preferably, the multiple threshold values are adjustable so that different thresholds can be set for different addressees.

According to a second aspect of the invention, electronic messages for an addressee are directed to a filtering station which checks whether or not the sender of the electronic message is on a list of approved senders for the addressee, and if so forwards the electronic message directly to the addressee. If the sender is not on the approved list of senders for the addressee, under predefined conditions the filtering station stores the received electronic message until instructions for processing the stored electronic messages are received from the addressee. In response to an instruction received from the addressee, the filtering station forwards the stored electronic message to the addressee and adds the sender of the stored electronic message to the list of approved senders. In this way, subsequent electronic messages from the sender are automatically directed to the addressee by the filtering station.

According to a third aspect of the invention, electronic messages for an addressee are directed to a filtering station which passes the received electronic message through a Bayesian filter. The co-efficients used by the Bayesian filter are updated in accordance with at least some of the electronic messages passing through the filtering station. In an embodiment, the co-efficients

are updated using all electronic messages passing through the filtering station. In another embodiment, separate sets of co-efficients are generated for different groups of addressees, and each set of co-efficients is updated using electronic messages for the members of the corresponding group of addressees. In another embodiment, each individual addressee has an associated set of co-efficients, and each set of co-efficients is updated using only the electronic messages for the corresponding addressee.

According to a fourth aspect of the invention, electronic messages for an addressee are directed to a filtering station which filters the received electronic message in accordance with predefined rules. The filtering station generates and transmits an electronic message to the addressee which includes interface data allowing the addressee to enter instructions for implementation by the filtering station. These instructions may alter the predefined rules, or may indicate how to handle electronic messages stored by the filtering station in accordance with the predefined rules. In an embodiment, the electronic message generated and transmitted by the filtering station is an HTML e-mail. In an alternative embodiment, the electronic message generated and transmitted by the filtering station is a plain text e-mail.

According to a fifth aspect of the invention, electronic messages for an addressee are directed to a routing station which stores a copy of the electronic message in an archive associated with the addressee of the electronic message. By forming such an archive, if

the addressee deletes the original electronic message, then subsequently a copy of the electronic message can be retrieved from the archive.

In an embodiment, the routing apparatus periodically sends sets of archive data to an archiving apparatus for storage. The archiving apparatus may be either local to the addressee, or may be a server attached to a communications network such as the Internet. If the archiving apparatus is a server attached to the Internet, preferably a web browser program is used as an interface to enable the addressee to access electronic messages stored in the archiving apparatus.

According to a sixth aspect of the invention, electronic messages for an addressee are directed to a filtering station which checks whether or not the sender of the electronic messages is on a list of approved senders for the addressee, and if so forwards the electronic message directly to the addressee. In order to generate the list of approved senders, electronic message addresses are retrieved from an electronic address book for the addressee, the retrieved electronic message addresses are displayed to the addressee to allow the addressee to identify one or more electronic message addresses for addition to the list of approved senders, and then the identified electronic message addresses are transmitted to the filtering station which updates the list of approved senders accordingly. This is particularly advantageous when initially establishing a list of approved senders.

According to a seventh aspect of the invention,

electronic messages for a family are directed to a filtering station which filters the electronic messages in accordance with predefined rules set by a senior member of the family. This type of "parental control" enables the senior member of the family to control which electronic messages are forwarded to children within the family. This is particularly advantageous given the pornographic nature of a large number of spam e-mails. Preferably, the senior member of the family sets the predefined rules so that the children of the family only receive electronic messages from an approved list of senders. In this way, electronic messages are only sent to the children of the family from senders who are approved by the senior member of the family.

Various embodiments of the invention will now be described with reference to the accompanying Figures, in which:

Figure 1 schematically shows an electronic mail delivery system according to a first embodiment of the invention;

Figure 2 schematically shows the configuration of a client database stored in a mail filtering station which forms part of the electronic mail delivery system illustrated in Figure 1;

Figure 3 schematically shows the configuration of anti-spam options stored in the client database illustrated in Figure 2;

Figure 4 schematically shows the configuration of a spam quarantine stored in the client database illustrated in Figure 2;

Figure 5 is a block diagram schematically showing the interaction of the main functional components of the mail filtering station illustrated in Figure 1;

Figure 6 is a block diagram schematically showing the interaction of the main functional components of a mail filter forming part of the mail filtering station with data stored in the client database;

Figure 7 is a block diagram schematically showing the interaction of the main functional components of an anti-spam filter illustrated in Figure 6 with data stored in the client database;

Figures 8A and 8B show a flow chart illustrating the operations performed by the mail filtering station in response to the receipt of an e-mail;

Figure 9 shows a flow chart illustrating operations performed by a client administrator computer, which forms part of the electronic mail delivery system illustrated in Figure 1, and the mail filtering station to adjust threshold parameters stored in the client database;

Figure 10 schematically shows a portion of a web page forming a user interface at the client administrator computer via which a client administrator adjusts threshold parameters stored in the client data base stored in the mail filtering station;

Figure 11 shows a flow chart illustrating operations performed by the client administrator computer and the mail filtering station to process e-mails stored in the spam quarantine of the mail filtering station;

Figure 12 schematically shows a portion of a web page forming a user interface at the client administrator

computer via which the client administrator inputs instructions for processing e-mails stored in the spam quarantine;

Figure 13 shows a flow chart illustrating the operations performed to process quarantined e-mails using received instructions;

Figure 14 shows a flow chart illustrating the operations performed on a periodic basis by the mail filtering station to process automatically e-mails stored in the spam quarantine;

Figure 15 schematically shows the contents of a code memory of a mail filtering station forming part of an electronic mail delivery system of a second embodiment of the invention;

Figure 16 schematically shows the configuration of client data stored in the client database of the mail filtering station of the second embodiment of the invention;

Figure 17 schematically shows in more detail the configuration of user data which forms part of the client data illustrated in Figure 16;

Figure 18 is a block diagram schematically showing the interaction of the main functional components of the mail filtering station of the second embodiment of the invention;

Figures 19A and 19B show a flow chart illustrating the operations performed by the mail filtering station of the second embodiment of the invention in response to the receipt of an e-mail;

Figure 20 shows a flow chart illustrating in more

detail an operation to adjust Bayesian filter coefficients which forms part of the flow chart illustrated in Figures 19A and 19B;

Figure 21 shows a flow chart illustrating the operations performed by a user computer and the mail filtering station of the electronic mail delivery system of the second embodiment to process e-mails stored in the spam quarantine of the mail filtering station;

Figure 22 shows a flow chart illustrating in more detail an operation to process e-mails stored in the spam quarantine in accordance with user instructions which forms part of the flow chart illustrated in Figure 21;

Figure 23 is a block diagram schematically showing the contents of a mail filtering station forming part of an electronic mail delivery system of the third embodiment of the invention;

Figure 24 schematically shows the configuration of an e-mails archive forming part of the mail filtering station illustrated in Figure 23;

Figure 25 schematically shows the configuration of a client archive forming part of the e-mails archive illustrated in Figure 24;

Figure 26 is a block diagram schematically showing the interaction of the main functional components of the mail filtering station of the third embodiment of the invention;

Figure 27 schematically shows the interaction of the main functional components of an archiver forming part of the mail filtering station with data stored in the e-mails archive;

Figure 28 schematically shows an electronic mail delivery system according to a fourth embodiment of the invention;

Figure 29 is a block diagram schematically showing the interaction of the main functional components of the mail filtering station illustrated in Figure 28;

Figure 30 schematically shows the main components of an on-line e-mails archive forming part of the electronic mail delivery system illustrated in Figure 28;

Figure 31 schematically shows the configuration of a user database forming part of the on-line e-mails archive illustrated in Figure 30;

Figure 32 is a block diagram schematically showing the interaction of the main functional components of the on-line e-mails archive illustrated in Figure 30;

Figure 33 is a block diagram schematically showing the interaction of the main functional components of an archiver forming part of the on-line e-mails archive illustrated in Figure 32;

Figure 34 schematically shows the main components of a client computer forming part of an electronic mail delivery system according to a fifth embodiment of the invention;

Figure 35 shows a flow chart illustrating the operations performed to obtain and transmit e-mail address information to a mail filtering station forming part of the electronic mail delivery system of the fifth embodiment; and

Figure 36 schematically shows a portion of a user display forming a user interface at the client computer

via which a user inputs instructions identifying e-mail address information.

FIRST EMBODIMENT

System Overview

Figure 1 shows an e-mail delivery system for sending e-mails to the employees of a firm, hereafter called a client, via a mail filtering station 1 which processes received e-mails to identify e-mails which are likely to be wanted by the addressee, checks the identified wanted e-mails for viruses, and forwards the e-mails which pass the virus check to the client. E-mails which are identified as potential spam e-mails by the mail filtering station 1 are stored in the mail filtering station 1 along with respective spam scores which are indicative of the likelihood of the corresponding e-mail being a spam e-mail. In particular, an e-mail is stored in the mail filtering station 1 if the corresponding spam score is greater than a quarantine threshold. Storing potential spam e-mails at the mail filtering station 1 has the advantage of reducing network data traffic, and in particular reducing the amount of data sent to the client.

The mail filtering station 1 also processes e-mails sent by the employers of the firm to identify and quarantine spam e-mails and virus infected e-mails. In this way, the chance of the employees of the firm sending customers and other addressees viruses is reduced, and also an early warning is provided in case their mail server should be hacked into by unscrupulous senders of spam e-mails.

Although only one client is shown in Figure 1 for

ease of illustration, plural clients can take advantage of the processing performed by the mail filtering station 1. In this embodiment, each client has an associated hostname and each employee of each client has an associated username, so that the e-mail address of an employee is of the form username@hostname.com. The client shown in Figure 1 is based at an office 3 which includes a client mail server 5 to which are connected a plurality of user computers 7a, 7b. The client office 3 also includes a client administrator computer 9, which is connected to the client mail server 5, via which a client administrator is able to adjust mail system settings. In this embodiment, the client mail server 5, the user computers 7 and the client administrator computer 9 are all conventional.

The mail filtering station 1 and the client mail server 5 are connected to each other, and to a plurality of other conventional mail servers 11 (only one of which is shown in Figure 1 for ease of illustration), via a communications network 13. In this embodiment, the communications network 13 forms part of the Internet. Each of the mail servers 11 are connected to a respective plurality of conventional sender computers 15a,15b, and users of the sender computers 15 are able to send e-mails to and receive e-mails from the employees of the client by using a conventional e-mail program.

A domain name server 17, which stores a database containing network address data for a plurality of hostnames, is also connected to the communications network 13. The network address data includes a MX record giving the mail server address to which e-mails

for the hostname are to be delivered. In this embodiment, the mail server address provided in the MX record for the hostname of a client of the mail filtering station 1 is the mail address of the mail filtering station 1 instead of the client mail server 5, as would normally be the case. In this way, when the user of one of the sender computers 15 sends an e-mail to an employee at the client office 3, the e-mail is directed to the mail filtering station 1.

As described above, the mail filtering station 1 stores an e-mail if an associated spam score is greater than a quarantine threshold. In this embodiment, the manner in which an e-mail stored in mail filtering station 1 is processed varies in dependence upon how much the corresponding spam score is above the quarantine threshold. If the spam score of a stored e-mail is between the quarantine threshold and a drop threshold, then the e-mail is stored until instructions are received from the client administrator indicating how the e-mail is to be processed. The client administrator sends these instructions by downloading a web page giving an index of all of the stored e-mails, and identifying using the index which e-mails are to be forwarded and which e-mails are to be deleted. If the spam score of a received e-mail is above the drop threshold, then the received e-mail is only stored for a short period of time, and if no instructions are received from the client administrator by the end of this short period of time then the mail filtering station 1 automatically deletes the stored e-mail. By automatically deleting e-mails which have a high likelihood of being a spam e-mail, the amount of work required by the client administrator to

review the e-mails stored in the mail filtering station 1 is reduced.

In this embodiment, the client administrator is able to set the quarantine threshold and the drop threshold by accessing a quarantine configuration web page. In this way, each client is able to customise the performance of the mail filtering station 1. For example, if a client finds that too many spam e-mails are being allowed through by the mail filtering station 1, then the client is able to lower the quarantine threshold. Further, if a client finds that virtually all e-mails stored at the mail server 1 are spam e-mails, then the client is able to reduce the drop threshold so that a larger proportion of the stored e-mails are automatically deleted.

The Mail Filtering station

As shown in Figure 1, the mail filtering station 1 includes a communications network interface 19 which receives signals 21 from the communications network 13 and transmits signals 21 via the communications network 13. The communications network interface 19 is connected to a processor 23 which processes received signals in accordance with program code stored in a code memory 25 which is also connected to the processor 23. As shown in Figure 1, the code memory 25 includes a control module 27 which controls the overall operation of the mail filtering station 1, a mail filtering module 29 which processes received e-mails to check for spam e-mails and virus-infected e-mails, and a web page generating module 31 which generates web page data which provides a user interface via which the client administrator sends

instructions for dealing with stored e-mails and for adjusting parameters which determine how received e-mails are processed.

A data memory 33, a clock 35 and an operator interface 37 are also connected to the processor 23. The operator interface 37 enables the program code stored in the code memory 25 or data stored in the data memory 33 to be modified by an operator of the mail filtering station 1. The operator interface 37 includes a reader (not shown in Figure 1) which enables program code or data to be downloaded from a floppy disk 39. The clock 35 provides time and date information.

The data memory 33 includes a client database 41 storing details for a plurality of clients who utilise the mail filtering station 1, a set of generic filter rules 43 to be applied by the mail filtering module 29 for all clients, web page templates data 45 used by the web page generating module 31, and an e-mail cache memory 47 for temporarily storing e-mails which are to be forwarded to the client mail server 5.

As shown in Figure 2, the client database 41 stores plural sets of client data 51a to 51c which store information for respective clients. Each set of client data 51 is configured to store the hostname 53 for the client, a password 55 which is used by the client administrator to access web pages generated by the mail filtering station 1 giving details of stored e-mails and of parameter settings for the client, an account status 57 indicating whether or not the account is active, an e-mail address 59 to which messages generated by the mail filtering station 1 for the client administrator are

sent, and a client mail server address 61. Each set of client data also stores anti-spam options 63, anti-virus options 65, a spam quarantine 67 in which e-mails which are likely to be spam e-mails are stored and an infected e-mails quarantine 69 in which e-mails which fail the virus check are stored. In this embodiment, the anti-virus options indicate which one or more of a plurality of virus-checking programs are to be applied to received e-mails. Each set of client data also includes configuration data 71 giving details of the amount of memory dedicated to the spam quarantine 67 and to the infected e-mails quarantine 69, the maximum number of e-mails to be stored in the spam quarantine 67 and in the infected e-mails quarantine 69, the maximum amount of time e-mails are to be stored in the spam quarantine 67 and in the infected e-mails quarantine 69 and the maximum number of lines of an e-mail stored in the spam quarantine 67 and in the infected e-mail quarantine 69 to be forwarded as a preview.

The anti-spam options 63 are shown in more detail in Figure 3. As shown, the anti-spam options 63 include a client Black List 81 which lists addresses for known sources of spam e-mails, a client White List 83 which contains addresses from which e-mails are definitely wanted by the client, client filter rules 85 which are set by the client administrator and applied by the mail filtering module 25 to e-mails addressed to the client, the quarantine threshold 87 which is set by the client administrator to determine the spam score above which received e-mails are stored in the spam e-mails quarantine 67 rather than being forwarded to the addressee, and the drop threshold 89 which is set by the

client administrator to determine the spam score above which e-mails are only stored in the spam quarantine 67 for a short period of time (i.e. shorter than the maximum period of time set in the configuration data 71). Figure 4 shows in more detail the contents of the spam quarantine 67. As shown, the spam quarantine 67 includes an index 91 of all the e-mails stored in the spam quarantine 67, together with the stored e-mails 93a to 93c.

Figure 5 shows a schematic functional overview of the mail filtering station 1, in which operations performed by code in the code memory 25 are represented by functional blocks.

In a conventional manner, world wide web data is transmitted over the communications network 13 using the HTTP protocol and e-mail data is transmitted over the communications network 13 using the SMTP protocol. As shown in Figure 5, HTTP-encoded data received from the communications network 13 via the communications network interface 19, which conventionally is addressed to IP port eighty, is processed by an HTTP codec 101, which removes the HTTP encoding. Similarly, SMTP-encoded data received from the communications network 13 via the communications network interface 19, which conventionally is addressed to IP port twenty-three, is directed to an SMTP codec 103 which removes the SMTP encoding. Data processed by the HTTP codec 101 or the SMTP codec 103 is directed to a controller 105, which controls the processing of data within the mail filtering station 1. The controller 105 is also able to transmit data to the HTTP codec 101 or the SMTP codec 103, which encode data

received from the controller 105 in accordance with their respective protocols and transmit the encoded data to the communications network 13 via the communications network interface 19.

The controller 105 is also able to cause a web page generator 107 to generate web page data for a plurality of web pages using the web page templates data 45. For some web pages, the web page generator 107 inserts data retrieved from the client database 41 into a corresponding web page template. When web page data for a requested web page has been generated by the web page generator 107, the web page data is sent by the controller 105 to the HTTP codec 101 prior to transmission over the communications network 13.

The controller 105 is also able to send received e-mails to a mail filter 109, which processes the received e-mails to check for spam e-mails and for virus-infected e-mails in accordance with the generic filter rules 43 and anti-spam options 63 and anti-virus options 65 retrieved from the client database 41. The operator interface 31, the clock 35 and the e-mail cache memory 47 are also connected to the controller 105.

Figure 6 shows a schematic functional overview of the mail filter 109, together with the data within the client database 41 which is used by the mail filter 109. As shown, the mail filter 109 is formed by an anti-spam filter 121 and an anti-virus filter 123. The anti-spam filter 121 operates in accordance with parameters stored in the generic filter rules 43 and the anti-spam options 63 associated with the client to which the e-mail being processed is addressed. The anti-spam filter 121 sends

potential spam e-mails to the spam quarantine 67 for the client associated with the processed e-mail. The anti-virus filter 123 operates in accordance with parameters retrieved from the anti-virus options 65, and sends infected e-mails to the infected e-mails quarantine 69 for the client associated with the processed e-mail.

Figure 7 shows a schematic functional overview of the anti-spam filter 121, together with the anti-spam options 63 and the generic filter rules 43. As shown, a received e-mail is initially processed by a Black List filter 131 which checks if the sender of the received e-mail is on the client Black List 81 for the client associated with the received e-mail. If the sender is on the client Black List 81, then the received e-mail is deleted, schematically represented in Figure 7 by being sent to a deleted e-mails bin 133. If the sender of the received e-mail is not on the client Black List 81, then the received e-mail is processed by a White List filter 135 which checks if the sender of the received e-mail is on the client White List 83 for the client associated with the received e-mail. If the sender is on the client White List 83, then the received e-mail is directly output by the anti-spam filter 121 to the anti-virus filter 123. If, however, the sender is not on the client White List 83, then the received e-mail is processed by a content-based filter 137.

In this embodiment, the content-based filter 137 applies the SpamAssassin computer program, which applies the client filter rules 85 and the generic filter rules 43 to the received e-mail to generate a spam score. The spam score is input to a comparator 141 which compares

the spam score with the quarantine threshold 87. The output of the comparator 141 forms a control signal for a switch 139 which is arranged so that if the spam score is less than the quarantine threshold 87, the switch 139 causes the anti-spam filter 121 to output the received e-mail to the anti-virus filter 123. If, however, the spam score is greater than the quarantine threshold 87, then the control signal output by the comparator 141 causes the switch 139 to direct the received e-mail to the client spam quarantine 67.

The operations performed by the mail filtering station 1 to process a received e-mail, and the operations performed by the client administrator computer 7 and the mail filtering station 1 to adjust the quarantine threshold and the drop threshold and to process e-mails stored in the spam quarantine 67 will now be discussed in more detail.

The processing of received e-mails

Figures 8A and 8B show a flow chart illustrating the main operations performed by the mail filtering station 1 to process a received e-mail. As shown, after receiving, at S1, an e-mail, the mail filtering station 1 checks, at S3, if the addressee hostname for the received e-mail is known (i.e. if the hostname corresponds to one of the clients stored in the client database). If the addressee hostname for the received e-mail is not known, then the mail filtering station 1 checks, at S4, if the sender hostname is known. If neither the sender hostname nor the addressee hostname is known, the mail filtering station 1 sends, at S5, an unknown address signal to the sender of the received e-mail. If the one of the

addressee hostname and the sender hostname of the received e-mail is known, then the mail filtering station 1 checks, at S7, if the corresponding client account is active. If the client account is not active, then the received e-mail is forwarded, at S9, to the addressee without anti-spam filtering or anti-virus filtering.

If the client account is active, then the mail filtering station 1 checks, at S11, if the sender of the received e-mail is on the client Black List for the client associated with the received e-mail. If the sender is on the client Black List, then the mail filtering station 1 deletes, at S13, the received e-mail. If the sender is not on the client Black List, then the mail filtering station 1 checks, at S15, if the sender of the received e-mail is on the client White List for the client associated with the received e-mail.

If the sender of the received e-mail is not on the client White List, then the mail filtering station 1 calculates, at S17, a spam score for the received e-mail and checks, at S19, if the calculated spam score is greater than the quarantine threshold stored in the client database 41 for the client associated with the received e-mail. If the spam score is greater than the quarantine threshold, then the mail filtering station 1 stores, at S21, the received e-mail in the spam quarantine 67 for the client and updates the index of the spam quarantine with header information from the received e-mail and the calculated spam score.

If the sender of the received e-mail is on the client White List for the addressee, or if the spam score is less than the quarantine threshold for the client,

then the mail filtering station 1 checks, at S23, if the e-mail is virus infected. If the e-mail is virus infected, then the mail filtering station 1 stores, at S25, the received e-mail in the infected e-mails quarantine 69 for the client. If no virus infection is found, then the mail filtering station 1 forwards, at S27, the received e-mail to the addressee.

The adjusting of the quarantine threshold and the drop threshold

Figure 9 shows a flow chart illustrating operations performed by both the client administrator computer 9 and the mail filtering station 1 to adjust the quarantine threshold and the drop threshold.

After receiving, at S31, a request from the client administrator for the quarantine configuration web page, the request being input using a conventional web browser program, the client administrator computer 9 transmits, at S33, a request for the quarantine configuration web page to the mail filtering station 1. After receiving, at S35, the request for the quarantine configuration web page, the mail filtering station 1 transmits, at S37, the quarantine configuration web page data, which is generated using a web page template stored in the web page templates data 45 and parameters stored in the anti-spam options 63 and the configuration data 71, to the client administrator computer 9.

After receiving, at S39, the quarantine configuration web page data, the client administrator computer 9 displays, at S41, the quarantine configuration web page to the client administrator. As shown in Figure 10, the displayed quarantine configuration web page

includes a configure quarantine form 151 having a common settings region 153, a virus specific region 155 and a spam specific region 157. In the common settings region 153, an edit box 159 displays the value for the number of header lines which are to be sent in a preview of a stored e-mail. Three edit boxes 161,163 and 165 in the virus specific region respectively display the memory size of the virus-infected e-mails quarantine, the number of days an e-mail is to be kept in the virus-infected e-mails quarantine and the number of messages which can be stored within the virus-infected e-mails quarantine. Five edit boxes 167,169,171,173,175 in the spam specific region 157 respectively display the memory size of the spam quarantine 67, the maximum number of days for which an e-mail is to be stored in the spam quarantine 67, the maximum number of e-mails to be stored in the spam quarantine 67, the drop score and the quarantine score. The edit boxes allow the client administrator to insert new parameters, including a new drop threshold and a new quarantine threshold.

The configure quarantine form 151 also includes a save button 177 and a reset button 179. After entering new values in the edit boxes, the client administrator "clicks" the save button 177 (by moving a cursor over the save button 177 using a mouse and then pressing a mouse button) to initiate the sending of the new parameters to the mail filtering station 1. The reset button 179 enables the client administrator to recover the parameter values currently stored at the mail filtering station 1.

After receiving, at S43, user instructions from the client administrator identifying new threshold

parameters, the client administrator computer 9 transmits, at S45, the new threshold parameters to the mail filtering station 1. After receiving, at S47, the new threshold parameters, the mail filtering station 1 updates, at S49, the drop score and the quarantine score stored in the client database.

The processing of the spam quarantine

The e-mails stored in the spam quarantine 67 are processed either by the client administrator or automatically by the mail filtering station 1. Figure 11 shows a flow chart illustrating both the operations performed by the client administrator computer 9 and the operations performed by the mail filtering station 1 when the client administrator processes the spam quarantine 67.

As shown, after receiving, at S61, a request by the client administrator to download the spam quarantine web page, the client administrator computer 9 transmits, at S63, the request for the spam quarantine web page to the mail filtering station 1. After receiving, at S65, the request for the spam quarantine web page, the mail filtering station 1 generates, at S67, spam quarantine web page data using one of the templates stored in the web page templates data 45 and information stored in the client database 41, and transmits, at S69, the spam quarantine web page data to the client administrator computer 9.

After receiving, at S71, the spam quarantine web page data, the client administrator computer 9 displays, at S73, the spam quarantine web page to the client administrator. As shown in Figure 12, the spam

quarantine web page includes a form 191 listing index data for the e-mails stored in the spam quarantine 67. For each of the e-mails in the spam quarantine 67, the form 191 shows the time and date of receipt, the addressee, the sender, the subject heading, the size and the spam score. Further the index data for e-mails having a spam score between the quarantine threshold and the drop threshold (which are five and ten respectively for this example) are highlighted.

The form 191 also includes check boxes 193a to 193i and hyper-text links 195a to 195 j, with one check box 193 and one hyper-text link 195 being associated with each stored e-mail. In order to delete a stored e-mail, the client administrator "checks" the corresponding check box 193 and "clicks" a delete button 193. In order to forward one of the stored e-mails, the client administrator checks the corresponding check box 193 and clicks a forward button 199. If the client administrator wishes to obtain more information concerning a stored e-mail, then the client administrator clicks on the corresponding hyper-text link 195 which causes further information concerning the e-mail, including a preview of a number of lines of the e-mail, to be sent to the client administrator computer 9. A reset button 201 is also provided which enables the client administrator to remove checks inserted in the check boxes 193.

After receiving, at S75, instructions from the client administrator for dealing with the quarantined e-mails, the client administrator computer 9 transmits, at S77, the instructions to the mail filtering station 1. After receiving, at S79, the client administrator

instructions, the mail filtering station 1 processes, at S81, the quarantined e-mail in accordance with the client administrator instructions.

Figure 13 shows in more detail the operations performed by the mail filtering station 1 to process the quarantined e-mails in accordance with the client administrator instructions. In this embodiment, the mail filtering station 1 initially deletes, at S91, e-mails identified for deletion by the client administrator. The mail filtering station 1 then adds, at S93, the senders of any e-mails identified for forwarding by the client administrator to the client White List so that in future e-mails from those senders are directly forwarded to the client mail server 5 by the mail filtering station 1. The mail filtering station 1 then checks, at S95, the e-mails identified by the client administrator for forwarding for viruses. If a virus is found, the mail filtering station 1 stores, at S97, the virus infected e-mail in the infected e-mails quarantine. Otherwise, the mail filtering station 1 transmits, at S99, the e-mails which pass the virus check to the client mail server 5.

Figure 14 is a flow chart showing the main operations performed by the mail filtering station 1 when automatically processing e-mails stored in the spam quarantine 67. This automatic processing is initiated on a periodic basis in accordance with time and date signals from the clock 35. Initially, the mail filtering station 1 retrieves, at Sill, the index data for the first e-mail stored in the spam quarantine 67. The mail filtering station 1 then checks, at S113, if the spam score of the retrieved e-mail index data is less than the drop

threshold. If the spam score is less than the drop threshold, the mail filtering station 1 checks, at S115, if the e-mail is older than the maximum age set in the configuration data 71, and if the e-mail is not older than the maximum age the mail filtering station 1 leaves, at S119, the e-mail in the spam quarantine 67. If the e-mail is older than the maximum age, the mail filtering station 1 deletes, at S121, the e-mail. If, at S113, the spam score is more than the drop threshold, the mail filtering station 1 checks, at S117, if the e-mail is more than two days old. If the e-mail is not more than two days old then the mail filtering station 1 leaves, at S119, the e-mail in the spam quarantine 67. If the e-mail is more than two days old then the mail filtering station 1 deletes, at S121, the e-mail.

The mail filtering station 1 then checks, at S123, for index data for any more e-mails. If there is more index data, then the mail filtering station 1 retrieves, at S125, the index data for the next e-mail and repeats the index data processing operations for the newly-retrieved index data. If there is no more index data, then the mail filtering station 1 ends, at S127, the automatic processing of the spam quarantine 67.

SECOND EMBODIMENT

In the first embodiment, the content-based filtering applied by the mail filtering module applies a set of tests to a received e-mail to derive a spam score. A second embodiment will now be described with reference to Figures 15 to 22 in which the mail filtering module applies Bayesian filtering to received e-mails. In Figures 15 to 22, components which are identical to

corresponding components in the first embodiment have been referenced by the same numerals and will not be described in detail again.

A Bayesian filter separates an e-mail into a plurality of components, commonly referred to as tokens, and for each token either retrieves a previously generated coefficient indicative of the likelihood of an e-mail including the token being a spam e-mail, or assigns a new co-efficient. The coefficients are calculated by a learning process in which a large number of spam e-mail messages and a large number of non-spam e-mail messages are separated into tokens, and the rate at which each token occurs in the spam e-mail messages and the non-spam e-mail messages is analysed to derive a coefficient which is indicative of the probability of an e-mail including the token being a spam e-mail. Further details of Bayesian filtering can be found in the article "A Plan for Spam" by Paul Graham whose content is incorporated herein by reference, and which is available at http://www.paulgraham.com/spam.html.

As the content of wanted e-mail messages tends to vary between individual users, in this embodiment the Bayesian filter coefficients are determined on a user by user basis. Further, in this embodiment each individual user of the client is able to set personalised anti-spam options including a Black List, a White List, a quarantine threshold and a drop threshold. Each user of the client also has a dedicated spam quarantine, and is able to process e-mails stored in the spam quarantine.

The e-mail delivery system of the second embodiment differs from the e-mail delivery system of the first

embodiment only in the program code stored in the code memory (and the functionality associated with the program code) and in the client database stored in the data memory of the mail filtering station. As shown in Figure 15, the code memory 211 stores: a control module 213 which controls the overall operation of the mail filtering station; a mail filtering module 215 which processes received e-mails to check for spam e-mails and virus-infected e-mails; a web page generating module 217 which generates web page data which provides a user interface via which users and the client administrator send instructions for dealing with stored e-mails and for adjusting parameters which determine how received e-mails are processed; and a Bayesian filter coefficients adjusting module 219 which adjusts coefficients used in the Bayesian filter in response to e-mails passing through the mail filtering station.

The client database is modified to include details associated with individual users of the client hostname. As shown in Figure 16, which shows the data 231 stored for a single client within the client database, the client data 231 stores sets of user data 233a to 233c in addition to the data stored in the client database of the first embodiment. As shown in Figure 17, each set of user data 233 is configured to store the corresponding username 241, a user password 243, a user e-mail address 245, a user Black List 247, a user White List 249, user content filter rules 251, a user drop threshold 253, a user quarantine threshold 255 and a user spam quarantine 257. In this embodiment, the user content filter rules 251 stores a set of Bayesian filter coefficients associated with the corresponding username.

Figure 5 shows a schematic functional overview of the mail filtering station of the second embodiment, in which operations performed by code in the code memory 211 are represented by functional blocks.

In the same manner as the first embodiment, data is transferred between the communications network interface 19 and a controller 271 via a HTTP codec 101 and a SMTP codec 103. The operator interface 37, the clock 35, the e-mail cache memory 47 and the generic filter rules 43 are also connected to the controller 271 in the same manner as the first embodiment.

The controller 271 sends received e-mails to a mail filter 273, which processes the received e-mails to check for spam e-mails and for virus-infected e-mails. In this embodiment the mail filter 273 is functionally equivalent to the mail filter of the first embodiment except that the content-based filter comprises a Bayesian filter and that if the username of the received e-mail is recognised, then the anti-spam options associated with the username are retrieved from the client database 275 and employed by the mail filter 273.

The controller 271 is also able to instruct a web page generator 277 to generate web page data using a web page template stored in the web page templates data memory 279. For some web pages, the web page generator 277 incorporates data retrieved from the client database 275 in the web page template to form the web page data.

The controller 271 is also able to send a received e-mail together with a current set of Bayesian filter coefficients for the addressee of the e-mail, which are retrieved from the client database 275, to a Bayesian

filter coefficients adjuster 281 which adjusts the Bayesian filter coefficients in dependence on the content of the received e-mail. The adjusted Bayesian filter coefficients are sent back to the controller 271 which stores the adjusted coefficients in the client database 275 in place of the previous Bayesian coefficients. In this way, slow variations in the content of spam e-mails and non-spam e-mails for the addressee can be compensated for by adjusting the stored Bayesian filter coefficients.

The operations performed by the mail filtering station to process a received e-mail, and the operations performed by the mail filtering station and a client computer to process e-mails stored in the spam quarantine will now be discussed in more detail.

The processing of received e-mails.

Figure 19A and 19B show a flow chart illustrating the main operations performed by the mail filtering station to process a received e-mail. As shown, after receiving, at S151, an e-mail, the mail filtering station checks, at S153, if the addressee hostname for the received e-mail is known. If the addressee hostname for the received e-mail is not known, then the mail filtering station sends, at S155, an unknown address signal to the sender of the received e-mail. If the addressee hostname of the received e-mail is known, then the mail filtering station checks, at S157, if the corresponding client account is active. If the client account is not active, then the received e-mail is forwarded, at S159, to the addressee without anti-spam filtering or anti-virus filtering.

If the client account for the addressee is active,

then the mail filtering station checks, at S161, if the username is known. If the username is known, then the mail filtering station retrieves, at S163, the corresponding user anti-spam options, otherwise the mail filtering station retrieves, at S165, the client anti-spam options.

The mail filtering station then checks, at S167, if the sender of the received e-mail is on the Black List included within the retrieved anti-spam options. If the sender is on the Black List, then the mail filtering station deletes, at S169, the received e-mail. If the sender is not on the client Black List, then the mail filtering station checks, at S171, if the sender of the received e-mail is on the White List included within the retrieved anti-spam options.

If the sender of the received e-mail is not on the White List, then the mail filtering station calculates, at S173, a spam score for the received e-mail utilising Bayesian filtering. The mail filtering station then checks, at S175, if the calculated spam score is greater than the quarantine threshold included within retrieved anti-spam options. If the spam score is greater than the quarantine threshold, then the mail filtering station stores, at S177, the received e-mail in the spam quarantine for the addressee and updates the index of the spam quarantine with header information from the received e-mail and the calculated spam score.

If the sender of the received e-mail is on the retrieved White List of if the spam score is less than the quarantine threshold, then the mail filtering station checks, at S177, if the e-mail is virus-infected. If the

e-mail is virus-infected, then the mail filtering station stores, at S179, the received e-mail in the infected e-mails quarantine. If no virus infection is found, then the mail filtering station adjusts, at S181, the Bayesian filter coefficients to take account of the content of the received e-mail, and then forwards, at S183, the received e-mail to the addressee.

The adjustment of the Bayesian filter coefficients will now be described in more detail with reference to Figure 20. As shown, the mail filtering station separates, at S191, the received e-mail into tokens and then counts, at S193 the number of times each token appears in the e-mail. The mail filtering station then retrieves, at S195, the previous coefficient for each token and adjusts, at S197, the previous coefficient in accordance with the number of times the token appears in the received e-mail.

The processing of the spam quarantine

In this embodiment, the mail filtering station prompts a user to give instructions for dealing with e-mails stored in the associated user spam quarantine 257 by sending an e-mail conveying an HTML page listing the index data for the e-mail stored in the user spam quarantine 257. Figure 22 shows a flow chart illustrating both the operations performed by the user computer of the user and the operations performed by the mail filtering station when the user processes the spam quarantine 257.

The processing of the spam quarantine is initiated on a periodic basis in response to time and date signals received from the clock 35 of the mail filtering station.

The mail filtering station then generates, at S211, spam quarantine web page data using one of the templates stored in the web page templates data 279 and the index of documents stored in the spam quarantine 257 of the user provided in the client database. The mail filtering station then transmits, at S213, the spam quarantine web page data to the user e-mail address provided in the set of user data 233 for the user.

The HTML e-mail is received, at S215, by the user computer of the user and in response to receiving, at S217, an instruction from the user to open the spam quarantine e-mail, the user computer displays, at S219, the quarantine web page to the user. In this embodiment, the quarantine web page includes a form which is identical to the form illustrated in Figure 12, and which enables the user to indicate how to deal with the e-mails in the user spam quarantine 257. On receiving, at S221, the user instructions for dealing with the quarantined e-mails, the user computer transmits, at S223, the user instructions to the mail filtering station in accordance with the HTTP protocol.

After receiving, at S225, the user instructions, the mail filtering station processes, at S221, the quarantined e-mails using the received user instructions.

Figure 22 shows in more detail the steps performed by the mail filtering station to process the quarantined e-mails using the received user instructions. As shown, the mail filtering station first deletes, at S231, e-mails which have been identified for deletion by the user. The mail filtering station then adds, at S233, the senders of e-mails identified for forwarding to the White

List for the user so that in future e-mails from those senders are directly forwarded to the user. The mail filtering station then checks, at S235, the e-mails identified for forwarding for viruses and stores, at S237, the e-mails in which viruses are found in the infected e-mails quarantine. The mail filtering station then adjusts, at S239, the Bayesian filter coefficients in the same manner as described with reference to Figure 20 using the virus-free e-mails. Finally, the mail filtering station transmits, at S241, the virus-free e-mails to the user.

Adjusting user anti-spam options

In this embodiment, when a user is first added to the list of users for a client, the mail filtering station sends to the user e-mail address an HTML e-mail incorporating the form illustrated in Figure 10 for the first embodiment. The user is then able to set initial anti-spam options and configuration options by opening the HTML e-mail, entering the desired parameters in the appropriate edit boxes, and clicking the save button 177. After having established the initial settings, the user is subsequently able to alter the settings by accessing the configure quarantine web page using a conventional web browser.

THIRD EMBODIMENT

In the first and second embodiments, the mail filtering station checks if e-mails are virus-infected or likely to be spam e-mails, and temporarily stores those e-mails which fail these checks. A third embodiment of the invention will now be described with reference to Figures 23 to 27 in which a mail filtering station also

generates archive data for all e-mails sent by and sent to a client, and periodically sends the archive data to the client administrator computer for local storage. In Figures 23 to 27, components which are identical to corresponding components of the first embodiment have been referenced with the same numerals and will not be described in detail again.

As shown in Figure 23, the mail filtering station 301 differs from the mail filtering station of the first embodiment in that in addition to the mail filtering module 29 and the web page generating module 31, the code memory 303 includes an archiving module 305 and a control module 307 which is modified to take into account the addition of the archiving module 305. Further, the data memory 309 of the mail filtering station 301 of the third embodiment includes an e-mails archive 311 in addition to the client database 41, the generic filter rules 43, the web pages templates data 45 and the e-mail cache memory 47.

As shown in Figure 24, the e-mails archive 311 includes client archives 32 la to 32Ic for a plurality of clients who utilise the mail filtering station 301. As shown in Figure 25, each client archive 321 includes an index 331 storing bibliographic details for each of the e-mails stored in the client archive, together with a copy of each stored e-mail 333a to 333c.

Figure 26 shows a schematic functional overview of the mail filtering station 301. As shown, in this embodiment the controller 341 is connected to an archiver 343 (representing the functionality of the archiving module 305) which is in turn connected to the e-mails

archive. In this embodiment, before forwarding an e-mail sent to the client or sent by the client, the controller 341 sends the e-mail to the archiver 343 which updates the e-mails archive 311. Further, the controller 341 periodically sends a control signal to the archiver 343 to recover a client archive 321 from the e-mails archive 311, and the controller 341 then sends an e-mail including the recovered client archive 321 to the client administrator.

Figure 27 shows a schematic functional overview of the archiver 343. E-mails received from the controller 341 are input to an e-mail copier 351 which copies the e-mail and sends the original e-mail back to the controller 341 for forwarding to the addressee. The copied e-mail is output by the e-mail copier 351 to an index information extractor 353 which extracts index information for the e-mail. In this embodiment, the index information includes the time of sending, the identity of the sender, the identity of the addressee, the subject line from the header and the total size of the e-mail. The extracted index information is input to an index adjuster 355, which is also connected to an e-mails archive manager 357.

The e-mails archive manager 357 controls the storing and retrieval of data within the e-mails archive 345. On receiving extracted index information, the index adjuster 355 sends a control signal to the e-mails archive manager 357 causing the e-mails archive manager 357 to extract the index 331 from the appropriate client archive 321. The extracted index 331 is input to the index adjuster 355, which modifies the index 331 to

include the details of the new e-mail. The index adjuster 355 then sends the modified index back to the e-mails archive manager 357, which stores the modified index 331 in the appropriate client archive 321. The copied e-mail is output by the index information extractor 353 to a data compressor 359 which compresses the copied e-mail using a conventional data compression technique. The data compressor 359 outputs the compressed e-mail to an encrypter 361 which encrypts the compressed e-mail using a conventional encryption technique. The encrypter 361 sends the encrypted e-mail to the e-mails archive manager 357, which adds the encrypted e-mail to the appropriate client archive 321 within the e-mails archive 311.

When the controller 341 sends a request for a client archive 321, the request is sent directly to the e-mails archive manager 357, which retrieves the requested client archive 321 from the e-mails archive 311, and sends the retrieved client archive 321 to the controller 341.

As described above, in this embodiment the mail filtering station 301 periodically sends archive data to a client giving an index of all e-mails sent to that client and by that client over a period, together with encrypted and compressed copies of the e-mails. Sending archived data in this way facilitates the generation of a local archive of all e-mails sent to and by the client. Such a local archive is useful in situations where the client wishes to refer to an e-mail the original of which has been previously deleted.

FOURTH EMBODIMENT

In the third embodiment, the mail filtering station

301 periodically sends archive data to a client administrator for local storage. A fourth embodiment will now be described with reference to Figures 28 to 33 in which an archive of all e-mails sent by and to a client is stored on-line, rather than being stored locally by the client. In this way, the amount of local memory required by the client is reduced. In Figures 28 to 33, components which are identical to corresponding to components of the third embodiment have been referenced with the same numerals and will not be described in detail again.

Figure 28 schematically shows the main components of the fourth embodiment of an e-mail delivery system according to the invention, in which e-mails to and from a client computer 7 are delivered via a mail filtering station 401. As shown, in this embodiment an on-line e-mails archive 403 is also connected to the communications network 13. In the same manner as in the third embodiment, the mail filtering station 401 stores archive data for all e-mails sent to the client and by the client. In this embodiment, however, the stored archive data is periodically sent to the on-line e-mails archive 403 instead of to the client administrator computer 9.

The only difference between the mail filtering station 401 of this embodiment and the mail filtering station 301 of the third embodiment, is that the control module of the mail filtering station 401 is modified to send archive data from the e-mails archive 311 to the on-line e-mails archive 403 on a periodic basis using the FTP protocol. Figure 29 shows a schematic functional overview of the mail filtering station 401. As shown, the

controller 403 the mail filtering station 401 is connected to the communications network interface 19 via a FTP codec 407 in addition to the HTTP codec 101 and the SMTP codec 103. The controller 405 periodically sends a control signal to the archiver 343 to retrieve a client archive 321 from the e-mails archive 311, and the controller 405 sends the retrieved client archive to the on-line e-mails archive 403 by outputting the archive to the communications network interface 19 via the FTP codec 407.

Figure 30 shows the main components of the on-line e-mails archive 403. As shown, the on-line e-mails archive 403 includes a communications network interface 411 which receives signals from the communications network 13 and transmits signals via the communications network 13. The communications network interface 411 is connected to a processor 413 which processes received signals in accordance with program code stored in a code memory 415 which is also connected to the processor 413. A data memory 417 and an operator interface 419 are also connected to the processor 413. The operator interface 419 enables the program code stored in the code memory 415 or the data stored in the data memory 417 to be modified by an operator of the on-line e-mails archive 403. The operator interface 419 includes a reader (not shown in Figure 30) which enables program code or data to be downloaded from a floppy disk 421.

The data memory 417 includes a client database 423 storing details for a plurality of clients who utilize the on-line e-mails archive 403, an e-mails archive 425 which stores archive data for each of the clients and web

page templates data 427 which are used to form web pages which provide a user interface with the client. The code memory 415 stores a control module 429 which controls the overall operation of the on-line e-mails archive 403, an archiving module 431 which controls the storage of data in and the retrieval of data from the e-mails archive 425, and a web page generating module 433 which generates web page data using the web page templates data 427 stored in the data memory 417.

Figure 31 schematically shows the contents of the client database 423. As shown, the client database 423 shows a plurality of sets of client data 44 la to 44 Ic, with each set of client data 441 corresponding to a different client. As shown for one set of client data 44 la in Figure 31, each set of client data includes the client hostname 443, a client password 445 and an archive location index 447 indicating where in the e-mails archive 425 the archive data for that client is stored. In particular, in this embodiment the archive location index 447 stores the location of each set of archive data received from the mail filtering station 401.

Figure 32 shows a schematic functional overview of the on-line e-mails archive 403, in which operations performed by program code in the code memory 415 are represented by functional blocks. As shown, a controller 451 is connected to the communications network interface 411 via an HTTP codec 453 and an FTP codec 457.

On receiving an FTP communication enclosing archive data from the mail filtering station 401 via the communications network interface 411, the FTP communication is input to the FTP codec 457 which

recovers the archive data and outputs the recovered archive data to the controller 451. The controller 451 then sends the archive data to an archiver 459 which stores the received archive data in the e-mails archive 425. The archiver 459 sends archive location data to the controller 451 indicating where in the e-mails archive 425 the newly received archive data is stored. The controller 451 then updates the archive location index 447 in the appropriate client data 441 of the client database 423 to include the location of the newly stored archive data.

In this embodiment, a client administrator accesses data stored in the e-mails archive 425 of the on-line e-mails archive 403 by using a conventional web browser program as the user interface. When the on-line e-mails archive 403 receives, via the communications network interface 411, a request from a client administrator to download web page data, the request is directed to the controller 451 via the HTTP codec 453. Initially, the controller 451 instructs the web page generator 461 to generate a login web page using an appropriate template stored in the web page templates data 427, and then sends, via the HTTP codec 453 and the communications network interface 411, the login web page data to the client administrator. The login web page data is displayed at the client administrator computer 9 as a web page including edit boxes allowing the client administrator to enter the associated hostname and password, and to send the entered hostname and password data to the on-line e-mails archive 403.

After receiving the hostname and password data, the

controller 451 verifies that the hostname matches the hostname 443 stored in one of the sets of client data 441 stored in the client database 423, and that the received password matches the corresponding password 445 stored in the client data 441. If the hostname and password are verified, the controller 451 instructs the web page generator 461 to generate web page data showing an index of the stored sets of archive data for the client together with a check box for each set of archive data. The controller 451 then sends, via the HTTP codec 453 and the communications network interface 411, the web page data to the client administrator.

On receiving the web page data, the client administrator computer 9 displays the corresponding web page to the client administrator. The client administrator is able to select a set of archive data by checking the corresponding check box, and a control signal identifying the selected set of archive data is sent by the client administrator computer 9 to the on-line e-mails archive 403. The controller 451 of the on-line e-mails archive 403 then retrieves the index data of the selected set of archive data from the e-mails archive 425, and sends web page data conveying the retrieved index data to the client administrator computer 9. The client administrator 9 then displays the web page so that the client administrator is able to select one or more of the e-mails of the set of archive data. On receiving a signal identifying the selected e-mails, the controller 451 of the on-line e-mails archive 403 retrieves the selected e-mails from the e-mails archive 425 and sends a web page conveying the selected e-mails to the client administrator computer 9.

Figure 33 schematically shows the main functional components of the archiver 459. As shown, an e-mails archiver manager 471 controls the storing of data in, and the retrieval of data from, the e-mails archive 425. The e-mails archive manager 471 has a direct connection to the controller 451. The e-mails archive manager 471 stores sets of archive data received from the controller 451 in the e-mails archive 425, and is also able to output index data for stored sets of archive data to the controller 451. The e-mails archive manager 471 is also able to output e-mails stored in the e-mails archive 425 to the controller 451 via a decrypter 473, which decrypts the stored e-mail, and a data decompressor 475 which decompresses the stored e-mail.

FIFTH EMBODIMENT

In the second embodiment, a mail filtering station is used in which each individual user has an associated White List. A fifth embodiment will now be described with reference to Figures 34 to 36 in which an e-mail address book which has been compiled by the e-mail program of a user is processed at the user computer to generate White List data which is forwarded to the mail filtering station for inclusion within the White List for the user. This is particularly advantageous when a user first commences use of the mail filtering station because the user is able to establish more quickly an initial White List.

Figure 34 shows the main components of a user computer 501 in this embodiment. As shown, the user computer 501 has a communications network interface 503 for receiving signals 505 from, and transmitting signals

505 to, a communications network. The communications network interface 503 is connected to a processor 505 which implements program code stored in a code memory 507. The processor 505 is also connected to a data memory 509 and a user interface 511. The user interface includes a reader (not shown) for reading data from a computer disk 513 for storage in either the code memory 507 or the data memory 509.

As shown, the code memory 507 includes, among other programs, a conventional operating system 515, a conventional web browser module 517, and a conventional e-mail module 519 which has an associated e-mail address book 521 which is stored, along with other files, in the data memory 509. The code memory 507 also stores a White List generating module 523 which processes the address information stored in the e-mail address book 521 to generate White List information for transmission to a mail filtering station via the communications network. The White List generating module 523 can be provided in the code memory 507 either by downloading a signal 505 conveying the White List generating module from the computer network or by downloading the White List generating module from the computer disk 513.

Figure 35 shows the main operations performed by the White List generating module 523. In response to the user initiating execution of the White List generating module 523, the user computer 501 initially searches, at S301, for address book files stored in the data memory 509. In particular, in this embodiment the user is asked to specify a directory location of the data memory 509 to be searched for address book files, and then the

specified directory location of the data memory 509 is searched for *.csv, *.doc, *.xls and *.txt files. The user computer 501 then retrieves, at S303, e-mail address information from the identified address book files. In this embodiment, the processor 505 identifies both e-mail address information and domain information contained within the identified address book files. The computer then displays, at S305, the retrieved e-mail address information to the user.

Figure 36 schematically shows the format of the e-mail address information displayed to the user. The e-mail address information includes an addresses list 531 and a domains list 533. As shown, the addresses list 531 includes a list of e-mail addresses, with each e-mail address having an associated check box 535a, 535b and an associated hyperlink 537a, 537b. Similarly, the domains list 533 includes a list of domains with each domain having an associated check box 535c to 535e and an associated hyperlink 537c to 537e. In order to add one of the addresses from the address list onto the White List, the user checks the corresponding check box 535 and clicks on the corresponding hypertext link 537. Similarly, in order to add one of the domains to the White List, the user checks the corresponding check box 535 and then clicks on the corresponding hypertext link 537.

After receiving, at S307, user instructions identifying an e-mail address or a domain for inclusion in the White List, the computer 501 transmits, at S309, the user instruction to the mail filtering station via the communications network.

The White List generating module 523 described above has the advantage that e-mail addresses stored in the e-mail address book 521 are not automatically added to the White List at the mail filtering station, but rather the user is able to select which of the e-mail addresses is to be added. In this way, if the user had previously received spam e-mails and the senders of the spam e-mails have been incorporated within the e-mail address book 521, then the senders of the spam e-mails are not automatically added to the White List at the mail filtering station.

MODIFICATIONS AND FURTHER EMBODIMENTS

In the first embodiment, the spam score for a received electronic message is compared with two threshold values and in dependence upon the relationship between the spam score and the two threshold values the received electronic message is processed in one of three different ways. This additional flexibility allows for greater control of how an e-mail is processed in dependence upon the likelihood of the e-mail being a spam e-mail. In order to increase further the different ways in which a received e-mail may be handled, additional threshold values could be used.

In the first embodiment, the spam score is generated by a content-based filter which is used in conjunction with a White List filter and a Black List filter. It will be appreciated that the White List filter and the Black List filter are not required to achieve the advantages associated with using multiple threshold values to determine how e-mail processed by the content-based filter are handled by the mail filtering station.

In the first embodiment, if a received e-mail has a spam score which is below a quarantine threshold, then the received e-mail is forwarded to the addressee. Otherwise, the received e-mail is stored for a period of time which is determined by the relationship between the spam score and a drop threshold. In particular, if the spam score is between the quarantine threshold and the drop threshold, then the received e-mail is stored for a maximum number of days set by the user using the Configure Quarantine web page, whereas if the spam score of the received e-mail is above the drop threshold then the received e-mail is only stored for two days. In an alternative embodiment, the Configure Quarantine web page includes an additional edit box via which a user is able to set the amount of time for which a received e-mail having a spam score above the drop threshold is stored (e.g. 0,24,48,72,96 hours). In another alternative embodiment, if the spam score for a received e-mail is above the drop threshold, then the received e-mail is immediately deleted.

In the first embodiment, the spam score is a positive number having a magnitude which is indicative of the likelihood of the e-mail being a spam e-mail. In particular, the larger the value of the spam score, the greater the probability that the e-mail is a spam e-mail. It will be appreciated that alternatively, the content-based filter could be modified so that the smaller the spam score the larger the possibility that the e-mail is a spam e-mail with the processing in response to the relationship between the spam score and threshold values being modified accordingly.

In the first and second embodiments, the filtering station is provided at a separate connection to the communications network from the mail server of the addressee. In an alternative embodiment, the functionality of the filtering station is incorporated within the client mail server. It will be appreciated that the client mail server may be a mail server operated by the internet service provider for the client, or alternatively may be a mail server operated by a company providing a web-based mail service.

In the first embodiment, when an instruction is received to forward an e-mail stored in the spam quarantine to the addressee, the sender of the e-mail is added to the White List so that future e-mails from that sender are directly forwarded by the mail filtering sation to the addressee. It will be appreciated that this auto-adding of senders to a White List can also be applied if the content-based filter compares a spam score with only a single threshold value in order to determine whether or not to store the e-mail in the spam quarantine. Further, this auto-adding of senders to a White List could also be applied in a mail filtering station which simply applies a White List filter, with e-mails from senders who are not on the White List being stored in a quarantine at the filtering station until instructions are received from the addressee indicating how to handle them.

In the second embodiment, the mail filtering station updates Bayesian filter co-efficients for an individual addressee using e-mails which are forwarded to the addressee. In this way, changes in the type of

content of e-mails wanted by the addressee over time are reflected by corresponding changes in the Bayesian filter co-efficients. Alternatively, a set of Bayesian filter co-efficients could be used for all addressees at a particular hostname, with the mail filtering station updating the Bayesian filter co-efficients used in all e-mails forwarded to the hostname. In another alternative embodiment, a single set of Bayesian filter co-efficients are used for all the clients of the mail filtering station, with the single set of Bayesian filter co-efficients being updated using all of the e-mails forwarded by the mail filtering station to the respective addresses.

In the second embodiment, the mail filtering station only updates the Bayesian filter co-efficients using e-mails which are forwarded to the addressee, i.e. e-mails which are unlikely to be spam e-mails. Alternatively, the mail filtering station could also update the Bayesian filter co-efficients by analysing e-mails which are not forwarded to the addressee, either due to having a spam score about the drop threshold or in response to instructions to delete the e-mail.

In the second embodiment, the mail filtering station generates and transmits an HTML e-mail to an individual addressee which incorporates an HTML interface enabling the addressee, on opening the HTML e-mail, to send instructions to the mail filtering station. These instructions could either be to change configuration data or anti-spam options, or instructions for handling e-mails stored in the spam quarantine. By sending HTML e-mails in this way, the mail filtering station both

prompts the addressee to provide instructions, and also facilitates in the providing of these instructions because the HTML e-mail itself provides the interface via which the addressee enters the instructions.

It will be appreciated that HTML e-mails are not the only type of e-mail which can provide an interface via which a user is able to input instructions for sending back to the mail filtering station. For example, a plain text e-mail could include one or more text fields in which a user can insert instructions. The user then replies to the received e-mail, thereby sending the instructions to the mail filtering station which scans the returned e-mail to extract the users instructions. In an embodiment, for ease of recovery each data field for entering instructions is delimited by a pair of symbols (e.g. a pair of square brackets).

In the illustrated embodiments, when a client views the list of e-mails quarantined in the respective client spam quarantine, the client only has the option to delete or forward the e-mails. If the e-mail is forwarded, then the sender of the forwarded e-mail is automatically added to the White List for the client. In an alternative embodiment, the client has a choice of four instructions, namely to delete the stored message, forward the stored message without adding the sender of the stored message to the White List, delete the stored message and add the sender of the stored message to the Black List, and to forward the stored message and to add the sender of the stored message to the White List. In this way, the control by the client of the content of the White List and the Black List is facilitated.

In the third and fourth embodiments, the filtering station includes an archiver which generates archive data of all e-mails forwarded by the filtering station to a hostname. It will be appreciated that the archiver need not be implemented within a filtering station, but could be implemented separately. In an alternative embodiment, the archiver is implemented within the mail server of the addressee.

In the fourth embodiment, a single on-line e-mails archive is connected to the communications network. In an alternative embodiment, the data storage used by the on-line e-mails archive is distributed throughout a plurality of servers connected to different points of the communications network. In particular, the plurality of servers includes a master server and a plurality of slave servers. In order to view archived e-mails, a signal is sent to the master server which determines the location of the stored e-mail using an index, and then retrieves the stored e-mail from the location, which may be on the master server or may be on one of the slave servers.

In the described embodiments, the client of the filtering station is a firm, and all e-mails directed to individuals at the firm are passed through the mail filtering station. As described in the second embodiment, anti-spam options used by the mail filtering station may be set by an individual user for the filtering of e-mails for the individual user. It would be appreciated that the client could therefore be an individual user, rather than a firm.

In another embodiment, instead of the client being a firm, the client is a family in which case the client

administrator may be a senior member of the family such as the father or mother. If the family includes children, then by having an arrangement in which only the client administrator can set the anti-spam options, as described in the first embodiment, then the senior member of the family is able to control which e-mails are received by the children within the family.

In an embodiment, separate anti-spam options are provided for each member of the family, with the senior member of the family being the only member allowed to alter the anti-spam options. Preferably, the senior member of the family sets the anti-spam options for the children within the family so that only e-mails whose senders appear on a White List, which is set by the senior of the family, are received by the children within the family. In this way, the possibility of pornographic e-mails being received by children within the family is very low.

Although the invention has been described with reference to the processing of e-mails, it will be appreciated that the invention could also be applied to other systems of sending electronic messages. For example, the invention could be applied to the processing of SMS messages sent in accordance with the GSM specification for cellular phone communications.

In the described embodiments, the code memory and the data memory are represented as separate components. It will be appreciated that the code memory and the data memory could, in fact, be separate parts of a common data storage device.

Although the embodiments of the invention described

with reference to the drawings comprise computer apparatus and processes performed in the computer apparatus, the invention also extends to computer programs, particularly computer programs on or in a carrier, adapted for putting the invention into practice. The program may be in the form of source code, object code, a code intermediate source and object code such as a impartially compiled form, or in any other form suitable for using the implementation of the processes according to the invention.

The carrier may be any entity of device capable of carrying the program. For example, the carrier may comprise a storage medium, such as a ROM, for example a CD-ROM or a semi-conductor ROM, or a magnetic recording medium, for example a floppy disk, or a hard disk. Further, the carrier may be a transmissible carrier such as an electronic or optical signal which may be conveyed via electrical or optical cable or by radio or other means.

When the program is embodied in a signal which may be conveyed directly by cable or other device or means, the carrier may be constituted by such cable or other device or means. Alternatively, the carrier may be an integrated circuit in which the program is embedded, the integrated circuit being adapted for performing, or for use in the performance of, the relevant processes.

Although in the described embodiments the invention is implemented by software, it will be appreciated that alternatively the invention could be implemented by hardware devices, or a combination of hardware devices and software.

Various aspects of the invention are now summarised in the following numbered clauses:

1. A method of routing electronic messages transmitted between network devices coupled to a communications network, the method comprising a routing apparatus:

copying a received electronic message;

forwarding the received electronic message to the addressee;

identifying an addressee of the received electronic message; and

storing a copy of the received electronic message in an electronic messages archive associated with the addressee.

2. A method according to clause 1, wherein said storing of a received electronic message comprises storing the electronic message in an electronic messages archive at the routing apparatus.

3. A method according to clause 1 or 2, wherein said storing of a received electronic message comprises the routing apparatus updating an index of electronic messages stored in the electronic messages archive associated with the addressee of the received electronic message.

4. A method according to any of clauses 1 to 3, wherein said storing of an electronic message comprises the routing apparatus compressing the electronic message and storing a compressed version of the electronic message.

5. A method according to any of clauses 1 to 4, wherein said storing of an electronic message comprises the routing apparatus encrypting the electronic message and storing an encrypted version of the electronic message.

6. A method according to any of clauses 1 to 5, further comprising the routing apparatus periodically transmitting the electronic messages archive to a remote network device.

7. A method according to clause 6, wherein each electronic messages archive is associated with a single addressee, and said transmitting of the electronic messages archive comprises transmitting the electronic messages archive to the associated addressee.

8. A method according to clause 6, wherein each electronic messages archive is associated with a group of addressees, and said transmitting of the electronic messages archive comprises transmitting the electronic messages archive to a predefined one of the group of addressees.

9. A method according to clause 8, wherein said transmitting of the electronic messages archive comprises transmitting the electronic messages archive to an archiving apparatus.

10. A method of generating an archive of electronic messages addressed to an addressee, the method comprising an archiving apparatus:

periodically receiving a set of archive data comprising a plurality of electronic messages and an electronic messages index of said plurality of electronic

messages; and

on receiving each set of archive data, storing the received set of archive data and updating an index of the plurality of sets of archive data accordingly.

11. A method according to clause 10, further comprising the archiving apparatus generating an interface for accessing an electronic message in one of the stored sets of archive data; and

outputting an electronic message identified via the interface.

12. A method according to clause 11, wherein the generating of an interface comprises generating web page data for a web page including the index of stored sets of archive data.

13. A method according to clause 12, wherein in response to an instruction input via the interface, the method further comprises generating web page data for a web page including the electronic messages index for the selected set of archive data.

14. A method of generating electronic message address information identifying approved senders of electronic messages for an addressee and of transmitting the generated electronic message address information to a remote filtering apparatus, the method comprising a network device associated with the addressee:

retrieving electronic message addresses from one or more data stores of the network device;

displaying the retrieved electronic message addresses to an operator of the network device;

receiving instructions identifying one or more of the retrieved electronic message addresses for addition to a list of approved senders; and

transmitting the or each identified electronic message address to a remote filtering apparatus.

15. A method according to clause 14, wherein said retrieving of electronic message addresses comprises the network device:

scanning the one or more data stores for an address book file; and

retrieving the electronic message addresses stored in the address book file.

16. A method according to clause 15, wherein said scanning of the one or more data stores for an address book file comprises scanning the file names of files stored in the address book file to identify files stored in one or more predetermined formats.

17. An electronic message router operable to route electronic messages transmitted between network devices coupled to a communications network, the electronic message router comprising:

a copier operable to generate a copy a received electronic message;

a transmitter operable to forward the received electronic message to the addressee;

an identifier operable to identify an addressee of the received electronic message; and

a data store configured to store a plurality of electronic messages archives, each electronic messages

archive being associated with one or more addressees,

wherein the electronic message routing apparatus is operable to store said copy of the received electronic message in the electronic messages archive associated with the addressee of the received electronic message.

18. An electronic message router according to clause 17, wherein each of said electronic messages archives is configured to store an index of electronic messages stored in that archive, and wherein the electronic message router further comprises an updater operable to update an index of electronic messages stored in the electronic messages archive associated with the addressee of the received electronic message.

19. An electronic message router according to clause 17 or 18, further comprising a data compressor operable to compress said copy of the received electronic message,

wherein the electronic message router is operable to store a compressed version of the copy of the received electronic message in the electronic messages archive.

20. An electronic message router according to any of clauses 17 to 19, further comprising an encrypter operable to encrypt said copy of the received electronic message,

wherein the electronic message router is operable to store an encrypted version of the copy of the received electronic message.

21. An electronic message router according to any of clauses 17 to 19, wherein said transmitter is operable to output the electronic messages archive periodically to

a remote network device.

22. An electronic message router according to clause 21, wherein each electronic message archive is associated with a single addressee, and said transmitter is operable to transmit the electronic messages archive to the associated addressee.

23. An electronic message router according to clause 21, wherein each electronic messages archive is associated with a group of addressees, and the transmitter is operable to transmit the electronic messages archive to a predefined one of the group of addressees.

24. An electronic message router according to clause 21, wherein the transmitter is operable to transmit the electronic messages archive to an archiving apparatus.

25. An archiving apparatus for storing a plurality of sets of archive data, each set of archive data comprising a plurality of electronic messages for an addressee and an electronic messages index of said plurality of electronic messages, the archiving apparatus comprising:

a network interface;

a data store configured to store a plurality of sets of archive data and an index of the stored sets of archive data; and

a controller operable to store a set of archive data received via the network interface in the data store, and to update an index of the plurality of sets of archive data accordingly.

26. An archiving apparatus according to clause 25, further comprising:

an interface generator operable to generate an interface for accessing an electronic message in one of the stored sets of archive data; and

a message retriever operable to retrieve an electronic message identified via the interface.

27. An archiving apparatus according to clause 26, wherein the interface generator comprises a web server operable to generate web page data for a web page including the index of stored sets of archive data.

28. An archiving apparatus according to clause 27, wherein the interface generator is operable, in response to a received instruction, to generate web page data for a web page including the electronic messages index for the selected set of archive data.

29. A network device comprising:

at least one data store configured to store data including electronic message addresses;

an electronic message address finder operable to search said at least one data store to retrieve stored electronic message addresses;

a controller operable i) to generate a control signal for an interface device conveying the retrieved electronic message addresses and ii) to receive instructions identifying one or more of the retrieved electronic mail addresses for addition to a list of approved senders; and

a transmitter operable to transmit the or each

identified electronic message address to a remote filtering apparatus.

30. A network device according to clause 29, wherein said electronic message addresses finder is operable i) to scan the one or more data stores for an address book file; and ii) to retrieve the electronic message addresses stored in the address book file.

31. A network device according to clause 30, wherein said electronic message address finder is operable to scan the file names of files stored in said one or more data stores to identify files stored in one or more predetermined formats.

CLAIMS

1. A method of filtering electronic messages transmitted over a communications network to an addressee, the method comprising a filtering apparatus:

analysing a received electronic message using predefined tests to derive a message score in dependence thereon; and

filtering the received electronic message in dependence upon the relationship between the message score and multiple threshold values.

2. A method according to claim 1, wherein the filtering of the received electronic message comprises the filtering apparatus deleting the received electronic message if the associated message score is within a range of values defined by one or more of the multiple threshold values.

3. A method according to claim 1, wherein the filtering of the received electronic message comprises the filtering apparatus storing the received electronic message if the associated message score is within a range of values defined by one or more of the multiple threshold values.

4. A method according to claim 1, wherein the multiple threshold values define a first range of values, a second range of values and a third range of values,

and wherein the method further comprises the filtering apparatus:

forwarding the received electronic message to the

addressee if said message score is within the first range of values;

storing the received electronic message until the earlier of the receipt of instructions for handling the received electronic message and the elapse of a first period of time if said message score is within the second range of values; and

storing the received electronic message until the earlier of the receipt of instructions for handling the received electronic message and the elapse of a second period of time if said message score is within the third range of message values, wherein the second period of time is shorter the first period of time.

5. A method according to claim 1, wherein the multiple threshold values define a first range of values, a second range of values and a third range of values,

and wherein the method further comprises the filtering apparatus:

forwarding the received electronic message to the addressee if said message score is within the first range of values;

storing the received electronic message until instructions are received for handling the received electronic message if said message score is within the second range of values; and

deleting the received electronic message if said message score is within the third range of values.

6. A method according to claim 4 or 5, wherein the message score is indicative of the likelihood of the received electronic message being wanted by the addressee, and wherein the third range of values is

associated with a higher likelihood of the received electronic message being unwanted than the second range of values.

7. A method according to any of claims 3 to 6, wherein said storing of a received electronic message comprises the filtering apparatus updating an index of stored electronic messages associated with the addressee of the received electronic message with details of the received electronic message.

8. A method according to claim 1, further comprising the filtering apparatus:

transmitting said index of stored electronic messages to a remote network device;

receiving instructions from the remote network device for handling the stored electronic messages; and

implementing the received instructions.

9. A method according to claim 8, wherein said transmitting of the index comprises the filtering apparatus transmitting web page data for a web page including said index and an interface allowing an operator of the remote network device to enter said instructions.

10. A method according to claim 9, wherein said interface comprises mark-up language data having a data entry field associated with each electronic message identified in the index, each data entry field allowing the operator of the remote apparatus to enter an instruction for handling the corresponding stored electronic message.

11. A method according to claim 9 or 10, wherein said web page data is transmitted in response to a request received from the remote apparatus.

12. A method according to any preceding claim, further comprising a process of setting the multiple threshold values.

13. A method according to claim 12, wherein the process of setting the multiple threshold values comprises the filtering apparatus receiving a signal from a remote network device indicative of the multiple threshold values.

14. A method according to claim 13, wherein the process of setting the multiple threshold values comprises the filtering apparatus transmitting to a remote network device web page data for a web page including an interface allowing the entry of new threshold values by the operator of the remote apparatus.

15. A method according to any preceding claim, further comprising the filtering apparatus:

identifying the sender of the received electronic message; and

forwarding the received electronic message to the addressee if the sender is on a list of approved senders for the addressee.

16. A method according to claim 15, wherein if the sender of the received electronic message is not on the list of approved senders for the addressee and the filtering apparatus forwards the received electronic message to the addressee under predefined conditions, the

method further comprises adding the sender of an electronic message forwarded to the addressee to the list of approved senders for the addressee.

17. A method according to claim 16, wherein the predefined conditions include that the filtering of the received electronic message comprises the filtering apparatus storing the received electronic message, and the filtering apparatus receiving instructions to forward the stored electronic message to the addressee.

18. A method according to any preceding claim, wherein the electronic message comprises a header portion and a body portion, and wherein said analysing of an electronic message comprises applying tests to the header portion and the body portion.

19. A method according to any preceding claim, wherein said analysing of the received electronic message comprises performing a heuristic analysis using information derived from previous electronic messages.

20. A method of filtering electronic messages transmitted over a communications network to an addressee, the method comprising a filtering apparatus:

analysing a received electronic message to identify sender information indicative of a sender of said received electronic message;

determining if the sender corresponding to the identified sender information is on a list of approved senders for the addressee of said received electronic message;

if the sender is on the list of approved senders

for the addressee, forwarding the received electronic message to the addressee; and

if the sender is not on the list of approved senders for the addressee: i) storing the received electronic message; and ii) receiving and implementing instructions for handling the stored electronic message,

wherein in response to said received instructions the filtering apparatus forwards the stored electronic message to the addressee and adds the sender of the stored electronic message to the list of approved senders.

21. A method according to claim 20, wherein the filtering apparatus automatically adds the sender of the stored electronic message to the list of approved senders if said received instructions indicate to forward the stored message to the addressee.

22. A method according to claim 20 or 21, further comprising the filtering apparatus determining if the sender corresponding to the identified sender information is on a list of prohibited senders for the addresee,

wherein if the sender is on the list of prohibited senders, the filtering apparatus deletes the received electronic message,

wherein if the sender is not on the list of prohibited senders for the addressee, the filtering apparatus stores the received electronic message, and receives and implements instructions for handling the stored electronic message; and

wherein in response to a received instruction the filtering apparatus deletes the stored electronic message and adds the sender of the stored electronic message to

the list of prohibited senders.

23. A method of filtering electronic messages transmitted over a communications network to an addressee, the method comprising a filtering apparatus;

analysing a received electronic message to identify sender information indicative of a sender of said received electronic message;

determining if the sender corresponding to the identified sender information is on a list of prohibited senders for the addressee of said received electronic message;

if the sender is on the list of prohibited senders for the addressee, deleting the received electronic message; and

if the sender is not on the list of prohibited senders for the addressee: i) storing the received electronic message; and ii) receiving and implementing instructions for handling the stored electronic message,

wherein in response to a received instruction the filtering apparatus deletes the stored electronic message and adds the sender of the stored electronic message to the list of prohibited senders.

24. A method according to any of claims 20 to 23, further comprising the filtering apparatus:

applying a plurality of predefined tests to the received electronic message to derive a message score in dependence thereon; and

comparing said message score with at least one threshold value,

wherein said storing of the received electronic message occurs if the message value is within a range of

values defined by said at least one threshold value.

25. A method according to claim 24, wherein the comparison of the message score with at least one threshold value comprises comparing the message score with multiple threshold values.

26. A method according to claim 25, wherein the multiple threshold values define a first range of values, a second range of values and a third range of values,

and wherein the method further comprises the filtering apparatus:

forwarding the received electronic message to the addressee if said message score is within the first range of values;

storing the received electronic message until the earlier of the receipt of instructions for handling the received electronic message and the elapse of a first predetermined period of time if said message score is within the second range of values; and

storing the received electronic message until the earlier of the receipt of instructions for handling the received electronic message and the elapse of a second predetermined period of time if said message score is within the third range of message values, wherein the second predetermined period of time is shorter than the first predetermined period of time.

27. A method according to claim 25, wherein the multiple threshold values define a first range of values, a second range of values and a third range of values, and wherein the method further comprises the filtering apparatus:

forwarding the received electronic message to the addressee if said message score is within the first range of values;

storing the received electronic message until instructions are received for handling the received electronic message if said message score is within the second range of values; and

deleting the received electronic message if said message score is within the third range of values.

28. A method according to claim 26 or 27, wherein the message score is indicative of the likelihood of the received electronic message being wanted by the addressee, and wherein the third range of values is associated with a higher likelihood of the received electronic message being unwanted than the second range of values.

29. A method according to any of claims 20 to 28, wherein said storing of a received electronic message comprises updating an index of stored electronic messages associated with the addressee of the received electronic message with details of the received electronic message.

30. A method according to claim 29, further comprising the filtering apparatus:

transmitting said index of stored electronic messages to a remote network device;

receiving instructions from the remote network device for handling the stored electronic messages; and

implementing the received instructions.

31. A method according to claim 30, wherein said

transmitting of the index comprises transmitting web page data for a web page including said index and an interface allowing an operator of the remote apparatus to enter said instructions.

32. A method according to claim 31, wherein said interface comprises mark-up language data for a form including a data entry field for each electronic message identified in the index, each data entry field allowing the operator of the remote apparatus to enter an instruction for handling the corresponding stored electronic message.

33. A method according to claim 31 or 32, wherein said web page data is transmitted in response to a request received from the remote network device.

34. A method of filtering electronic messages transmitted over a communications network to an addressee, the method comprising a filtering apparatus:

transmitting an electronic message to a remote network device, said electronic message comprising an interface enabling entry of instructions for implementation by the filtering apparatus;

receiving instructions from the remote network device; and

implementing the instructions received from the addressee.

35. A method according to claim 34, wherein said transmitting of the electronic message comprises transmitting the electronic message to the addressee.

36. A method according to claim 34 or 35, wherein

the interface comprises mark-up language data for a form having data entry fields for the entry of said instructions.

37. A method according to claim 36, wherein the interface comprises hypertext mark-up language data for said form.

38. A method according to claim 34 or 35, wherein the electronic message comprises a text file including data entry fields for the entry of said instructions.

39. A method according to any of claims 34 to 38, wherein the interface identifies electronic messages stored by the filtering apparatus, and the instructions comprise instructions for handling the electronic messages stored by the filtering apparatus.

40. A method according to any of claims 34 to 38, wherein the instructions identify approved senders for the addressee.

41. A method according to any of claims 34 to 38, further comprising the filtering apparatus:

analysing a received electronic message using predefined tests to derive a message score in dependence thereon; and

filtering the received electronic message in dependence upon the relationship between the message score and at least one threshold value,

wherein said received instructions identify said at least one threshold value.

42. A method of filtering electronic messages

transmitted over a communications network to a plurality of addressees using a common filtering apparatus which is coupled to the communications network, the method comprising the filtering apparatus:

splitting a received electronic message for one of the plurality of addressees into a plurality of message tokens;

retrieving a plurality of token values respectively corresponding to at least some of the plurality of message tokens from a set of stored token values;

calculating a message score for the received message using the retrieved token values; and

if the calculated message score satisfies a predefined condition, forwarding the received electronic message to the addressee and updating the stored token values in dependance upon the message tokens of the received electronic message.

43. A method of filtering electronic messages according to claim 42, wherein the filtering apparatus stores a plurality of sets of token values, each set of token values being associated with a respective addressee, and the retrieving of the stored token values comprises identifying which of the plurality of sets of token values is associated with the addressee of the received electronic message.

44. A method of filtering electronic messages according to claim 42, wherein the filtering apparatus stores a plurality of sets of token values, each set of token values being associated with a respective group of addressees, and the retrieving of the stored token values comprises identifying which of the plurality of sets of

token values is associated with the addressee of the received electronic message.

45. A method of filtering electronic messages according to claim 42, wherein the filtering apparatus stores a single set of token values which are used for all electronic messages filtered by the filtering apparatus.

46. A method of filtering electronic messages transmitted to a set of electronic message addresses associated with a family, the family including a parent and at least one child, the method comprising a filtering apparatus:

receiving filtering instructions from the parent for said at least one child; and

filtering electronic messages for said at least child in accordance with the received filtering instructions from the parent.

47. A method according to claim 46, wherein the filtering instructions identify approved senders for said at least one child,

and wherein the filtering of electronic messages comprises the filtering apparatus:

identifying the sender of each received electronic message for said at least one child;

if the sender is on the list of approved senders, forwarding the electronic message to the addressee; and

if the sender is not on the list of approved senders, blocking the electronic message.

48. A method according to any preceding claim,

wherein the electronic message is an e-mail message.

49. A storage device storing instructions including instructions for causing a programmable processing apparatus to become operable to perform a method according to any preceding claim.

50. A signal conveying instructions including instructions for causing a programmable processing apparatus to become operable to perform a method according to any of claims 1 to 48.

51. An electronic message filtering apparatus comprising:

an analyser operable to analyse a received electronic message using predefined tests to derive a message score in dependence thereon;

a comparator operable to compare said message score with multiple threshold values; and

a filter operable to filter the received electronic message in dependence upon the relationship between the measured score and the multiple threshold values.

52. An electronic message filtering apparatus according to claim 51, wherein the filter is arranged to delete the received electronic message if the comparator determines that the associated message score is within a range of values defined by one or more of the multiple threshold values.

53. An electronic message filtering apparatus according to claim 52, further comprising an electronic messages store, wherein the filter is arranged to store the received electronic message in the electronic

messages store if the comparator determines that the associated message score is within a range of values defined by one or more of the multiple threshold values.

54. An electronic message filtering apparatus according to claim 51, wherein the multiple threshold values define a first range of values, a second range of values and a third range of values,

wherein the electronic message filtering apparatus comprises an electronic messages store,

and wherein the filter is operable to:

forward the received electronic message to the addressee if the comparator determines said message score is within the first range of values;

store the received electronic message in the electronic messages store until the earlier of the receipt of instructions for handling the received electronic message and the elapse of a first predetermined period of time if the comparator determines said message score is within the second range of values;

and

store the received electronic message in the electronic messages store until the earlier of the receipt of instructions for handling the received electronic message and the elapse of a second predetermined period of time if said message score is within the third range of message values, the second predetermined period of time being shorter than the first predetermined period of time.

55. An electronic message filtering apparatus according to claim 51, wherein the multiple threshold values define a first range of values, a second range of

values and a third range of values,

wherein the electronic messages filtering apparatus further comprises an electronic messages store;

and wherein the filter is operable to:

forward the received electronic message to the addressee if said message score is within the first range of values;

store the received electronic message in the electronic messages store until instructions are received for handling the received electronic message if said message score is within the second range of values; and

delete the received electronic message if said message score is within the third range of values.

56. An electronic message filtering apparatus according to claim 54 or 55, wherein the message score is indicative of the likelihood of the received electronic message being wanted by the addressee, and wherein the third range of values is associated with a higher likelihood of the received electronic message being unwanted than the second set of values.

57. An electronic message filtering apparatus according to any of claims 53 to 56, wherein said electronic messages store is configured to store an index of electronic messages stored in the electronic messages store,

and wherein said electronic messages filtering apparatus further comprises an index updater operable to update the index when an electronic message is added to the electronic messages store.

58. An electronic message filtering apparatus

according to claim 57, further comprising:

a network interface enabling communication with a remote network device via a communications network; and

a controller operable to transmit said index of stored electronic messages to the remote network device via the communications network, to receive instructions from the remote network device for handling the stored electronic messages, and to implement the received instructions.

59. An electronic message filtering apparatus according to claim 58, further comprising a web server operable to generate web page data for a web page including said index and an interface allowing an operator of the remote apparatus to enter said instructions.

60. An electronic message filtering apparatus according to claim 59, wherein said interface comprises mark-up language data for a form having a data entry field for each electronic message identified in the index, each data entry field allowing the operator of the remote network device to enter an instruction for handling the corresponding stored electronic message.

61. An electronic message filtering apparatus according to claim 59 or 60, wherein the web server is arranged to transmit said web page data in response to a request received from the remote network device.

62. An electronic message filtering apparatus according to any of claims 51 to 61, further comprising a threshold setter operable to set the multiple threshold

values.

63. An electronic message filtering apparatus according to claim 62, wherein the threshold setter is operable to set the multiple threshold values in accordance with a signal received from a remote network device.

64. An electronic message filtering apparatus according to claim 63, further comprising a web server operable to generate web page data for a web page including an interface allowing the entry of new threshold values by the operator of the remote apparatus.

65. An electronic message filtering apparatus according to any of claims 51 to 64, further comprising:

a data store for storing a list of approved senders;

an identifier operable to identify the sender of the received electronic message;

a determiner operable to determine if the identified sender is on the list of approved senders stored in the data store; and

an electronic message forwarder operable to forward the received electronic message to the addressee if the identified sender is on the list of approved senders.

66. An electronic message filtering apparatus according to claim 65, further comprising an updater operable to add the sender of an electronic message forwarded to the addressee to the list of approved senders under predefined conditions if the sender is not already on the list of approved senders.

67. An electronic message filtering apparatus according to claim 66, wherein the predefined conditions include that the received electronic message is stored by the filter, and is subsequently forwarded to the addressee in response to instructions received from a remote network device.

68. An electronic message filtering apparatus according to any of claims 51 to 67, wherein the electronic message comprises a header portion and a body portion, and wherein said analyser is operable to apply tests to the header portion and the body portion.

69. A method according to any of claims 51 to 68, wherein the analyser is operable to perform a heuristic analysis using information derived from analysis of previous electronic messages.

70. An electronic message filtering apparatus operable to filter electronic messages transmitted over a communications network to an addressee, the electronic message filtering apparatus comprising:

an analyser operable to analyse a received electronic message for an addressee to identify sender information indicative of a sender of said received electronic message;

a determiner operable to determine if the sender corresponding to the identified sender information is on a list of approved senders for the addressee of said received electronic message;

a filter operable i) to forward the received electronic message to the addressee if the determiner determines that the sender is on the list of approved

senders for the addressee, and ii) to store the received electronic message if the sender is not on the list of approved senders for the addressee; and a controller operable to implement a received instruction for handling the stored electronic message,

wherein said controller is operable to add the sender of the stored electronic message to the list of approved senders in response to a received instruction.

71. An electronic message filtering apparatus according to claim 70, wherein the controller is operable to add automatically the sender of the stored electronic message to the list of approved senders in response to a received instruction indicating to forward the stored message to the addressee.

72. An electronic message filtering apparatus according to claim 70 or 71, wherein the determiner is operable to determine if the sender corresponding to the identified sender information is on a list of prohibited senders,

wherein if the sender is on the list of prohibited senders, the filtering apparatus deletes the received electronic message,

wherein if the sender is not on the list of prohibited senders the filtering apparatus stores the received electronic message, and

wherein said controller is operable to delete the stored electronic message and add the sender of the stored electronic message to the list of prohibited senders in response to a received instruction.

73. An electronic message filtering apparatus

operable to filter electronic messages transmitted over a communications network to an addressee, the electronic message filtering apparatus comprising:

an analyser operable to analyse a received electronic message for an addressee to identify sender information indicative of a sender of said received electronic message;

a determiner operable to determine if the sender corresponding to the identified sender information is on a list of prohibited senders for the addressee of said received electronic message;

a filter operable i) to delete the received electronic message if the determiner determines that the sender is on the list of prohibited senders for the addressee, and ii) to store the received electronic message if the sender is not on the list of approved senders for the addressee; and

a controller operable to implement a received instruction for handling the stored electronic message,

wherein said controller is operable to add the sender of the stored electronic message to the list of prohibited senders in response to a received instruction.

74. An electronic message filtering apparatus according to claim 73, wherein the filter comprises:

a content filter operable to apply a plurality of predefined tests to the received electronic message to derive a message score in dependence thereon; and

a comparator operable to compare said message score with at least one threshold value,

wherein the filter is operable to store the received electronic message if the message value is

within a range of values defined by said at least one threshold value.

75. An electronic message filtering apparatus according to claim 74, wherein the comparator is operable to compare the message score with multiple threshold values.

76. An electronic message filtering apparatus according to claim 75, wherein the multiple threshold values define a first range of values, a second range of values and a third range of values,

and wherein the filter is operable:

to forward the received electronic message to the addressee if said message score is within the first range of values;

to store the received electronic message until the earlier of the receipt of instructions for handling the received electronic message and the elapse of a first predetermined period of time if said message score is within the second range of values; and

to store the received electronic message until the earlier of the receipt of instructions for handling the received electronic message and the elapse of a second predetermined period of time if said message score is within the third range of message values, wherein the second predetermined period of time is shorter than the first predetermined period of time.

77. An electronic message filtering apparatus according to claim 75, wherein the multiple threshold values define a first range of values, a second range of values and a third range of values,

and wherein the filter is operable:

to forward the received electronic message to the addressee if said message score is within the first range of values;

to store the received electronic message until instructions are received for handling the received electronic message if said message score is within the second range of values; and to delete the received electronic message if said message score is within the third range of values.

78. An electronic message filtering apparatus according to claim 76 or 77, wherein the message score is indicative of the likelihood of the received electronic message being wanted by the addressee, and wherein the third range of values is associated with a higher likelihood of the received electronic message being unwanted than the second range of values.

79. An electronic message filtering apparatus according to any of claims 70 to 78, wherein the data store is configured to store an index of stored electronic messages, and wherein the electronic message filtering apparatus further comprises an updater operable to update an index of stored electronic messages associated with the addressee of the received electronic message with details of the received electronic message.

80. An electronic message filtering apparatus according to claim 79, further comprising:

a transmitter operable to transmit said index of stored electronic messages to a remote network device;

and

a controller operable to implement instructions, received from the remote network device, for handling the stored electronic messages.

81. An electronic message filtering apparatus according to claim 80, wherein the transmitter is operable to transmit web page data for a web page including said index and an interface allowing an operator of the remote apparatus to enter said instructions.

82. An electronic message filtering apparatus according to claim 81, wherein said interface comprises mark-up language data for a form having a data entry field for each electronic message identified in the index, each data entry field allowing the operator of the remote apparatus to enter an instruction for handling the corresponding stored electronic message.

83. An electronic message filtering apparatus according to claim 81 or 82, wherein said web page data is transmitted in response to a request received from the remote network device.

84. An electronic message filtering apparatus operable to filter electronic messages transmitted over a communications network to an addressee, the electronic message filtering apparatus comprising:

a transmitter operable to transmit an electronic message to a remote network device, said electronic message comprising an interface enabling an operator of the remote network device to enter instructions for implementation by the filtering apparatus; and

a controller operable to implement the instructions received from the addressee.

85. An electronic message filtering apparatus according to claim 84, wherein the transmitter is arranged to transmit the electronic message to the addressee.

86. An electronic message filtering apparatus according to claim 84 or 85, wherein the interface comprises mark-up language data for a form having data entry fields for the entry of said instructions.

87. An electronic message filtering apparatus according to claim 86, wherein the interface comprises hypertext mark-up language data for said form.

88. An electronic message filtering apparatus according to any of claims 84 to 87, wherein the electronic message comprises a text file including data entry fields for the entry of said instructions.

89. An electronic message filtering apparatus according to any of claims 84 to 88, wherein the instructions comprise instructions for handling electronic messages stored by the filtering apparatus.

90. An electronic message filtering apparatus according to any of claims 84 to 88, wherein the instructions identify approved senders for the addressee.

91. An electronic message filtering apparatus according to any of claims 84 to 90, further comprising:

an analyser operable to analyse a received electronic message using predefined tests to derive a

message score in dependence thereon; and

a filter operable to filter the received electronic message in dependence on the relationship between the message score and at least one threshold value,

wherein said instructions identify said at least one threshold value.

92. An electronic message filtering apparatus operable to filter electronic messages transmitted over a communications network to a plurality of addressees, the electronic message filtering apparatus comprising:

a data store configured to store a database comprising a plurality of tokens and a respective plurality of token values;

a message splitter operable to split a received electronic message into a plurality of message tokens;

a retriever operable to retrieve token values corresponding to at least some of said message tokens from the data store;

a calculator operable to calculate a message score using the retrieved token values corresponding to at least some of the plurality of message tokens;

a transmitter operable to forward the received electronic message to the addressee if the message score satisfies a predefined condition; and

an updater operable to update the stored token values in dependance upon the message tokens of the received electronic message.

93. An electronic message filtering apparatus according to claim 92, wherein the data store is configured to store a plurality of sets of token values, each set of token values being associated with a

respective addressee,

wherein the electronic message filtering apparatus further comprises an identifier operable to identify the addressee of the received electronic message,

and wherein the retriever is operable to retrieve the stored token values from the set of token values corresponding to the addressee of the received electronic message.

94. An electronic message filtering apparatus according to claim 92, wherein the data stored is configured to store a plurality of sets of token values, each set of token values being associated with a respective group of addresses,

wherein the electronic message filtering apparatus further comprises an identifier operable to identify the addressee of the received electronic message,

and wherein the retriever is operable to retrieve the stored token values from the set of token values corresponding to the addressee of the received electronic message.

95. An electronic message filtering apparatus according to claim 92, wherein the data store is configured to store a single set of token values,

and wherein the retriever is operable to retrieve the stored token values from the single set of token values.

96. An electronic messages filtering apparatus for filtering electronic messages transmitted to a set of electronic message addresses associated with a family, the family including a parent and at least one child, the

electronic messages filtering apparatus comprising:

an interface operable to receive filtering instructions from the parent for said at least one child; and

a filter operable to filter electronic messages for said at least one child in accordance with the received filtering instructions from the parent.

97. An electronic messages filtering apparatus according to claim 96, further comprising a data store configured to store a list of approved senders for the or each child,

wherein the filtering instructions identify approved senders for addition to the list of approved senders, and

wherein the filter is operable i) to identify the sender of a received electronic message for said at least one child, ii) to forward the electronic message to the addressee if the sender is on the list of approved senders, and iii) to block the electronic message if the sender is not on the list of approved senders.

98. An electronics communications system comprising:

a plurality of network devices connected to a communications network;

an electronic message filtering apparatus according to any of claims 51 to 97; and

a router operable to route electronic messages for at least one of the network devices via the electronic message filtering apparatus.

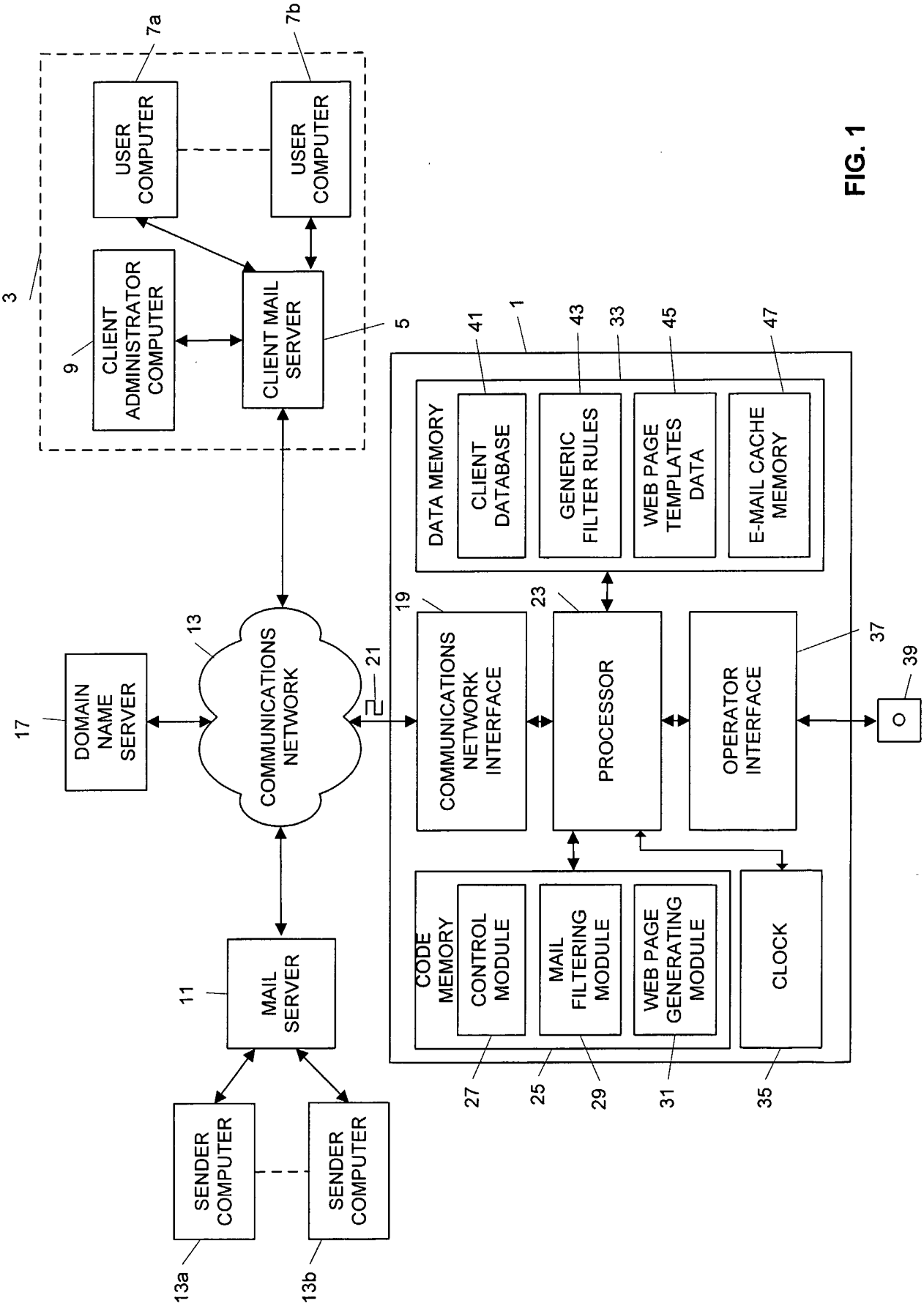

3
7a
USER COMPUTER
7b
USER COMPUTER
9
CLIENT ADMINISTRATOR COMPUTER
CLIENT MAIL SERVER
5
1
41
DATA MEMORY
CLIENT DATABASE
43
GENERIC FILTER RULES
33
45
WEB PAGE TEMPLATES DATA
47
E-MAIL CACHE MEMORY
19
COMMUNICATIONS NETWORK INTERFACE
23
PROCESSOR
OPERATOR INTERFACE
37
39
21
13
COMMUNICATIONS NETWORK
17
DOMAIN NAME SERVER
CODE MEMORY
CONTROL MODULE
MAIL FILTERING MODULE
WEB PAGE GENERATING MODULE
CLOCK
27
25
29
31
35
11
MAIL SERVER
SENDER COMPUTER
SENDER COMPUTER
13a
13b

FIG. 1

FIG. 2

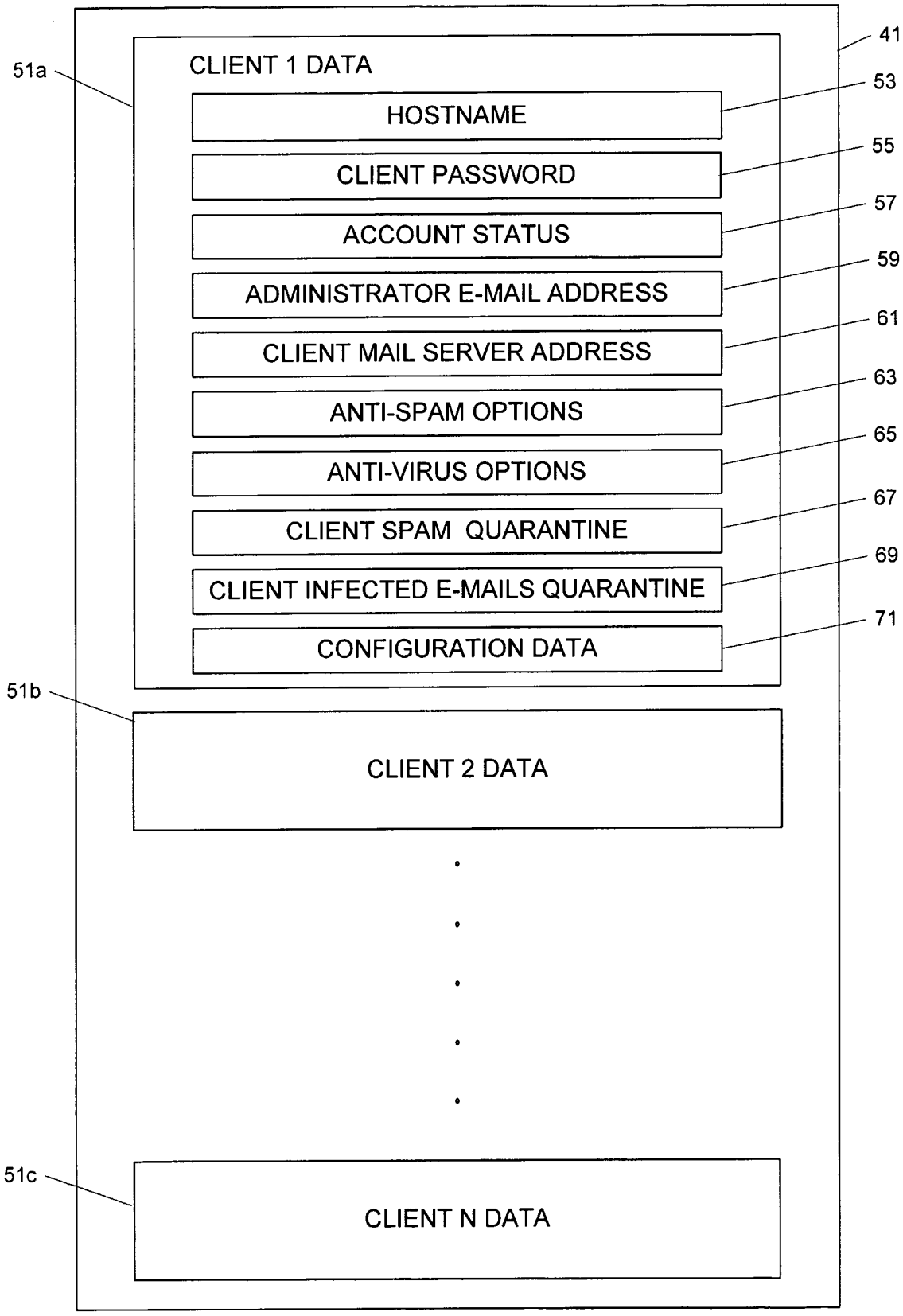

41
51a
CLIENT 1 DATA
53
HOSTNAME
55
CLIENT PASSWORD
57
ACCOUNT STATUS
59
ADMINISTRATOR E-MAIL ADDRESS
61
CLIENT MAIL SERVER ADDRESS
63
ANTI-SPAM OPTIONS
65
ANTI-VIRUS OPTIONS
67
CLIENT SPAM QUARANTINE
69
CLIENT INFECTED E-MAILS QUARANTINE
71
CONFIGURATION DATA
51b
CLIENT 2 DATA
51c
CLIENT N DATA

FIG. 3

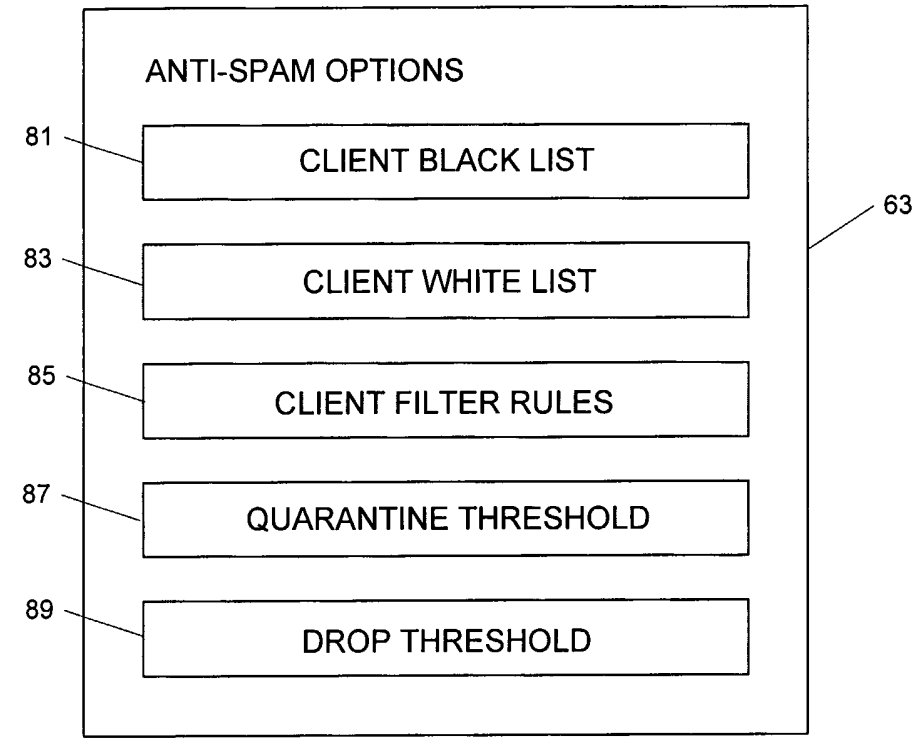
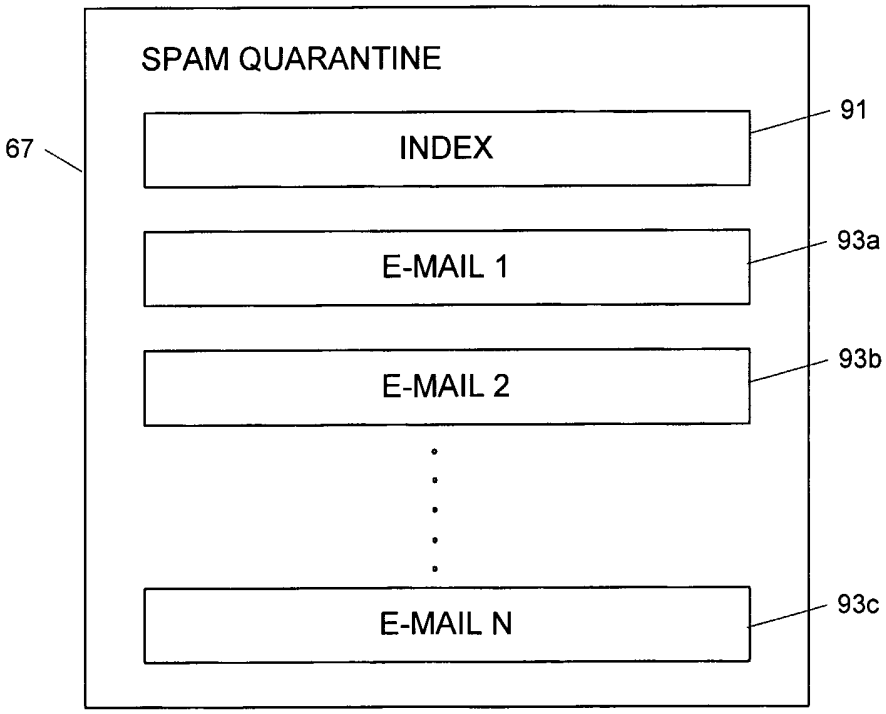

ANTI-SPAM OPTIONS
81
CLIENT BLACK LIST
83
CLIENT WHITE LIST
85
CLIENT FILTER RULES
87
QUARANTINE THRESHOLD
89
DROP THRESHOLD
63

FIG. 4


SPAM QUARANTINE
67
INDEX
91
E-MAIL 1
93a
E-MAIL 2
93b
E-MAIL N
93c

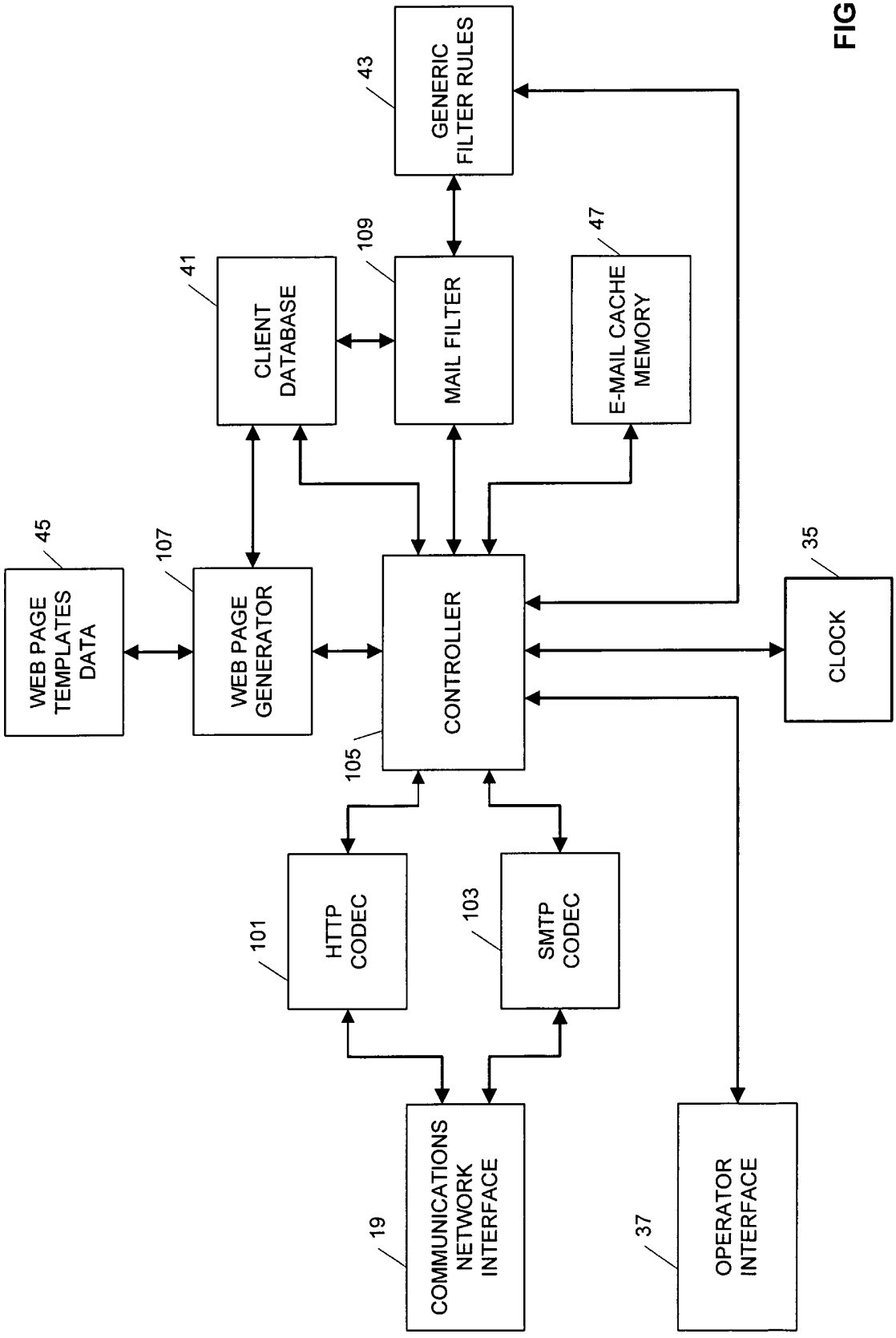

GENERIC FILTER RULES
43
CLIENT DATABASE
41
MAIL FILTER
109
E-MAIL CACHE MEMORY
47
WEB PAGE TEMPLATES DATA
45
WEB PAGE GENERATOR
107
CONTROLLER
105
CLOCK
35
HTTP CODEC
101
SMTP CODEC
103
COMMUNICATIONS NETWORK INTERFACE
19
OPERATOR INTERFACE
37

FIG. 5

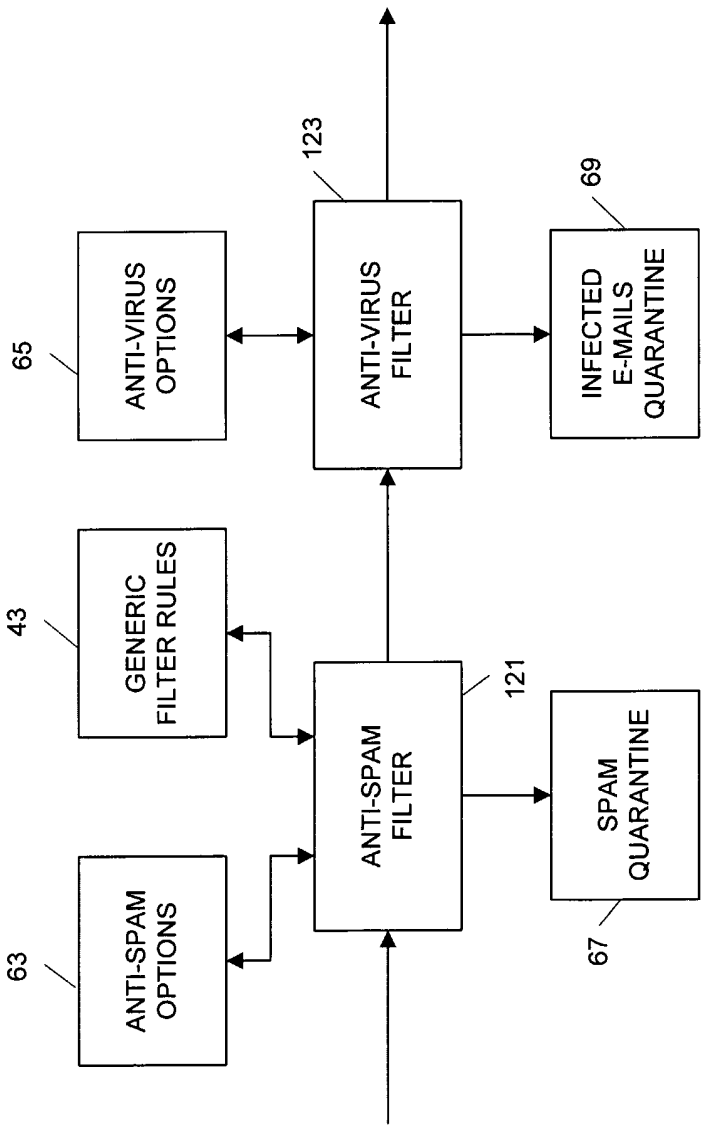

ANTI-VIRUS OPTIONS
65
ANTI-VIRUS FILTER
123
INFECTED E-MAILS QUARANTINE
69
GENERIC FILTER RULES
43
ANTI-SPAM FILTER
121
SPAM QUARANTINE
67
ANTI-SPAM OPTIONS
63

FIG. 6

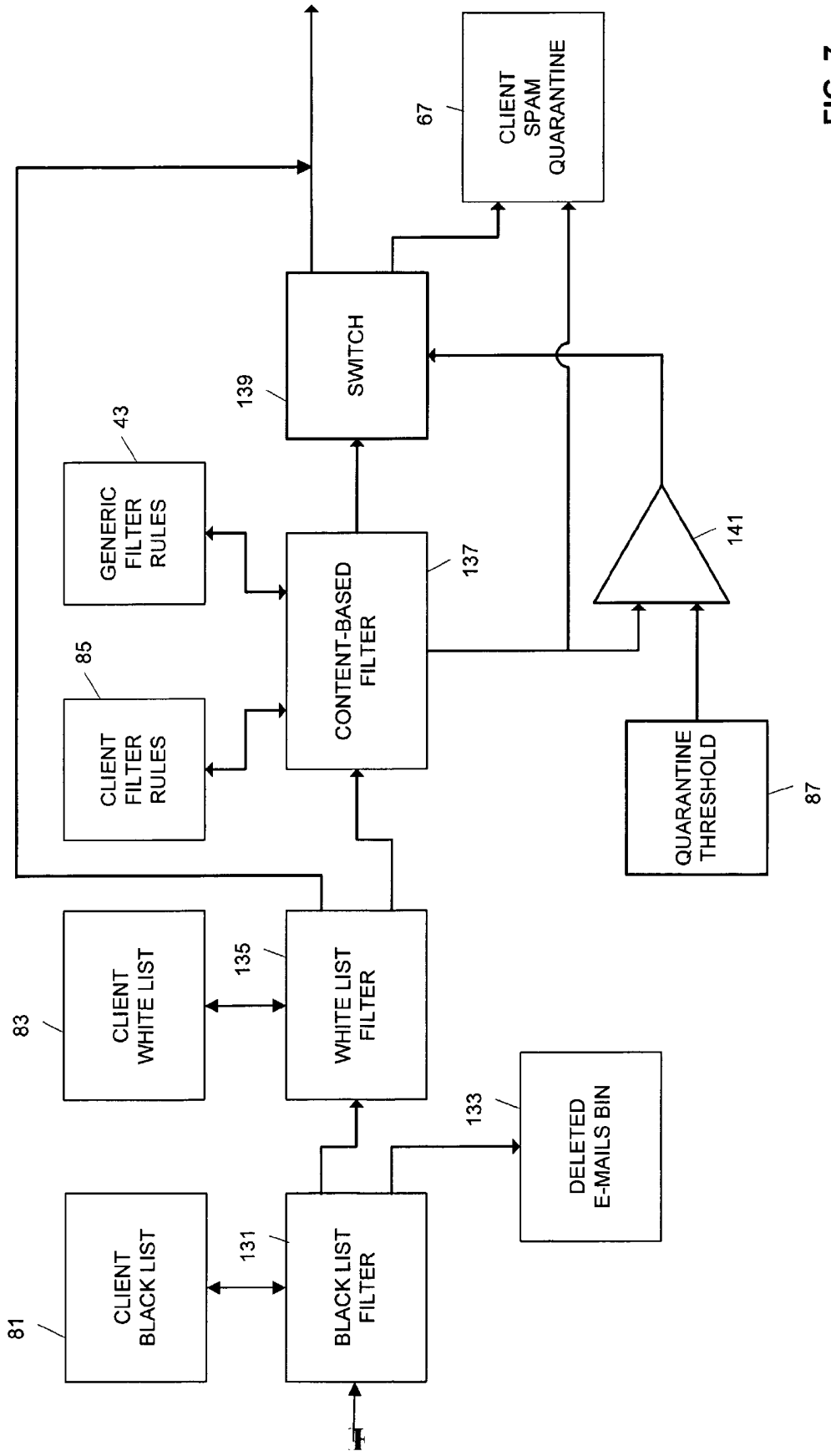

CLIENT BLACK LIST
81
BLACK LIST FILTER
131
DELETED E-MAILS BIN
133
CLIENT WHITE LIST
83
WHITE LIST FILTER
135
GENERIC FILTER RULES
43
CLIENT FILTER RULES
85
CONTENT-BASED FILTER
137
SWITCH
139
CLIENT SPAM QUARANTINE
67
QUARANTINE THRESHOLD
87
141

FIG. 7

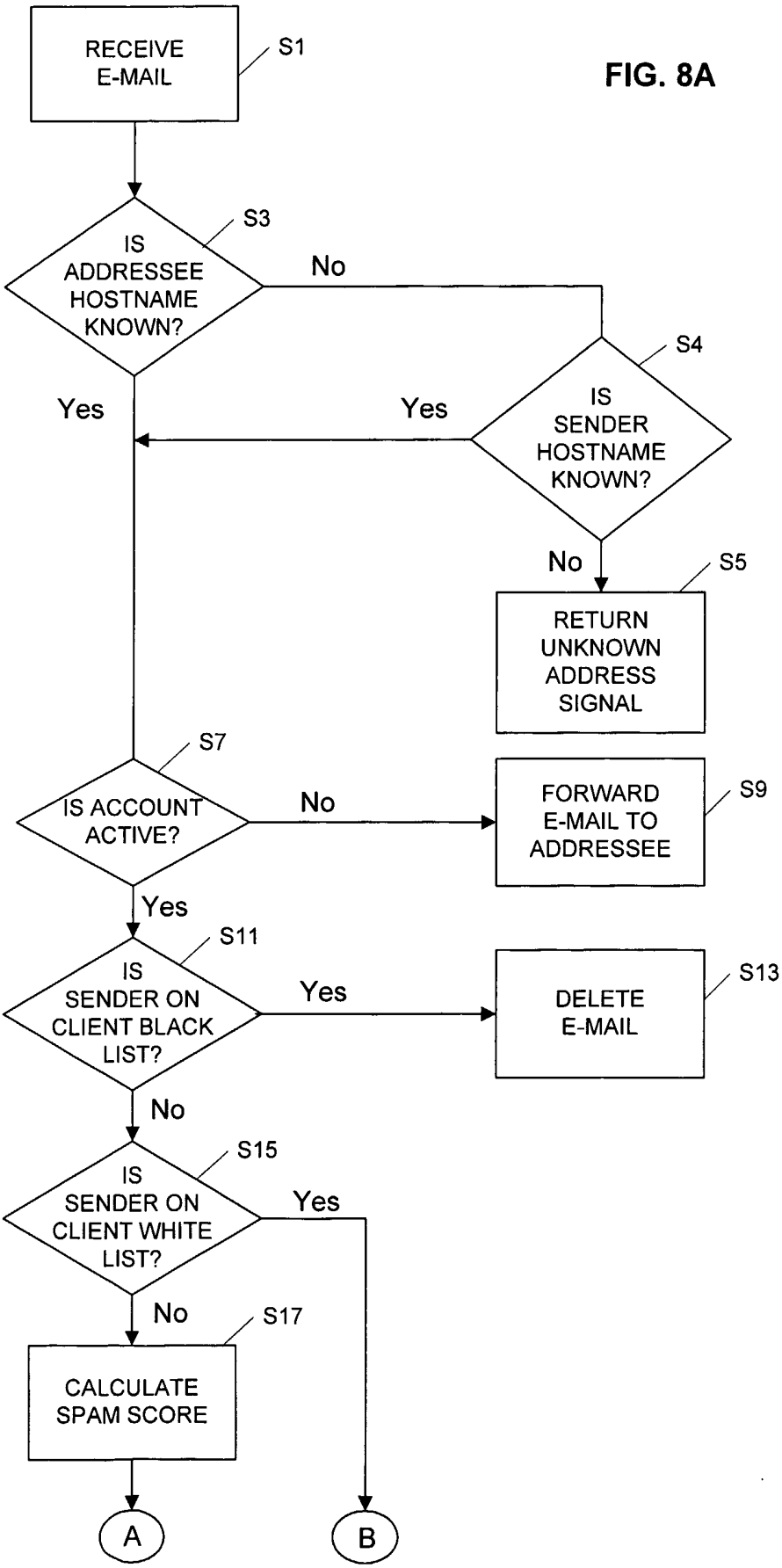

RECEIVE E-MAIL
S1
IS ADDRESSEE HOSTNAME KNOWN?
S3
No
Yes
IS SENDER HOSTNAME KNOWN?
S4
Yes
No
RETURN UNKNOWN ADDRESS SIGNAL
S5
IS ACCOUNT ACTIVE?
S7
No
FORWARD E-MAIL TO ADDRESSEE
S9
Yes
IS SENDER ON CLIENT BLACK LIST?
S11
Yes
DELETE E-MAIL
S13
No
IS SENDER ON CLIENT WHITE LIST?
S15
Yes
No
CALCULATE SPAM SCORE
S17
A
B

FIG. 8A

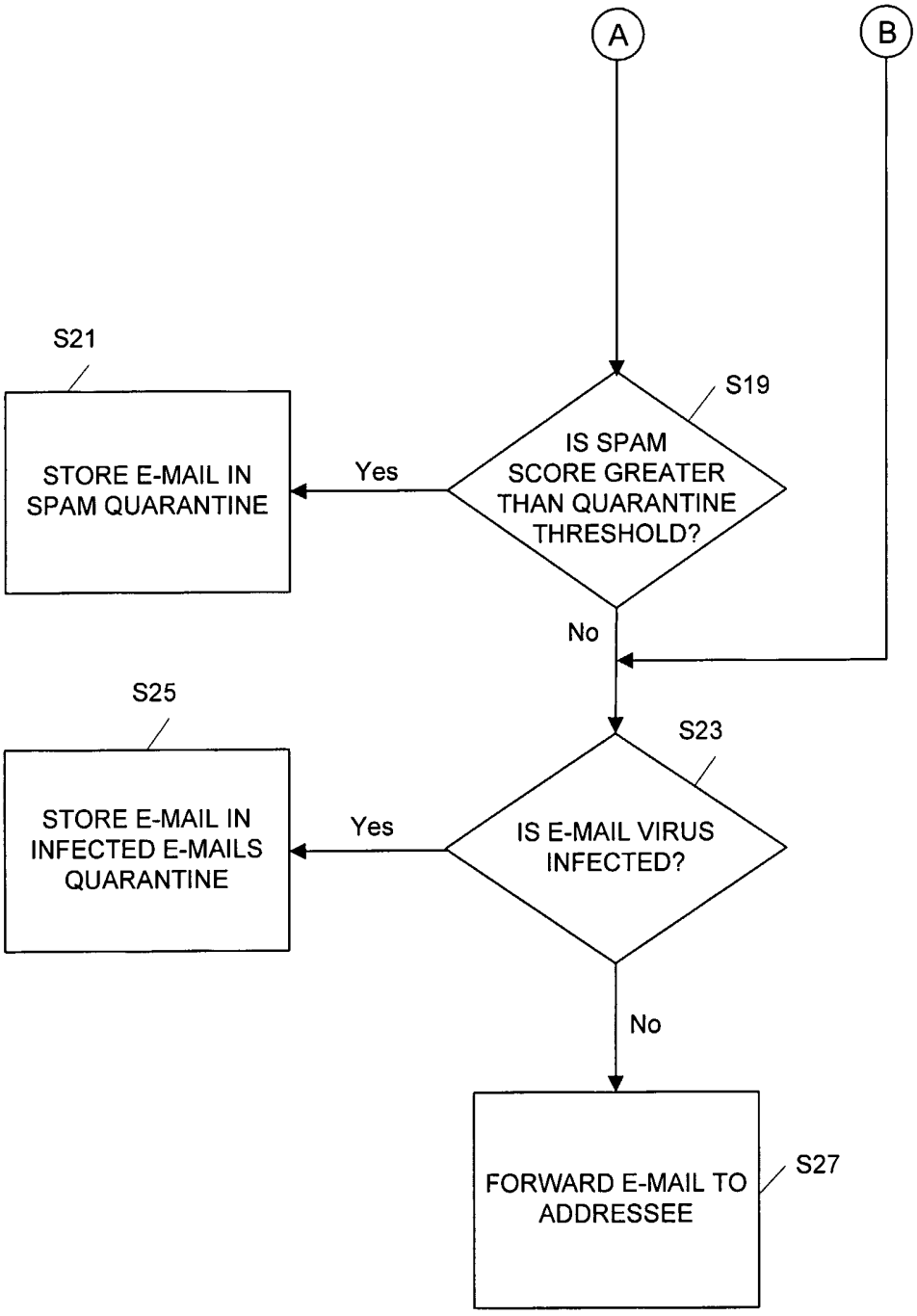

A
B
S21
STORE E-MAIL IN SPAM QUARANTINE
Yes
S19
IS SPAM SCORE GREATER THAN QUARANTINE THRESHOLD?
No
S25
STORE E-MAIL IN INFECTED E-MAILS QUARANTINE
Yes
S23
IS E-MAIL VIRUS INFECTED?
No
FORWARD E-MAIL TO ADDRESSEE
S27

FIG. 8B

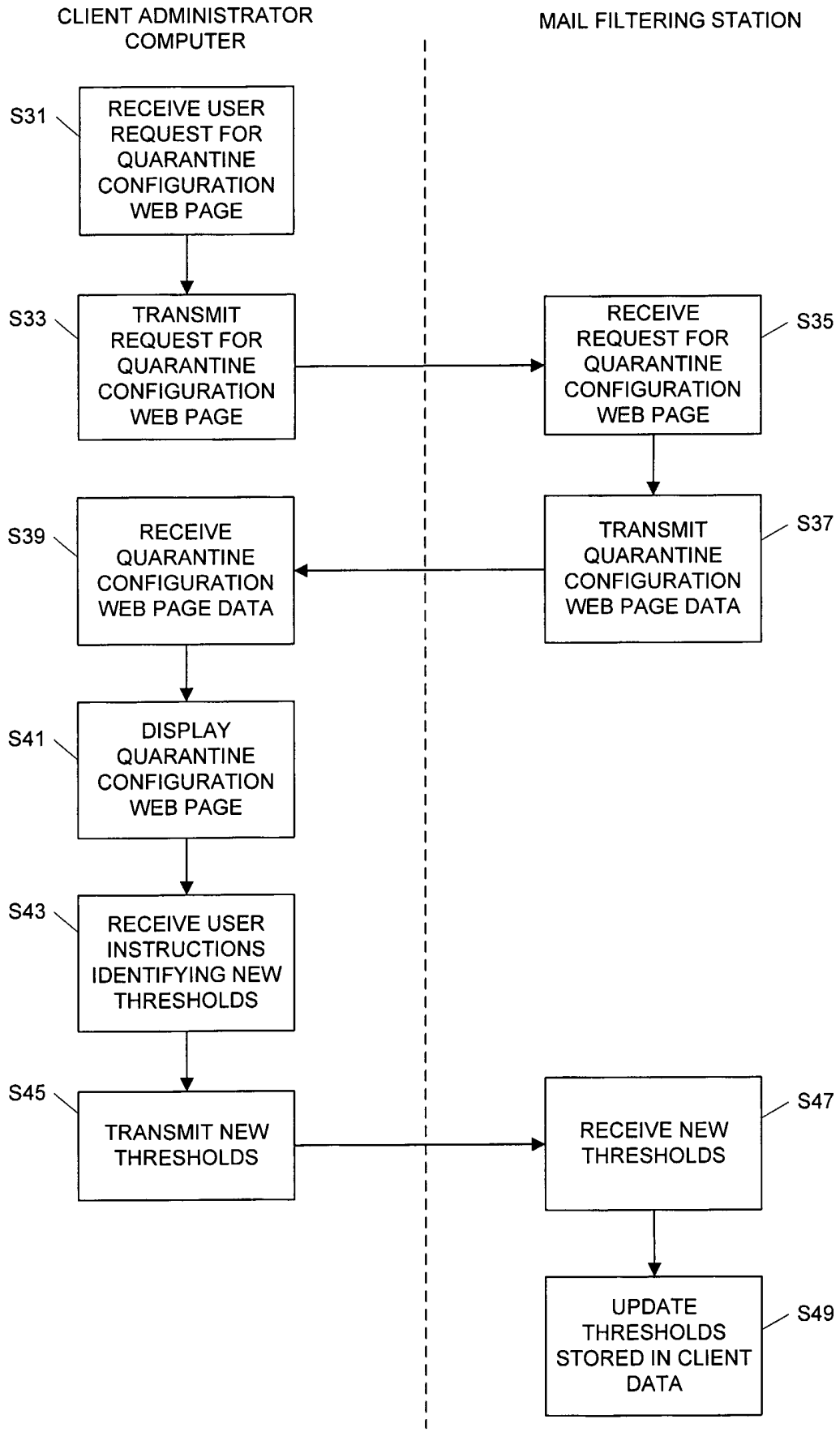

CLIENT ADMINISTRATOR COMPUTER
MAIL FILTERING STATION
S31
RECEIVE USER REQUEST FOR QUARANTINE CONFIGURATION WEB PAGE
S33
TRANSMIT REQUEST FOR QUARANTINE CONFIGURATION WEB PAGE
S35
RECEIVE REQUEST FOR QUARANTINE CONFIGURATION WEB PAGE
S37
TRANSMIT QUARANTINE CONFIGURATION WEB PAGE DATA
S39
RECEIVE QUARANTINE CONFIGURATION WEB PAGE DATA
S41
DISPLAY QUARANTINE CONFIGURATION WEB PAGE
S43
RECEIVE USER INSTRUCTIONS IDENTIFYING NEW THRESHOLDS
S45
TRANSMIT NEW THRESHOLDS
S47
RECEIVE NEW THRESHOLDS
S49
UPDATE THRESHOLDS STORED IN CLIENT DATA

FIG. 9

FIG. 10

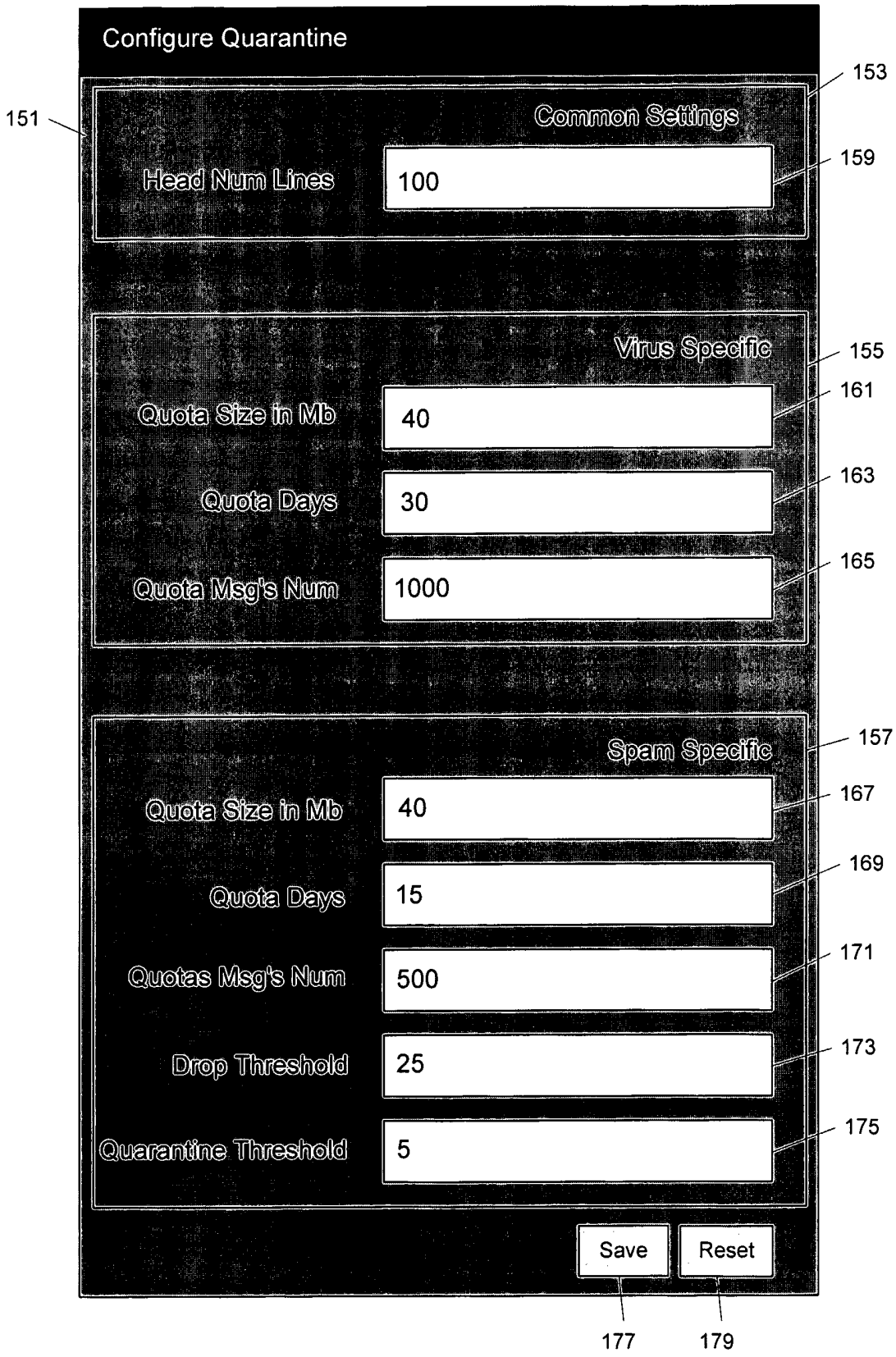
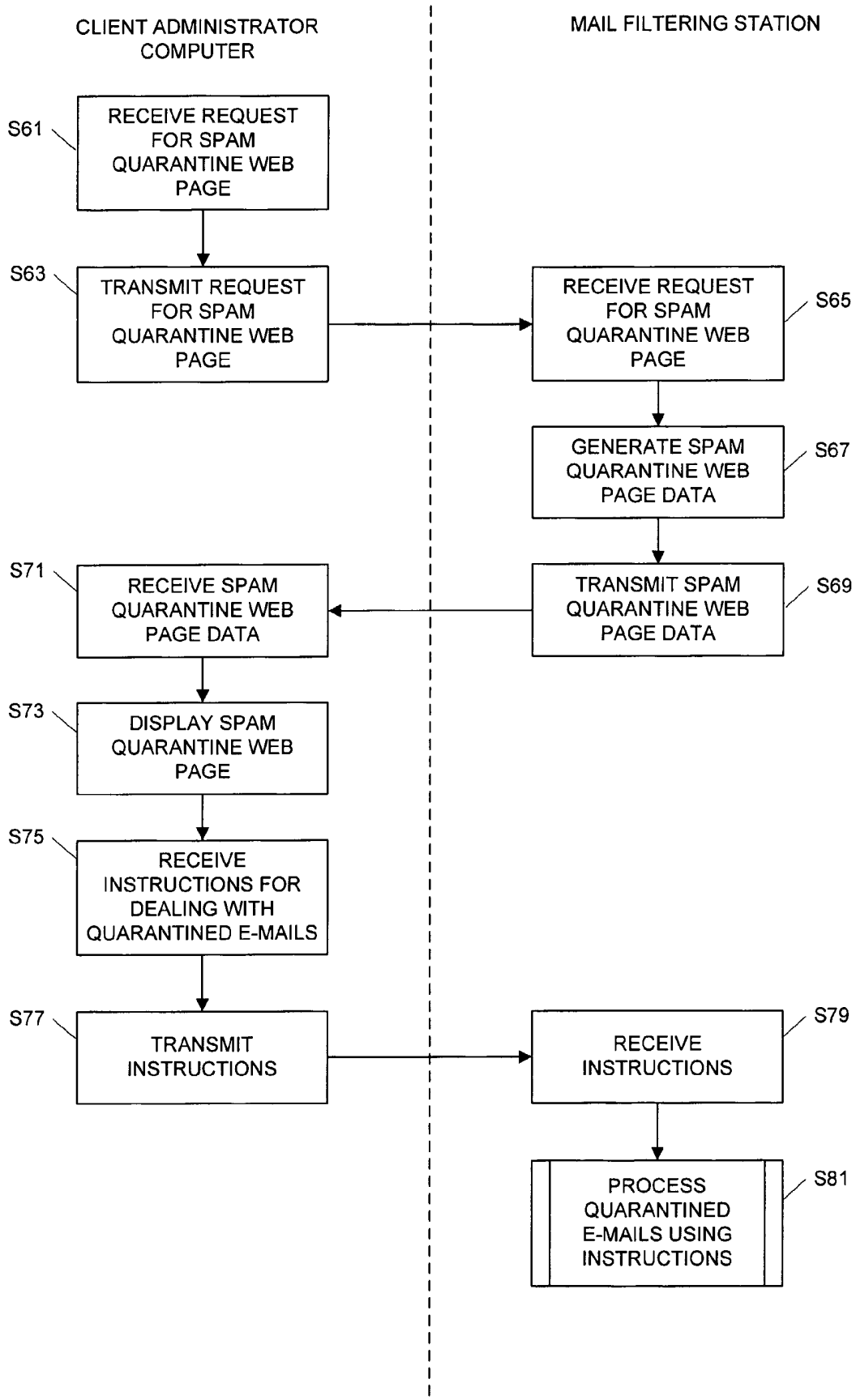

Configure Quarantine
151
153
Common Settings
Head Num Lines
100
159
Virus Specific
155
Quota Size in Mb
40
161
Quota Days
30
163
Quota Msg's Num
1000
165
Spam Specific
157
Quota Size in Mb
40
167
Quota Days
15
169
Quotas Msg's Num
500
171
Drop Threshold
25
173
Quarantine Threshold
5
175
Save
Reset
177
179

FIG. 11


CLIENT ADMINISTRATOR COMPUTER
MAIL FILTERING STATION
S61
RECEIVE REQUEST FOR SPAM QUARANTINE WEB PAGE
S63
TRANSMIT REQUEST FOR SPAM QUARANTINE WEB PAGE
RECEIVE REQUEST FOR SPAM QUARANTINE WEB PAGE
S65
GENERATE SPAM QUARANTINE WEB PAGE DATA
S67
TRANSMIT SPAM QUARANTINE WEB PAGE DATA
S69
S71
RECEIVE SPAM QUARANTINE WEB PAGE DATA
S73
DISPLAY SPAM QUARANTINE WEB PAGE
S75
RECEIVE INSTRUCTIONS FOR DEALING WITH QUARANTINED E-MAILS
S77
TRANSMIT INSTRUCTIONS
RECEIVE INSTRUCTIONS
S79
PROCESS QUARANTINED E-MAILS USING INSTRUCTIONS
S81

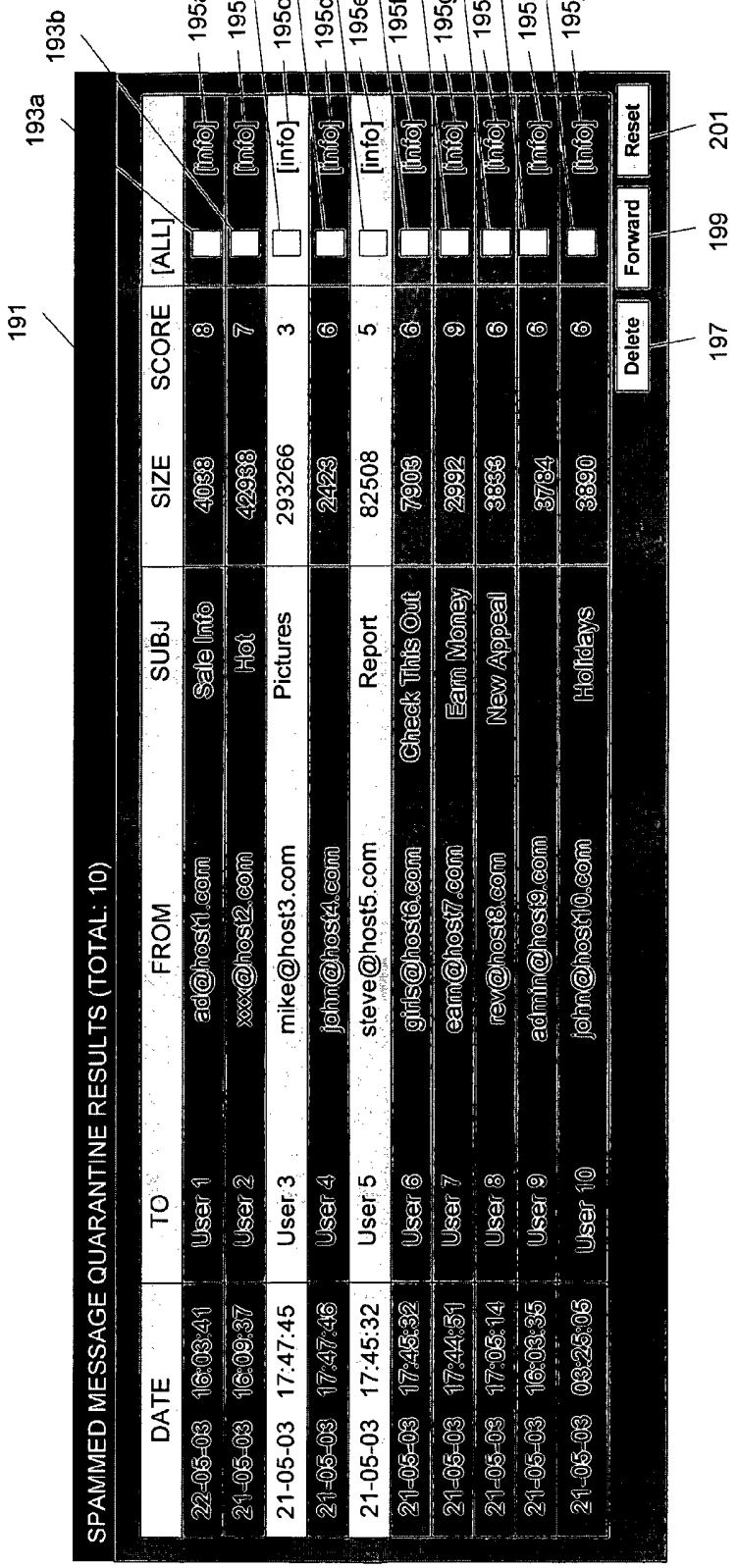

191
193a
193b
SPAMMED MESSAGE QUARANTINE RESULTS (TOTAL: 10)
DATE
TO
FROM
SUBJ
SIZE
SCORE
[ALL]
22-05-03 16:03:41 User 1 ed@host1.com Sale Info 4038 8 [info] 195a
21-05-03 16:09:37 User 2 xxx@host2.com Hot 42938 7 [info] 195b 193c
21-05-03 17:47:45 User 3 mike@host3.com Pictures 293266 3 [info] 195c 193d
21-05-03 17:47:46 User 4 john@host4.com 2423 6 [info] 195d 193e
21-05-03 17:45:32 User 5 steve@host5.com Report 82508 5 [info] 195e 193f
21-05-03 17:45:32 User 6 girls@host6.com Check This Out 7903 6 [info] 195f 193g
21-05-03 17:44:51 User 7 earn@host7.com Earn Money 2992 9 [info] 195g 193h
21-05-03 17:05:14 User 8 rev@host8.com New Appeal 3833 6 [info] 195h 193i
21-05-03 16:03:35 User 9 admin@host9.com 3784 6 [info] 195i 193j
21-05-03 03:25:05 User 10 john@host10.com Holidays 3890 6 [info] 195j
Delete
Forward
Reset
197
199
201

FIG. 12

FIG. 13

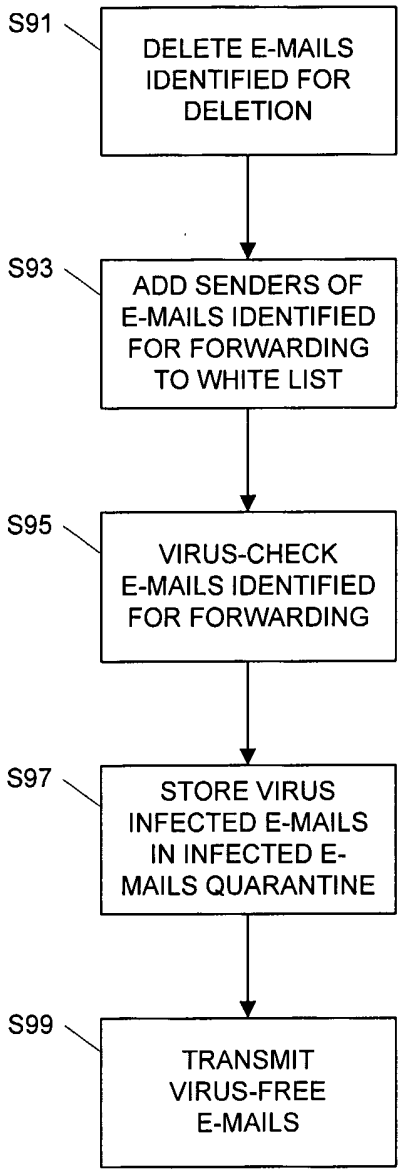

S91
DELETE E-MAILS IDENTIFIED FOR DELETION
S93
ADD SENDERS OF E-MAILS IDENTIFIED FOR FORWARDING TO WHITE LIST
S95
VIRUS-CHECK E-MAILS IDENTIFIED FOR FORWARDING
S97
STORE VIRUS INFECTED E-MAILS IN INFECTED E-MAILS QUARANTINE
S99
TRANSMIT VIRUS-FREE E-MAILS

FIG. 14

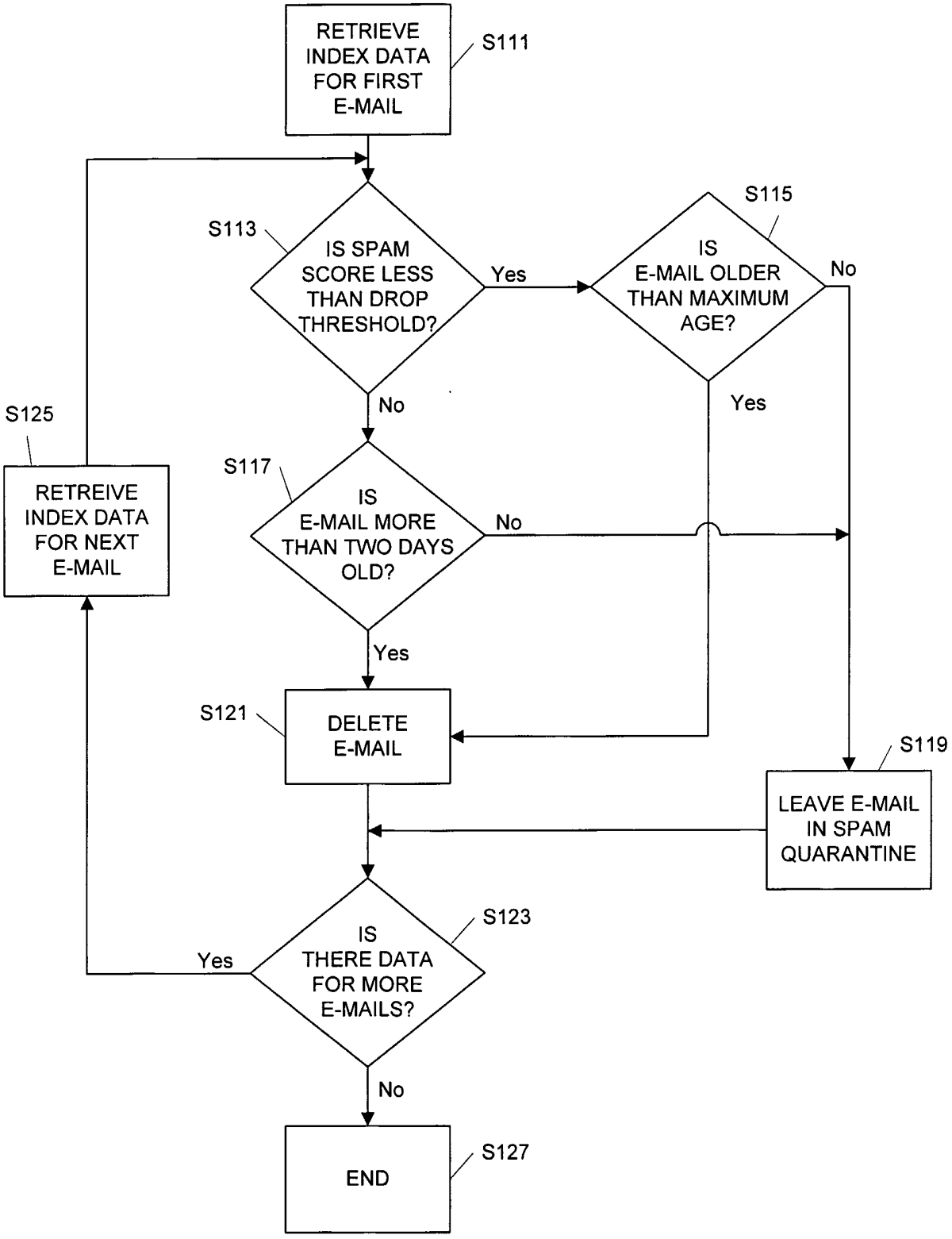

RETRIEVE INDEX DATA FOR FIRST E-MAIL
S111
S113
IS SPAM SCORE LESS THAN DROP THRESHOLD?
Yes
S115
IS E-MAIL OLDER THAN MAXIMUM AGE?
No
No
Yes
S125
RETREIVE INDEX DATA FOR NEXT E-MAIL
S117
IS E-MAIL MORE THAN TWO DAYS OLD?
No
Yes
S121
DELETE E-MAIL
S119
LEAVE E-MAIL IN SPAM QUARANTINE
S123
IS THERE DATA FOR MORE E-MAILS?
Yes
No
S127
END

FIG. 15

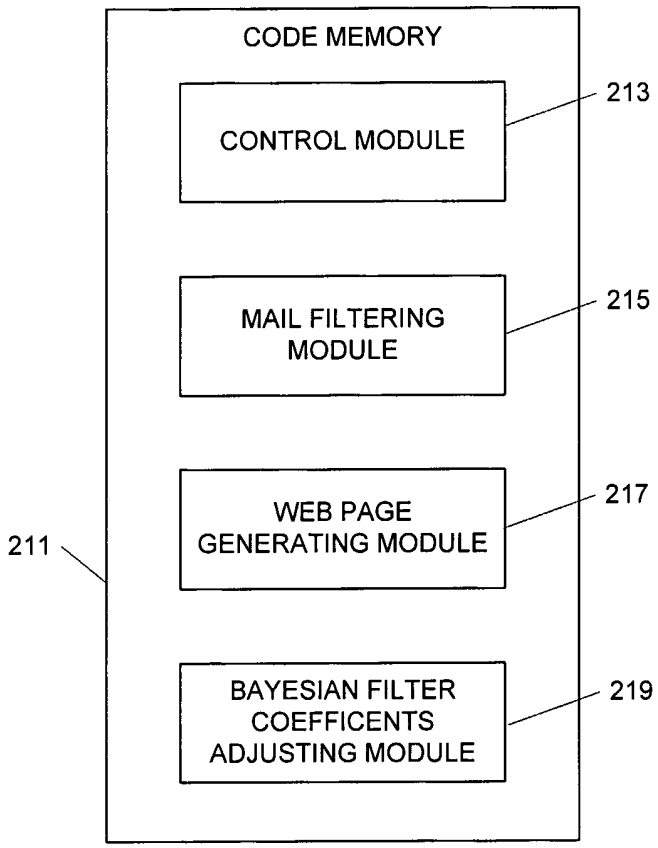

CODE MEMORY
CONTROL MODULE
213
MAIL FILTERING MODULE
215
WEB PAGE GENERATING MODULE
217
211
BAYESIAN FILTER COEFFICENTS ADJUSTING MODULE
219

FIG. 16

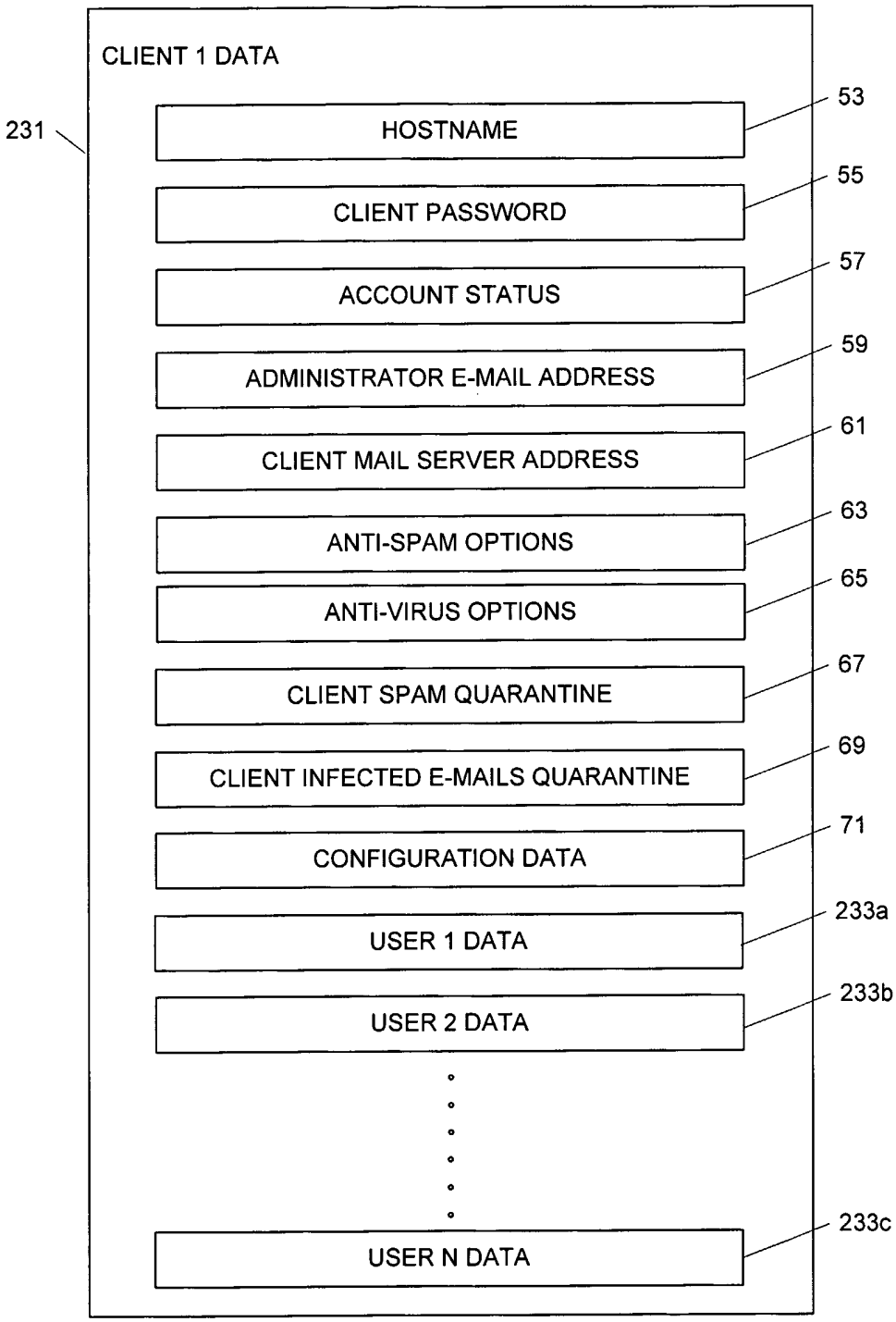
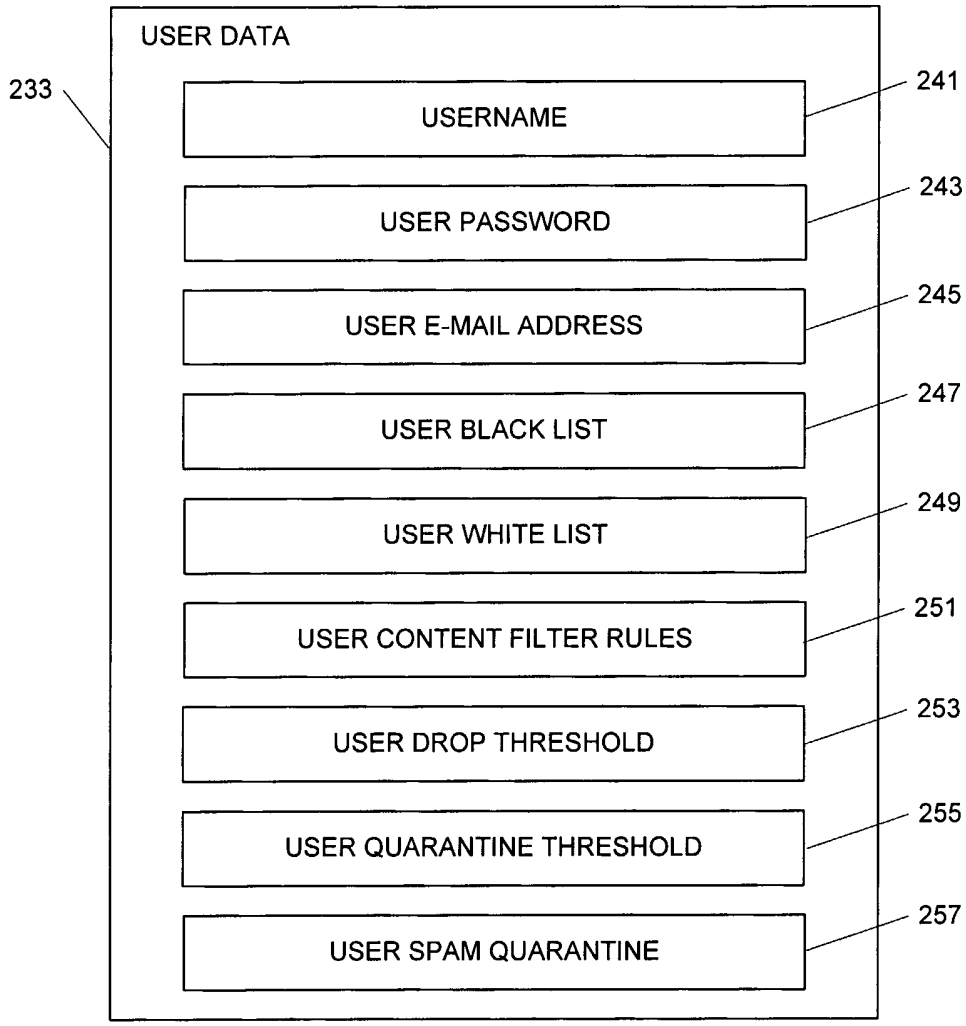

CLIENT 1 DATA
231
HOSTNAME
53
CLIENT PASSWORD
55
ACCOUNT STATUS
57
ADMINISTRATOR E-MAIL ADDRESS
59
CLIENT MAIL SERVER ADDRESS
61
ANTI-SPAM OPTIONS
63
ANTI-VIRUS OPTIONS
65
CLIENT SPAM QUARANTINE
67
CLIENT INFECTED E-MAILS QUARANTINE
69
CONFIGURATION DATA
71
USER 1 DATA
233a
USER 2 DATA
233b
USER N DATA
233c

FIG. 17


USER DATA
233
USERNAME
241
USER PASSWORD
243
USER E-MAIL ADDRESS
245
USER BLACK LIST
247
USER WHITE LIST
249
USER CONTENT FILTER RULES
251
USER DROP THRESHOLD
253
USER QUARANTINE THRESHOLD
255
USER SPAM QUARANTINE
257

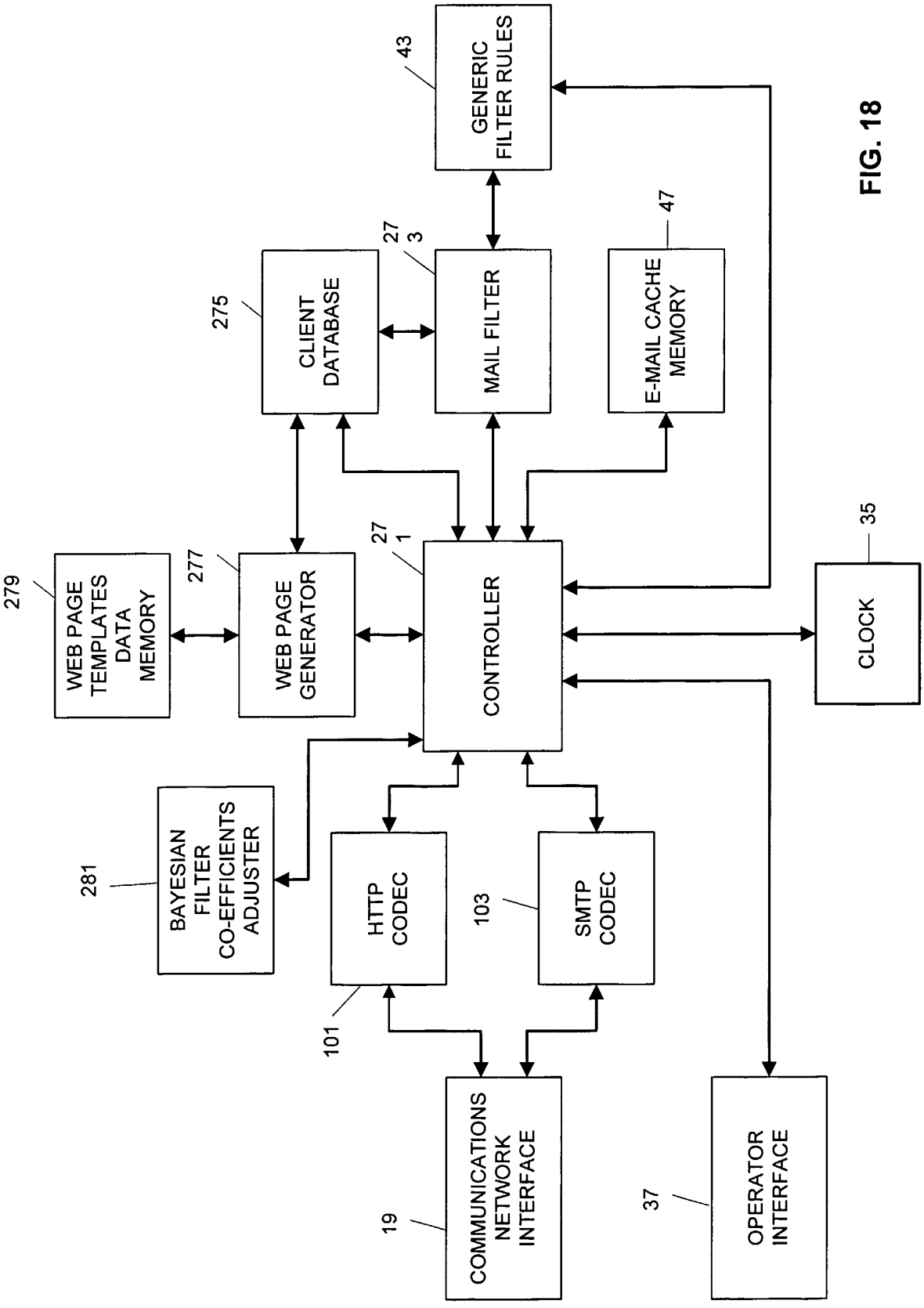

GENERIC FILTER RULES
43
CLIENT DATABASE
275
MAIL FILTER
273
E-MAIL CACHE MEMORY
47
WEB PAGE TEMPLATES DATA MEMORY
279
WEB PAGE GENERATOR
277
CONTROLLER
271
CLOCK
35
BAYESIAN FILTER CO-EFFICIENTS ADJUSTER
281
HTTP CODEC
101
SMTP CODEC
103
COMMUNICATIONS NETWORK INTERFACE
19
OPERATOR INTERFACE
37

FIG. 18

FIG. 19A

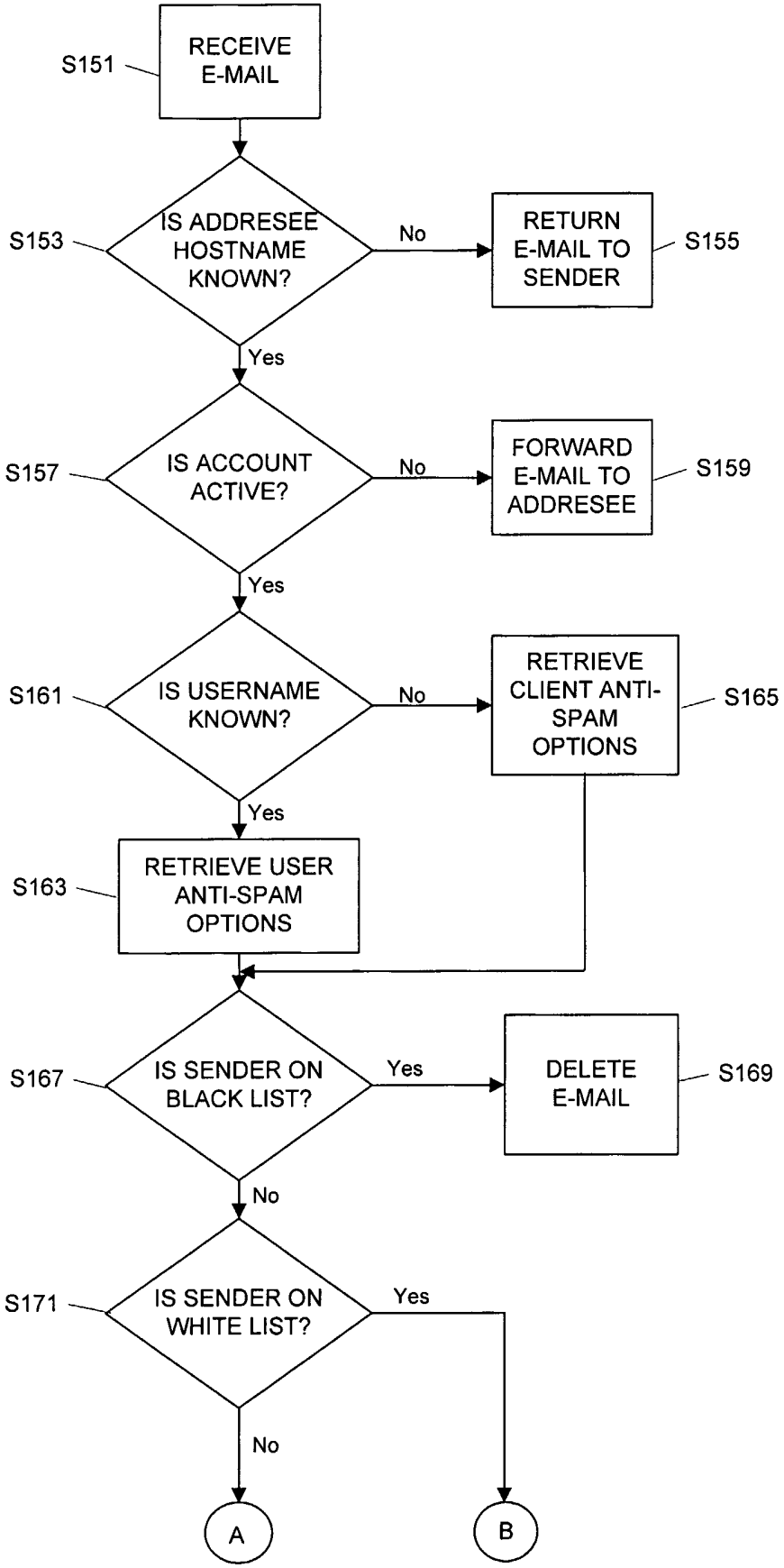

S151
RECEIVE E-MAIL
S153
IS ADDRESEE HOSTNAME KNOWN?
No
RETURN E-MAIL TO SENDER
S155
Yes
S157
IS ACCOUNT ACTIVE?
No
FORWARD E-MAIL TO ADDRESEE
S159
Yes
S161
IS USERNAME KNOWN?
No
RETRIEVE CLIENT ANTI-SPAM OPTIONS
S165
Yes
S163
RETRIEVE USER ANTI-SPAM OPTIONS
S167
IS SENDER ON BLACK LIST?
Yes
DELETE E-MAIL
S169
No
S171
IS SENDER ON WHITE LIST?
Yes
No
A
B

FIG. 19B

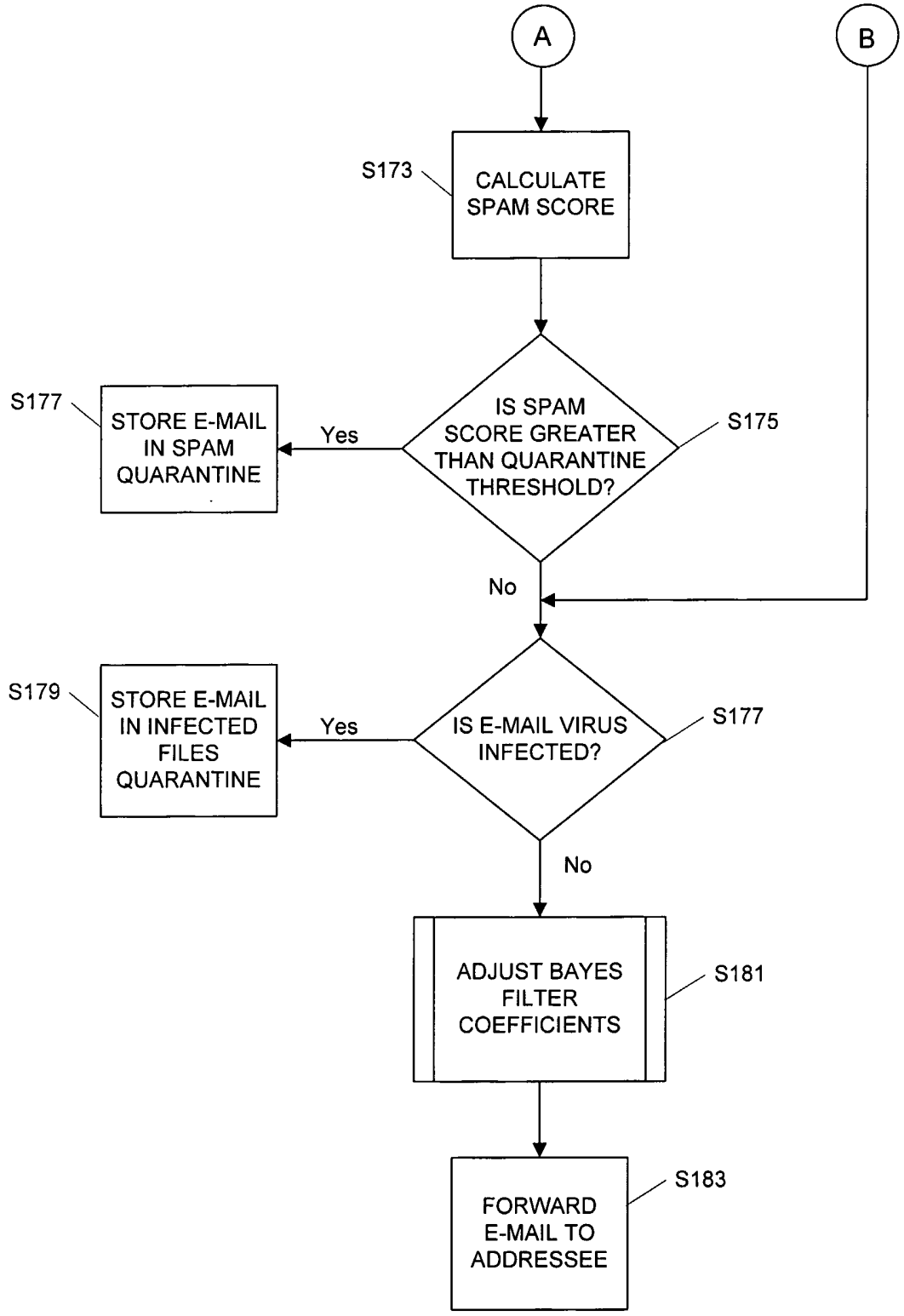

A
B
S173
CALCULATE SPAM SCORE
IS SPAM SCORE GREATER THAN QUARANTINE THRESHOLD?
S175
Yes
S177
STORE E-MAIL IN SPAM QUARANTINE
No
IS E-MAIL VIRUS INFECTED?
S177
Yes
S179
STORE E-MAIL IN INFECTED FILES QUARANTINE
No
ADJUST BAYES FILTER COEFFICIENTS
S181
FORWARD E-MAIL TO ADDRESSEE
S183

FIG. 20

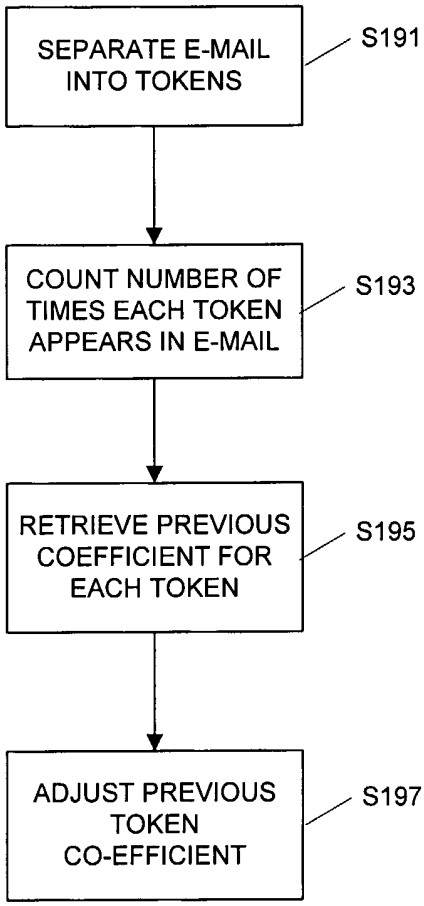

SEPARATE E-MAIL INTO TOKENS
S191
COUNT NUMBER OF TIMES EACH TOKEN APPEARS IN E-MAIL
S193
RETRIEVE PREVIOUS COEFFICIENT FOR EACH TOKEN
S195
ADJUST PREVIOUS TOKEN CO-EFFICIENT
S197

FIG. 21

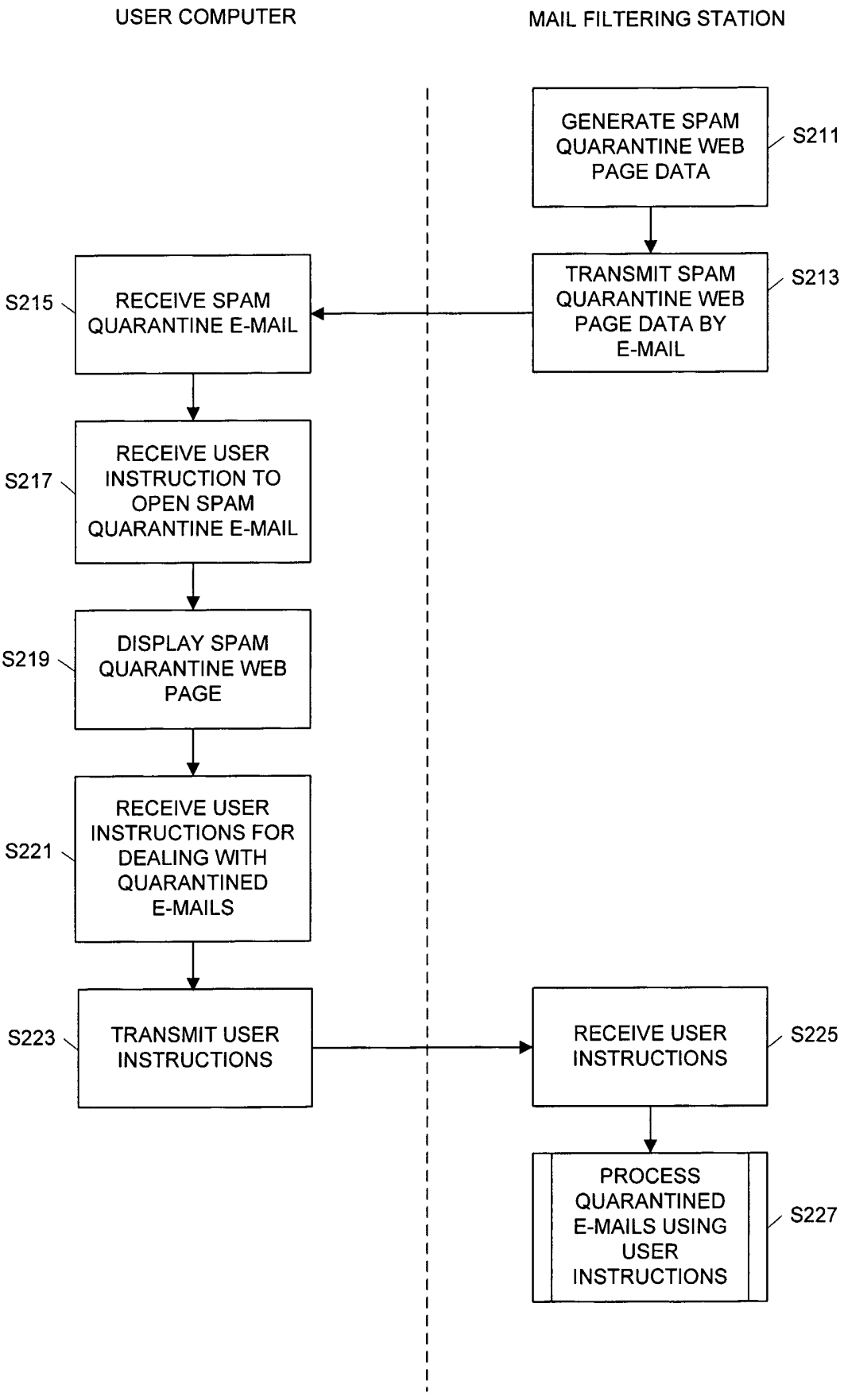

USER COMPUTER
MAIL FILTERING STATION
GENERATE SPAM QUARANTINE WEB PAGE DATA
S211
TRANSMIT SPAM QUARANTINE WEB PAGE DATA BY E-MAIL
S213
S215
RECEIVE SPAM QUARANTINE E-MAIL
S217
RECEIVE USER INSTRUCTION TO OPEN SPAM QUARANTINE E-MAIL
S219
DISPLAY SPAM QUARANTINE WEB PAGE
S221
RECEIVE USER INSTRUCTIONS FOR DEALING WITH QUARANTINED E-MAILS
S223
TRANSMIT USER INSTRUCTIONS
RECEIVE USER INSTRUCTIONS
S225
PROCESS QUARANTINED E-MAILS USING USER INSTRUCTIONS
S227

FIG. 22

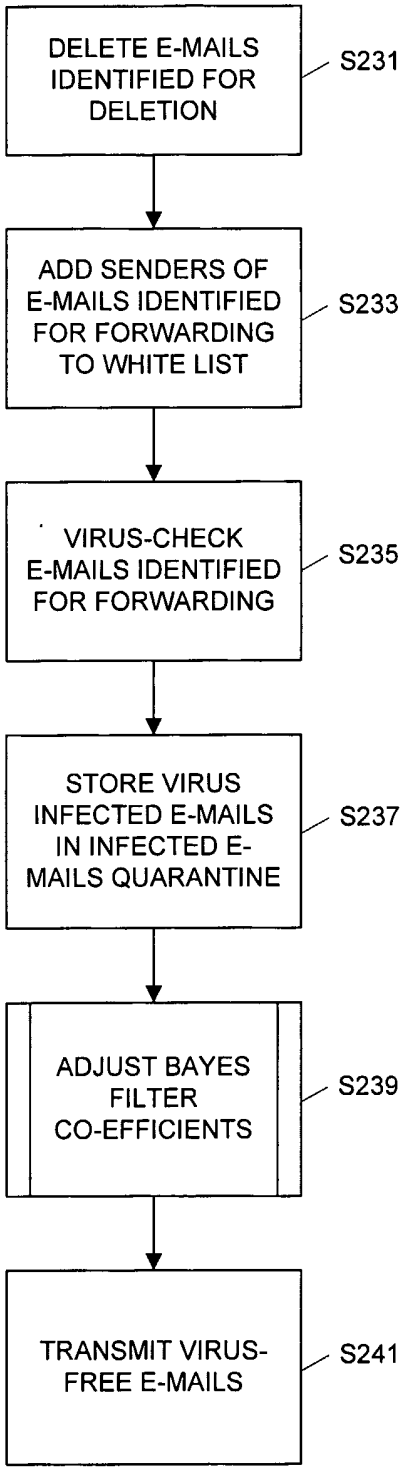

DELETE E-MAILS IDENTIFIED FOR DELETION
S231
ADD SENDERS OF E-MAILS IDENTIFIED FOR FORWARDING TO WHITE LIST
S233
VIRUS-CHECK E-MAILS IDENTIFIED FOR FORWARDING
S235
STORE VIRUS INFECTED E-MAILS IN INFECTED E-MAILS QUARANTINE
S237
ADJUST BAYES FILTER CO-EFFICIENTS
S239
TRANSMIT VIRUS-FREE E-MAILS
S241

FIG. 23

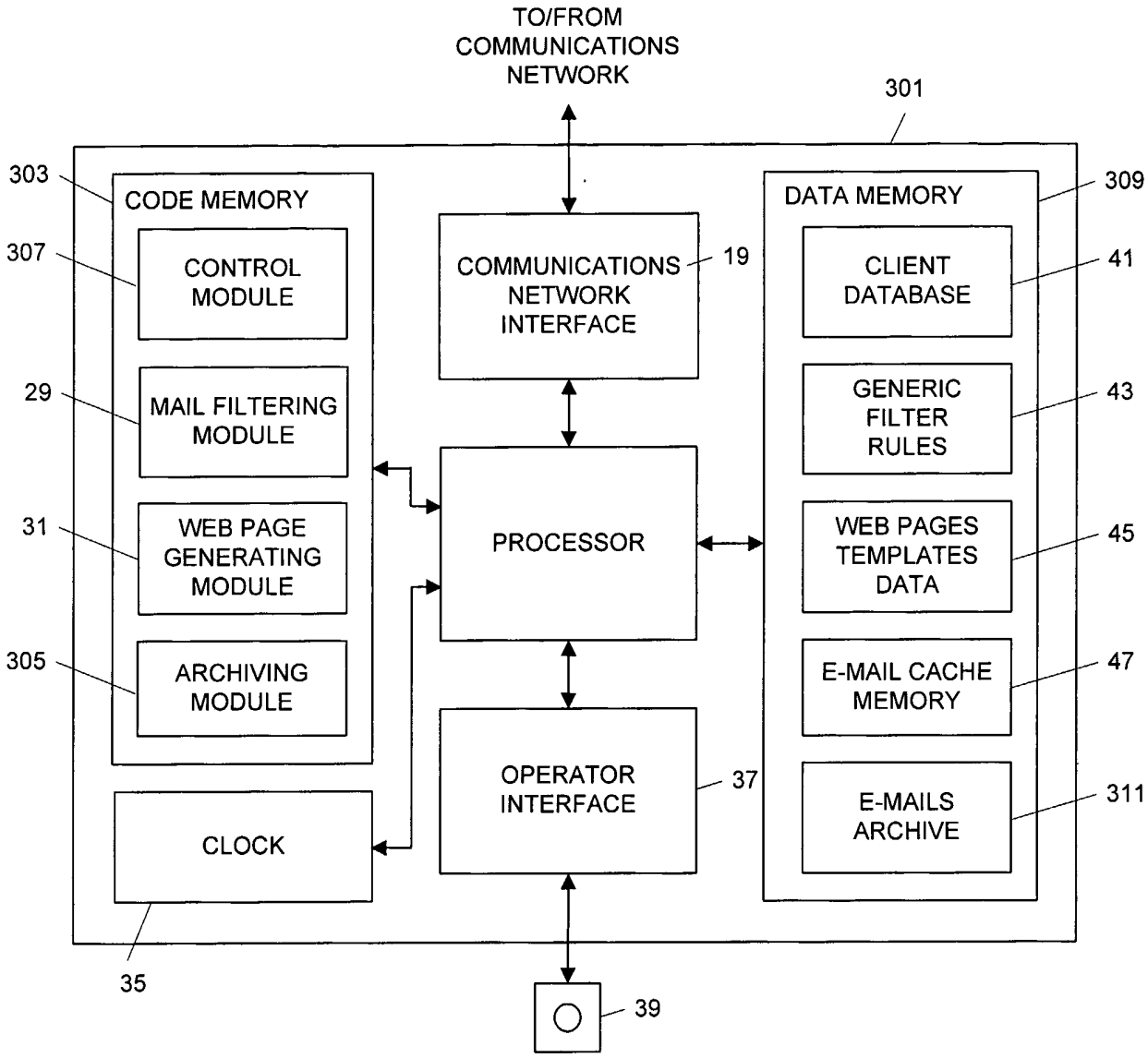

TO/FROM COMMUNICATIONS NETWORK
301
303
CODE MEMORY
307
CONTROL MODULE
29
MAIL FILTERING MODULE
31
WEB PAGE GENERATING MODULE
305
ARCHIVING MODULE
CLOCK
35
COMMUNICATIONS NETWORK INTERFACE
19
PROCESSOR
OPERATOR INTERFACE
37
39
DATA MEMORY
309
CLIENT DATABASE
41
GENERIC FILTER RULES
43
WEB PAGES TEMPLATES DATA
45
E-MAIL CACHE MEMORY
47
E-MAILS ARCHIVE
311

FIG. 24

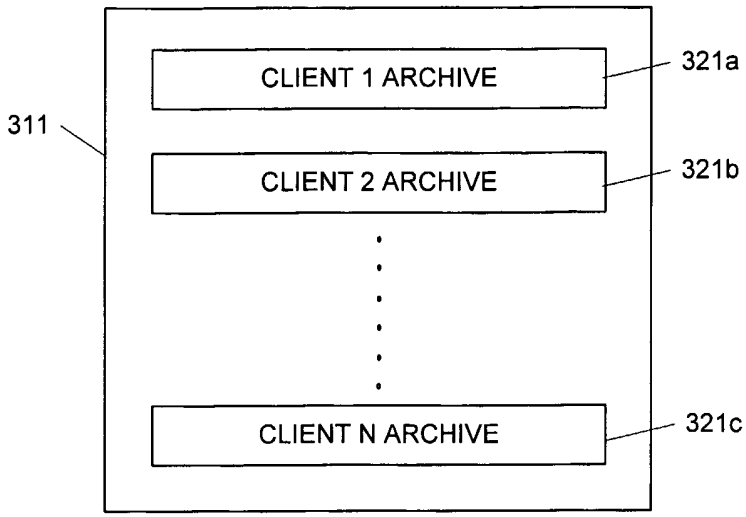
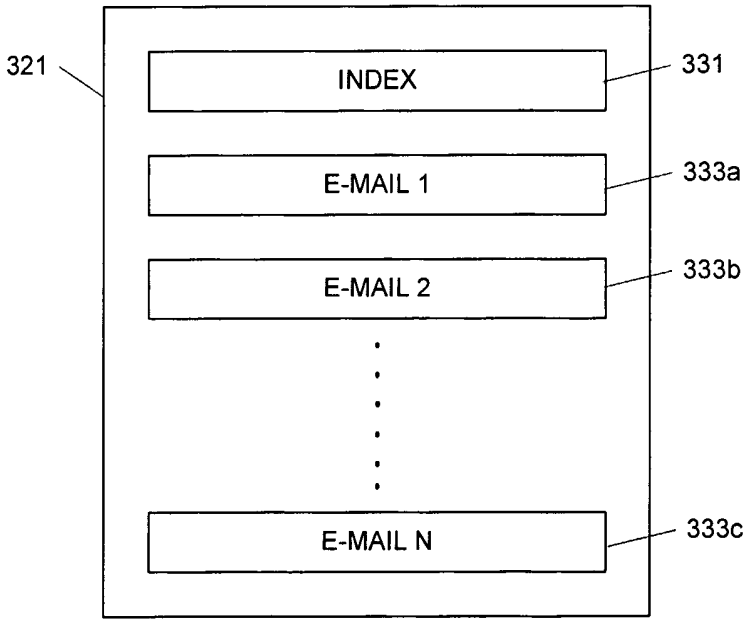

311
CLIENT 1 ARCHIVE
321a
CLIENT 2 ARCHIVE
321b
CLIENT N ARCHIVE
321c

FIG. 25


321
INDEX
331
E-MAIL 1
333a
E-MAIL 2
333b
E-MAIL N
333c

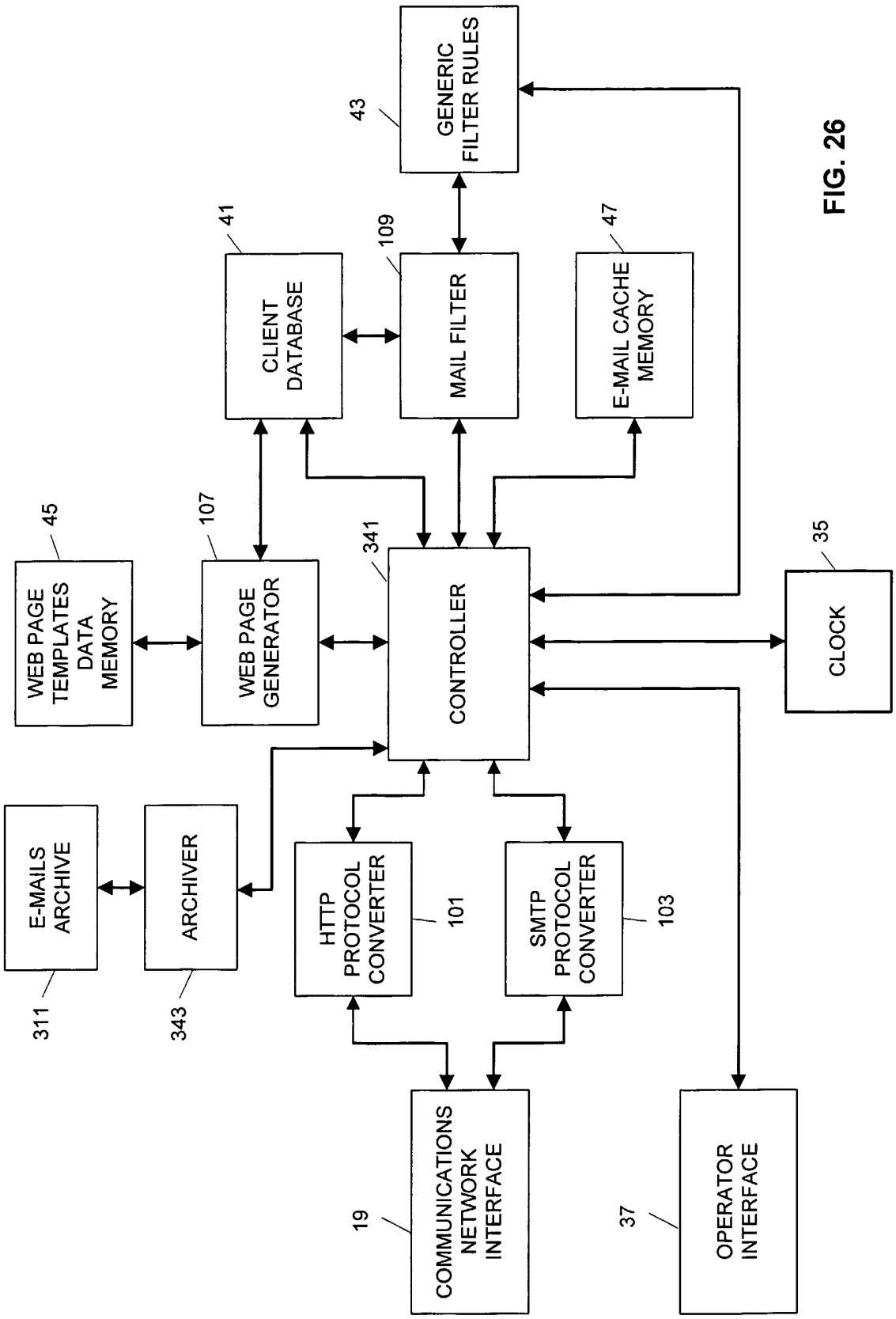

GENERIC FILTER RULES
43
CLIENT DATABASE
41
MAIL FILTER
109
E-MAIL CACHE MEMORY
47
WEB PAGE TEMPLATES DATA MEMORY
45
WEB PAGE GENERATOR
107
CONTROLLER
341
CLOCK
35
E-MAILS ARCHIVE
311
ARCHIVER
343
HTTP PROTOCOL CONVERTER
101
SMTP PROTOCOL CONVERTER
103
COMMUNICATIONS NETWORK INTERFACE
19
OPERATOR INTERFACE
37

FIG. 26

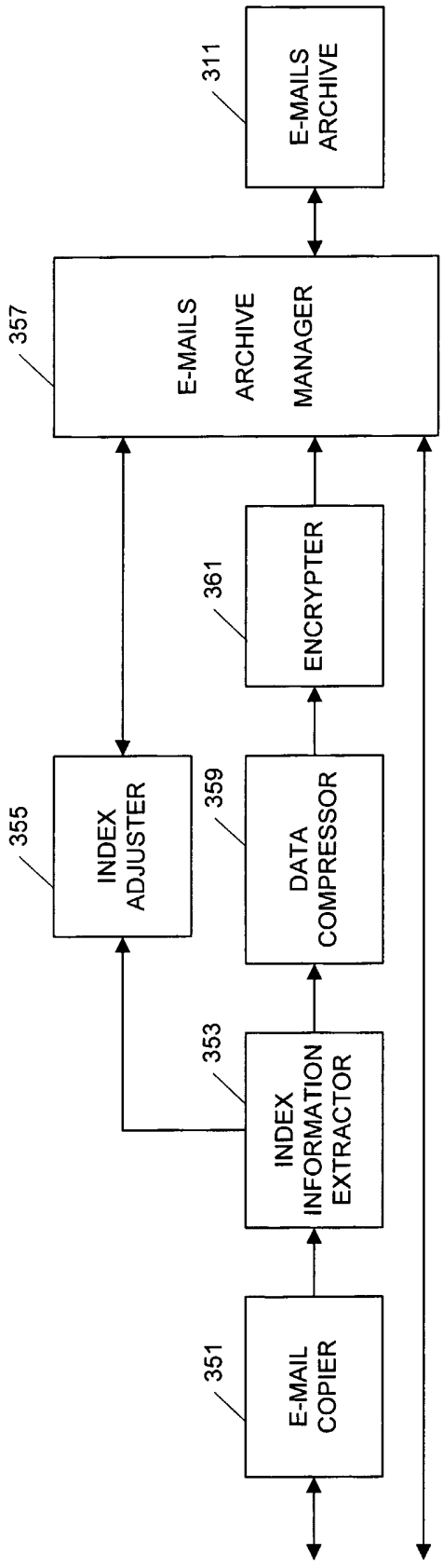

311
E-MAILS ARCHIVE
357
E-MAILS ARCHIVE MANAGER
361
ENCRYPTER
355
INDEX ADJUSTER
359
DATA COMPRESSOR
353
INDEX INFORMATION EXTRACTOR
351
E-MAIL COPIER

FIG. 27

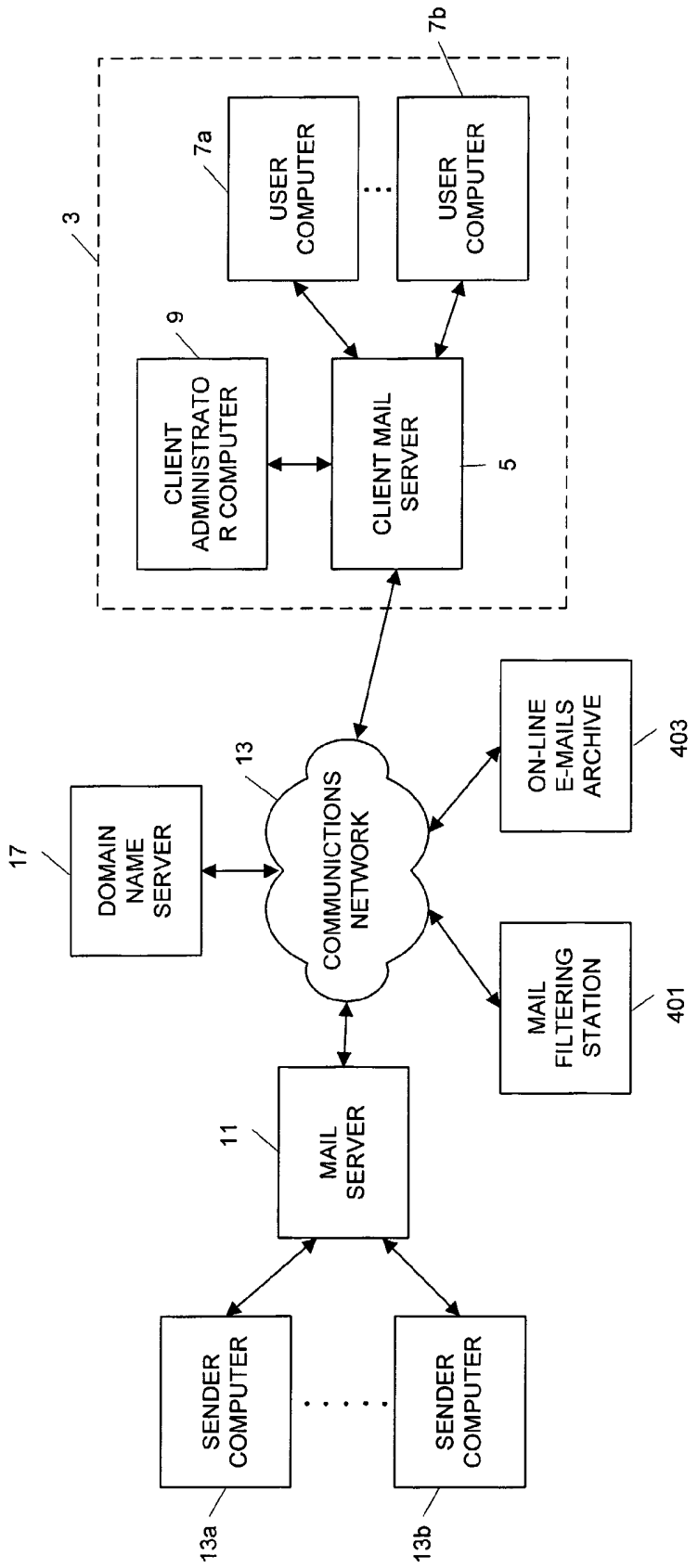

3
7a
USER COMPUTER
USER COMPUTER
7b
9
CLIENT ADMINISTRATOR COMPUTER
CLIENT MAIL SERVER
5
13
COMMUNICTIONS NETWORK
ON-LINE E-MAILS ARCHIVE
403
17
DOMAIN NAME SERVER
MAIL FILTERING STATION
401
11
MAIL SERVER
SENDER COMPUTER
SENDER COMPUTER
13a
13b

FIG. 28

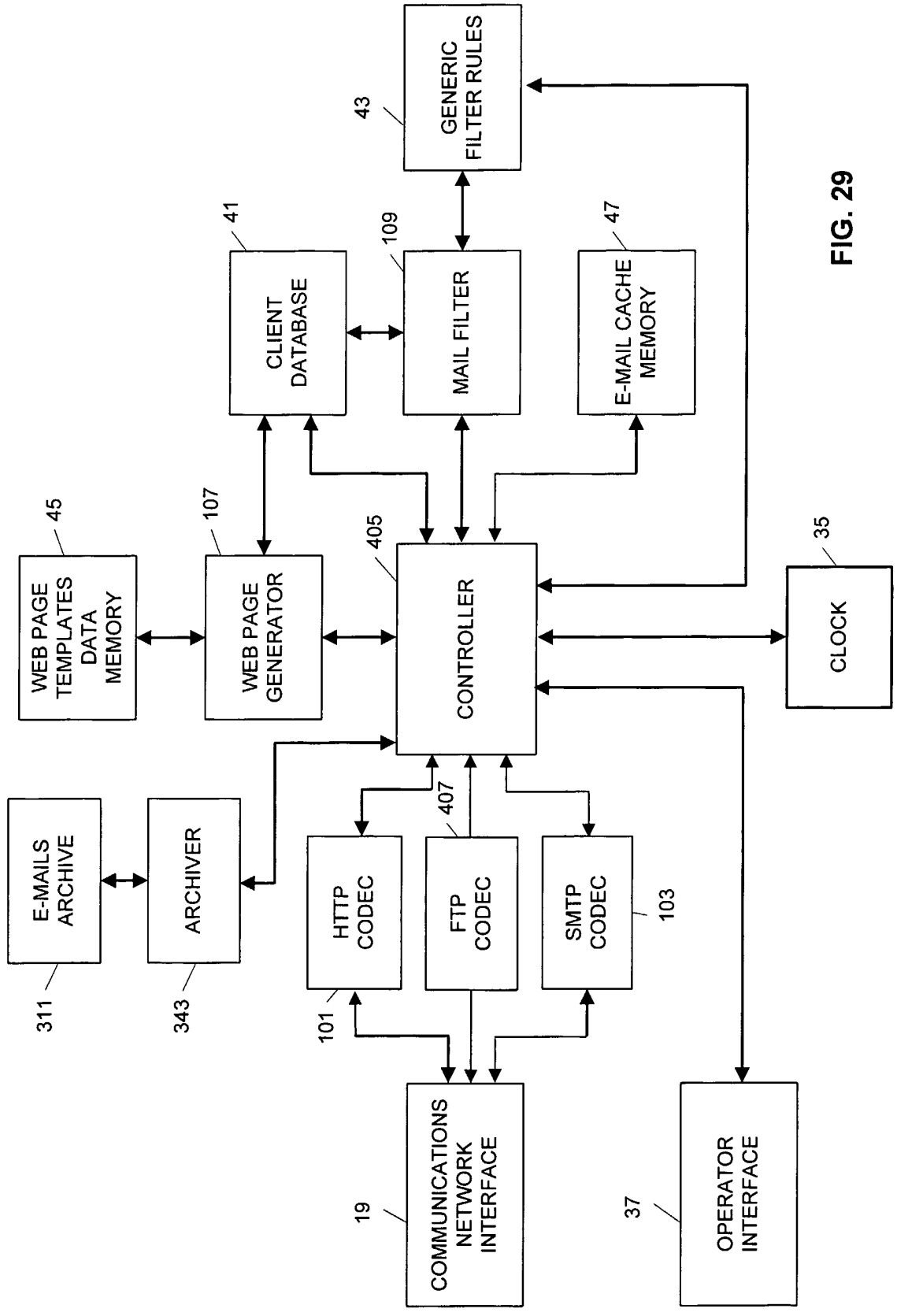

GENERIC FILTER RULES
43
CLIENT DATABASE
41
MAIL FILTER
109
E-MAIL CACHE MEMORY
47
WEB PAGE TEMPLATES DATA MEMORY
45
WEB PAGE GENERATOR
107
CONTROLLER
405
CLOCK
35
E-MAILS ARCHIVE
311
ARCHIVER
343
HTTP CODEC
FTP CODEC
407
SMTP CODEC
103
101
COMMUNICATIONS NETWORK INTERFACE
19
OPERATOR INTERFACE
37

FIG. 29

FIG. 30

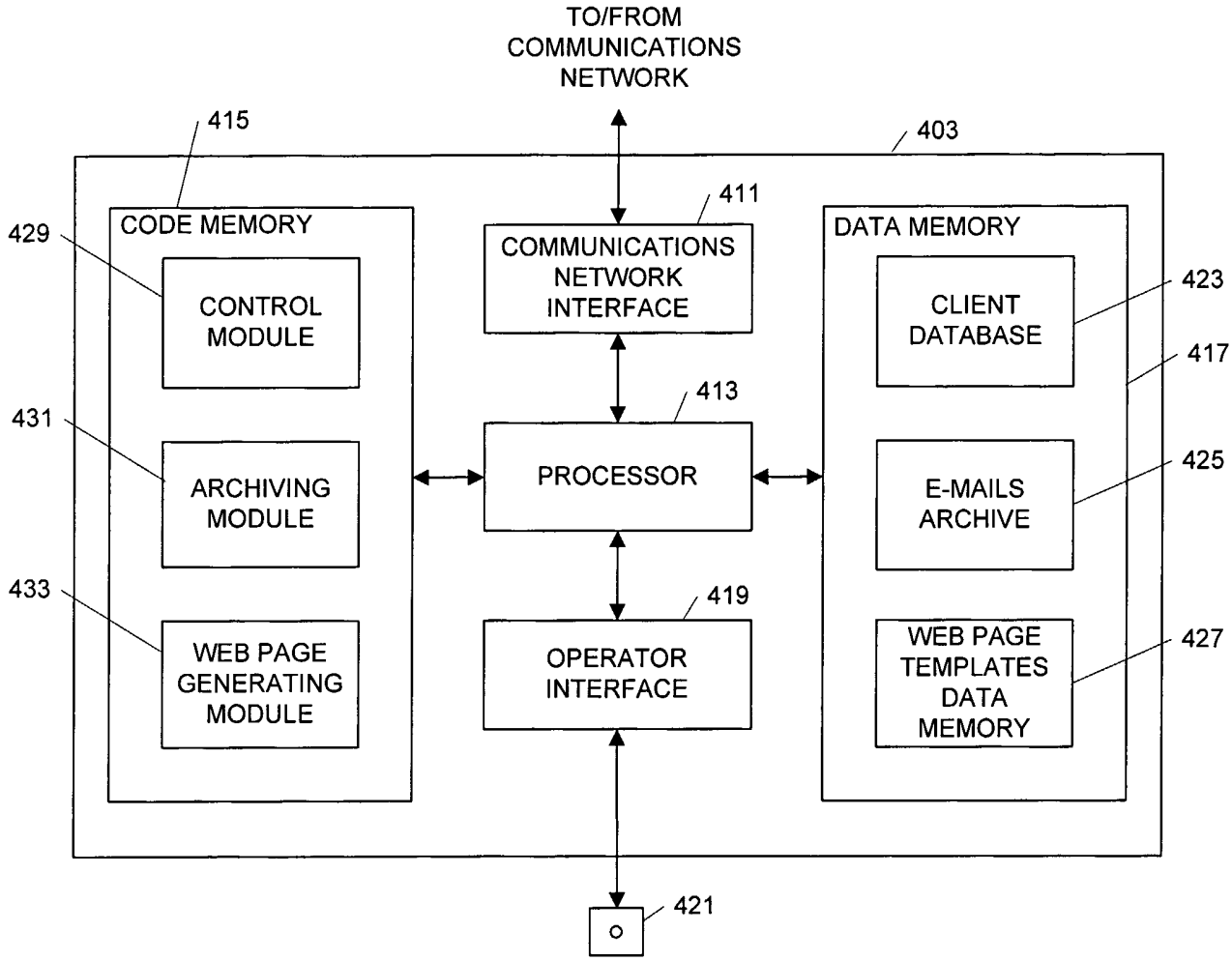
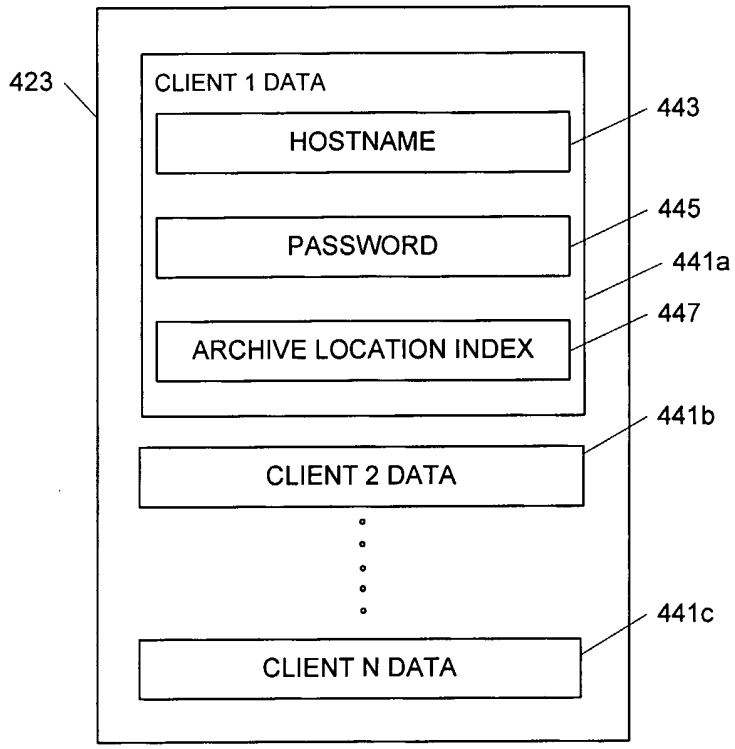

TO/FROM COMMUNICATIONS NETWORK
415
403
411
CODE MEMORY
429
CONTROL MODULE
COMMUNICATIONS NETWORK INTERFACE
DATA MEMORY
CLIENT DATABASE
423
417
413
431
ARCHIVING MODULE
PROCESSOR
E-MAILS ARCHIVE
425
433
419
WEB PAGE GENERATING MODULE
OPERATOR INTERFACE
WEB PAGE TEMPLATES DATA MEMORY
427
421

FIG. 31


423
CLIENT 1 DATA
HOSTNAME
PASSWORD
ARCHIVE LOCATION INDEX
CLIENT 2 DATA
CLIENT N DATA
443
445
441a
447
441b
441c

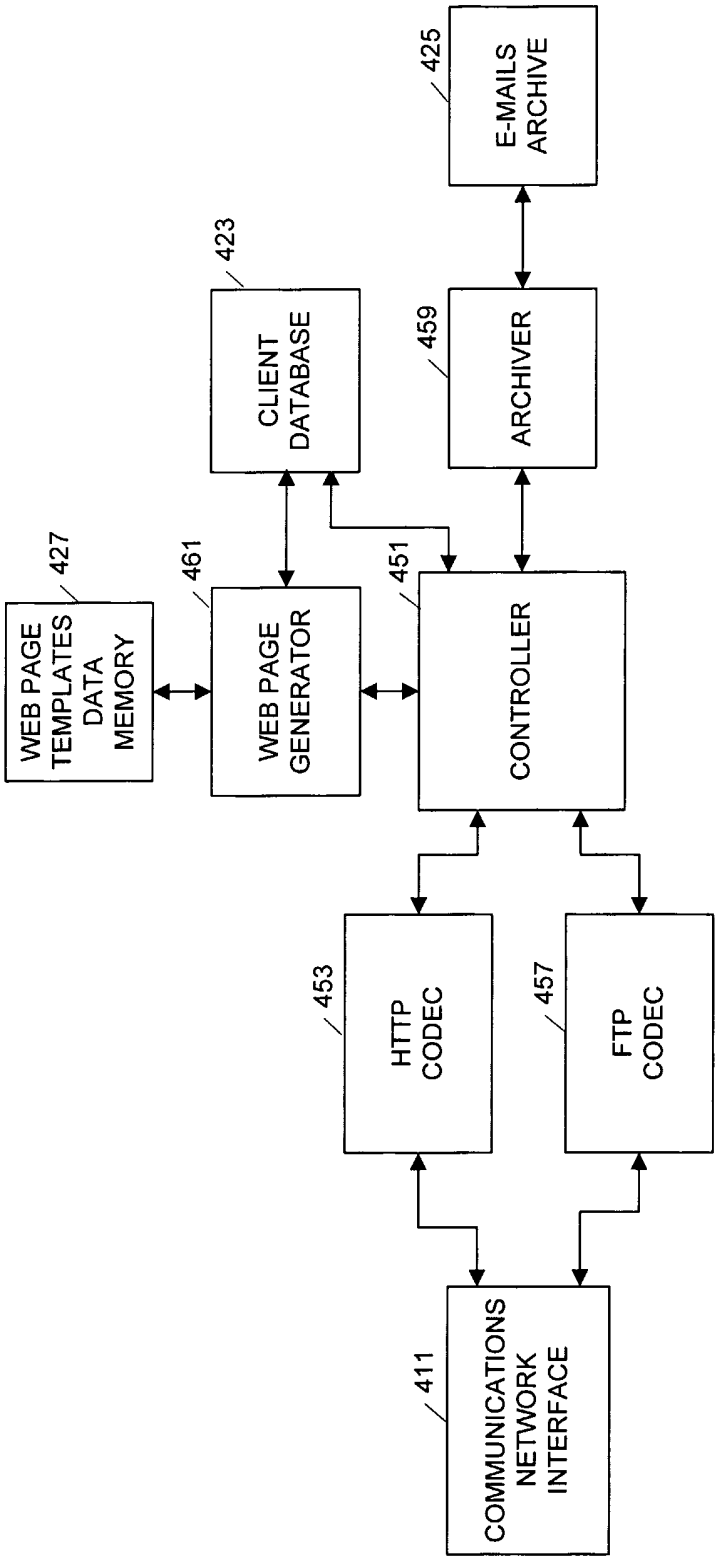

425
E-MAILS ARCHIVE
423
CLIENT DATABASE
459
ARCHIVER
427
WEB PAGE TEMPLATES DATA MEMORY
461
WEB PAGE GENERATOR
451
CONTROLLER
453
HTTP CODEC
457
FTP CODEC
411
COMMUNICATIONS NETWORK INTERFACE

FIG. 32

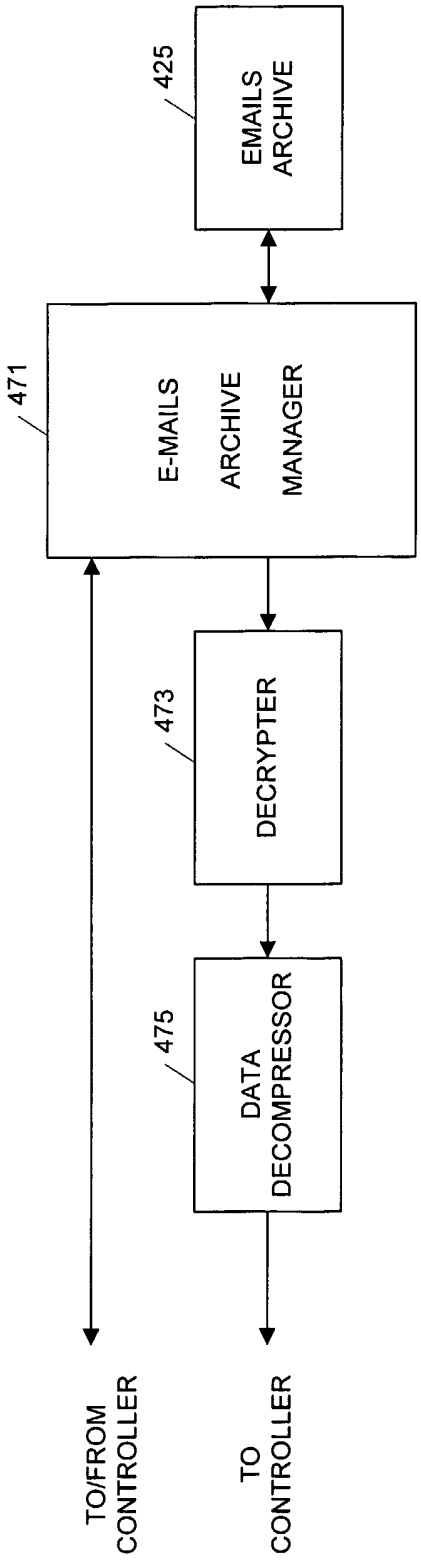

425
EMAILS ARCHIVE
471
E-MAILS ARCHIVE MANAGER
473
DECRYPTER
475
DATA DECOMPRESSOR
TO/FROM CONTROLLER
TO CONTROLLER

FIG. 33

FIG. 34

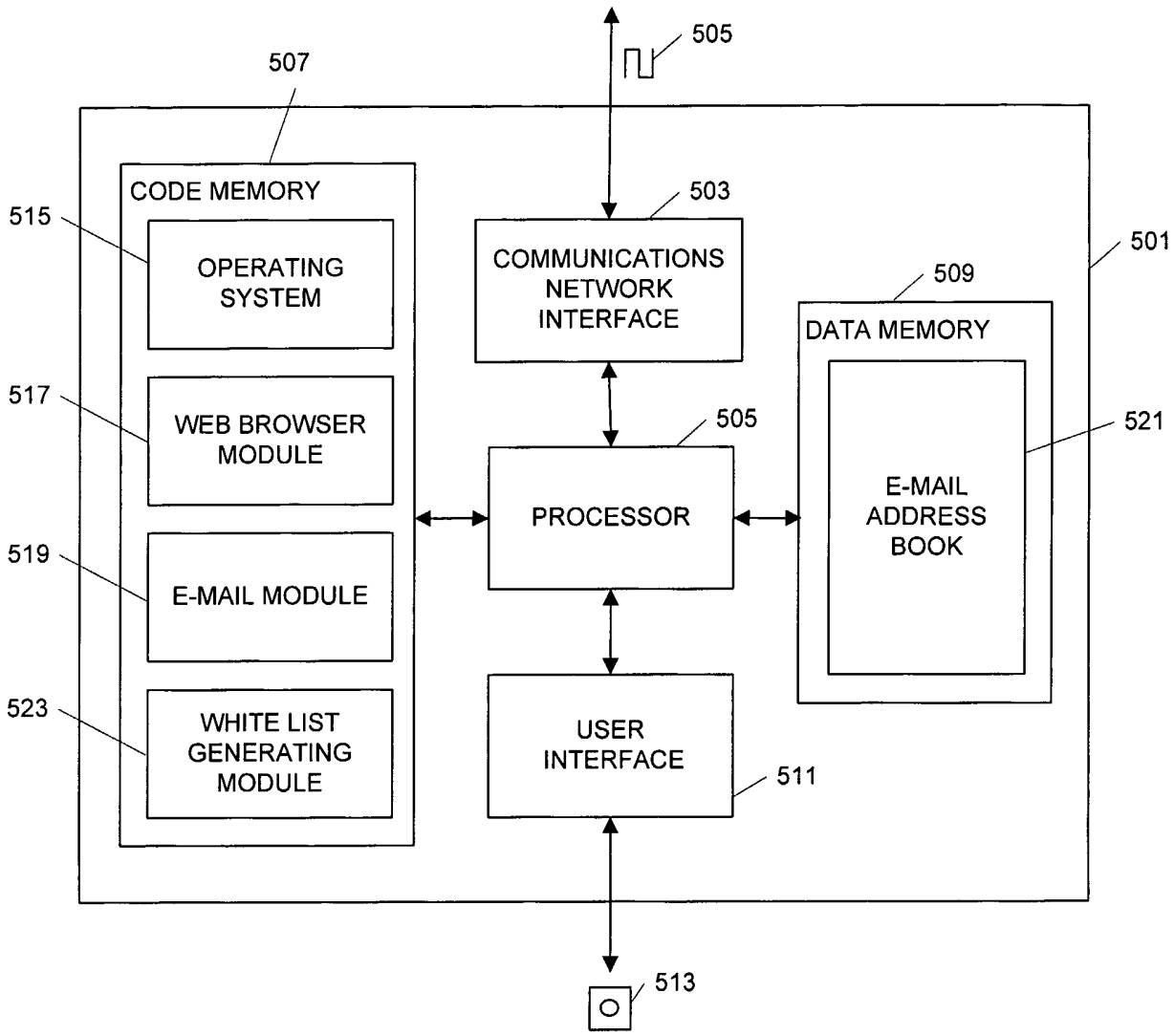

505
507
CODE MEMORY
515
OPERATING SYSTEM
517
WEB BROWSER MODULE
519
E-MAIL MODULE
523
WHITE LIST GENERATING MODULE
503
COMMUNICATIONS NETWORK INTERFACE
505
PROCESSOR
USER INTERFACE
511
513
501
509
DATA MEMORY
521
E-MAIL ADDRESS BOOK

FIG. 35

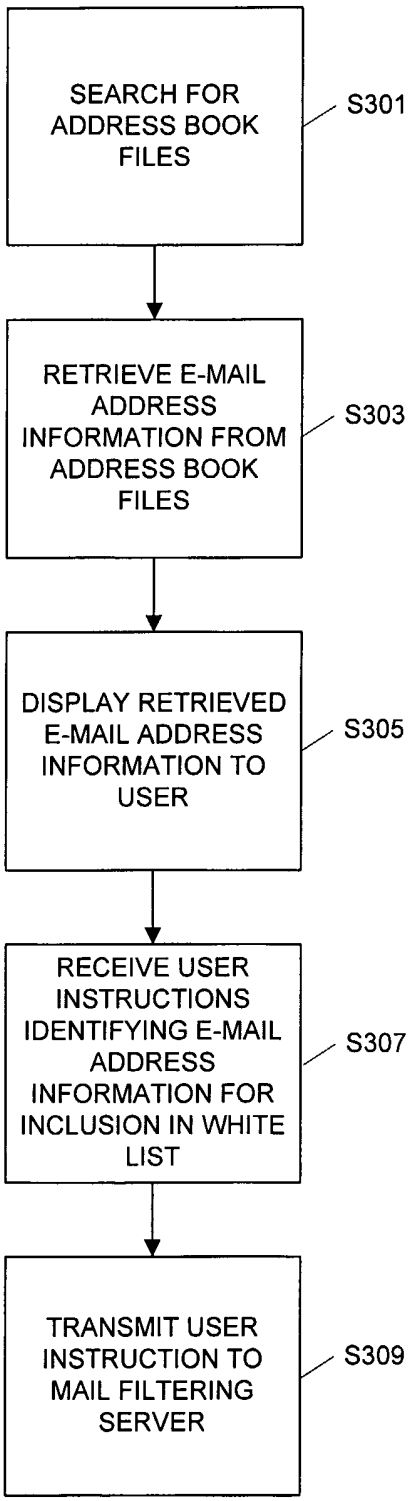
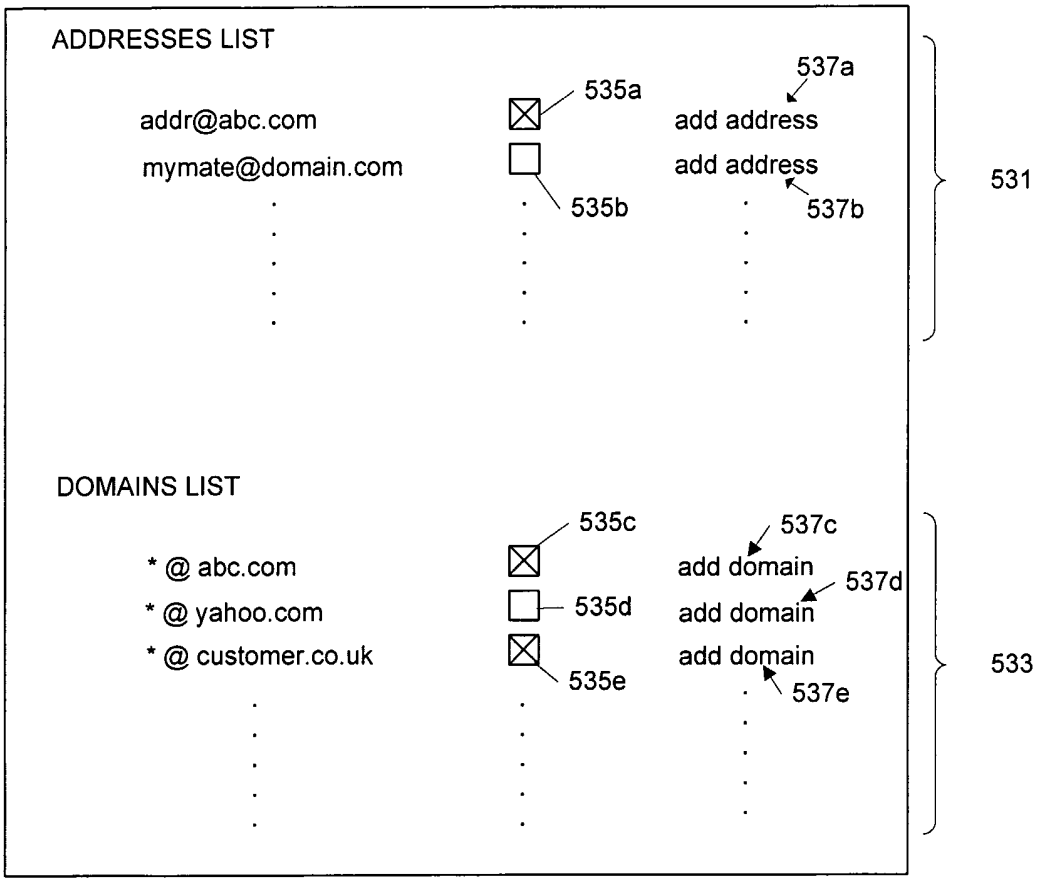

SEARCH FOR ADDRESS BOOK FILES
S301
RETRIEVE E-MAIL ADDRESS INFORMATION FROM ADDRESS BOOK FILES
S303
DISPLAY RETRIEVED E-MAIL ADDRESS INFORMATION TO USER
S305
RECEIVE USER INSTRUCTIONS IDENTIFYING E-MAIL ADDRESS INFORMATION FOR INCLUSION IN WHITE LIST
S307
TRANSMIT USER INSTRUCTION TO MAIL FILTERING SERVER
S309

FIG. 36


ADDRESSES LIST
addr@abc.com
mymate@domain.com
535a
535b
537a
add address
add address
537b
531
DOMAINS LIST
* @ abc.com
* @ yahoo.com
* @ customer.co.uk
535c
535d
535e
537c
add domain
add domain
add domain
537d
537e
533

INTERNATIONAL SEARCH REPORT

International Application No
PCT/RU 03/00476

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/58 G06F17/60

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)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/009526 A1 (BELLEGARDA JEROME R ET AL) 9 January 2003 (2003-01-09)	1-7, 12-14, 18,19, 42-57, 62-64, 68,69, 92-98
	paragraph '0039! - paragraph '0041! paragraph '0050!; figure 1	
Y		8-11, 15-17, 23-33, 41, 58-61, 65-67, 73-83,91

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° 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 document 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
31 August 2004	07/09/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ströbeck, A.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/RU 03/00476

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/023692 A1 (MOROO JUN) 30 January 2003 (2003-01-30) paragraph '0032! - paragraph '0036! paragraph '0046! - paragraph '0048! paragraph '0077!	20,21, 34-40, 70,71, 84-90
Y		8-11, 15-17, 22,41, 58-61, 65-67, 72,91
Y	US 6 161 130 A (HORVITZ ERIC ET AL) 12 December 2000 (2000-12-12) column 9, line 18 - column 10, line 31 column 13, line 17 - line 29 column 14, line 40 - line 42 column 15, line 10 - line 17	22-33, 72-83
A	GRAHAM P: "A Plan for Spam"'Online! August 2002 (2002-08), XP002273602 Retrieved from the Internet: URL:www.paulgraham.com/spam.html> the whole document	1-98
A	US 6 052 709 A (PAUL SUNIL) 18 April 2000 (2000-04-18) column 5, line 47 - line 62 column 9, line 5 - line 21	23-33, 73-83
A	US 2002/199095 A1 (BANDINI JEAN-CHRISTOPHE ET AL) 26 December 2002 (2002-12-26) paragraph '0019! - paragraph '0021!	46,47, 96,97
A	US 2002/116463 A1 (HART MATTHEW THOMAS) 22 August 2002 (2002-08-22) paragraphs '0037!, '0038!	34-41, 84-91

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/RU 03/00476

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003009526 A1	09-01-2003	EP 1397768 A1	17-03-2004
		WO 02103604 A1	27-12-2002
US 2003023692 A1	30-01-2003	JP 2003046576 A	14-02-2003
US 6161130 A	12-12-2000	EP 1090368 A1	11-04-2001
		WO 9967731 A1	29-12-1999
US 6052709 A	18-04-2000	AU 1631199 A	12-07-1999
		EP 1040584 A2	04-10-2000
		JP 2001527257 T	25-12-2001
		WO 9933188 A2	01-07-1999
US 2002199095 A1	26-12-2002	US 6609196 B1	19-08-2003
		US 2003196098 A1	16-10-2003
		US 2002169954 A1	14-11-2002
		US 2004054886 A1	18-03-2004
		AU 8759098 A	16-02-1999
		CA 2301147 A1	04-02-1999
		EP 1010283 A2	21-06-2000
		JP 2001518724 T	16-10-2001
		WO 9905814 A2	04-02-1999
US 2002116463 A1	22-08-2002	NONE	