

(21) Application No: **0618187.9**  
(22) Date of Filing: **15.09.2006**  
(30) Priority Data:  
(31) **518876** (32) **16.09.2005** (33) **GB**  
(31) **523360** (32) **17.11.2005**  
(31) **604543** (32) **07.03.2006**  
(31) **605650** (32) **21.03.2006**  
(31) **605655** (32) **21.03.2006**  
(31) **613430** (32) **06.07.2006**  
(31) **613431** (32) **06.07.2006**

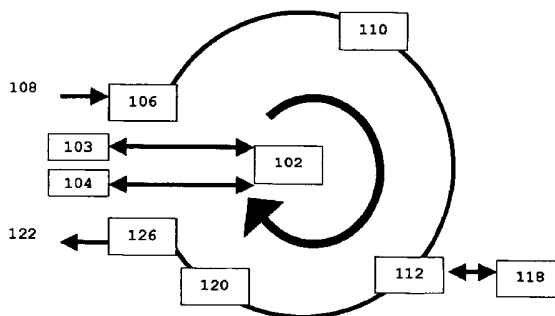
(51) INT CL:  
**H04L 12/58** (2006.01) **G06F 17/30** (2006.01)  
**G06Q 10/00** (2006.01)  
(52) UK CL (Edition X ):  
**G4A** AUSB AUXB  
(56) Documents Cited:  
**EP 1509014 A2** **WO 2004/003704 A2**  
**US 20040254988 A1** **US 20040133645 A1**  
(58) Field of Search:  
INT CL **H04L**  
Other: **Online: EPODOC, WPI**

(71) Applicant(s):  
**Jeroen Oostendorp**  
**Postbus 110, 7000 AC Doetinchem,**  
**Netherlands**  
(72) Inventor(s):  
**Jeroen Oostendorp**  
(74) Agent and/or Address for Service:  
**Stuart Harbron**  
**44 Swing Gate Lane, BERKHAMSTED,**  
**Hertfordshire, HP4 2LL, United Kingdom**

(54) Abstract Title: **Platform for message management**

(57) In a first aspect the present invention is a digital message filtering system that comprises a database module containing one or more configuration options relating to one or more end-users and a scanning engine module connected to the database module. The system also includes a message archiving system and a message prioritization system also connected to the database module. The message archiving system includes an auto-archiving engine whose behavior is determined by settings in said database so that if a particular message in a message steam 108 falls within criteria specified in said database a copy of said message is added to an auto-archive database. The behavior of the scanning engine module, the message archiving system and the message prioritization system are modified on a message-by-message basis according to the configuration options for the end-users. The digital message may be: IM for text and image messaging computer to computer, SMS for text messaging via mobile devices. VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax. In further aspects, the message filtering system may additionally include a set-up process so that a third party database may be synchronized as appropriate with the database module. The scanning engine module may additionally include a pre-filtering engine.

Figure 1



At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

Figure 1

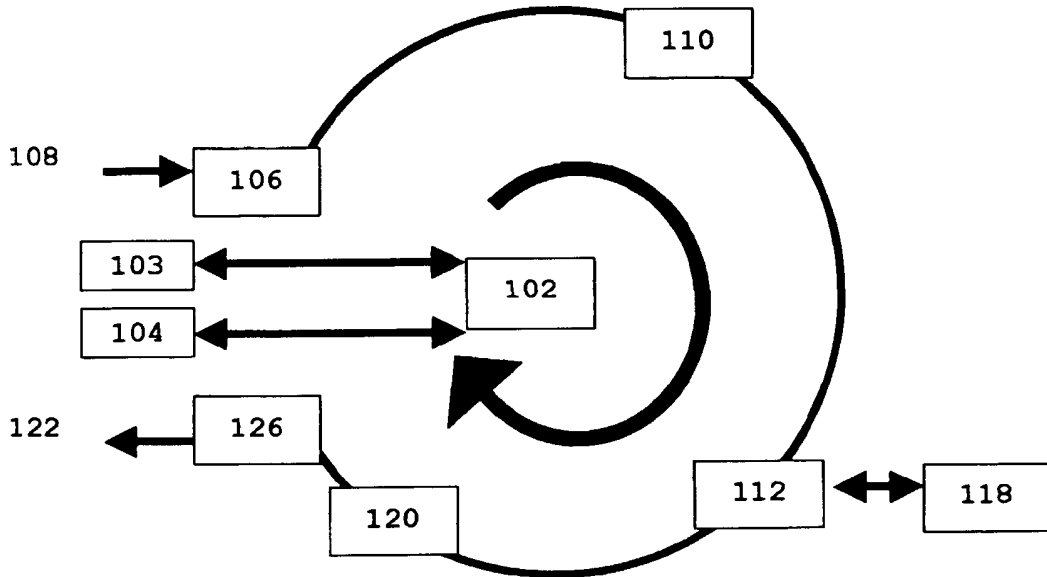


Figure 2

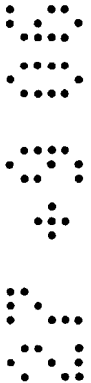
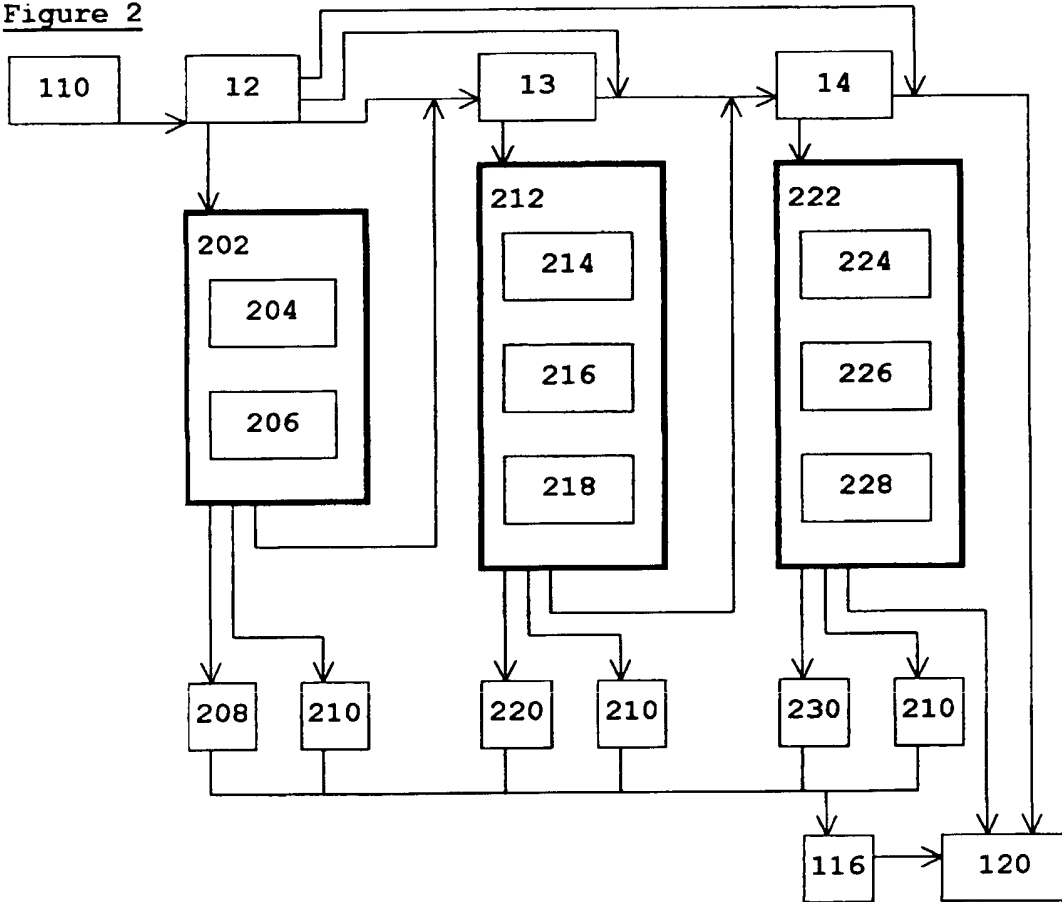


Figure 3a

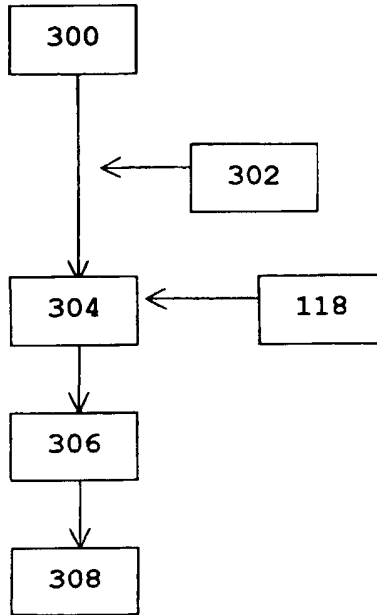


Figure 3b

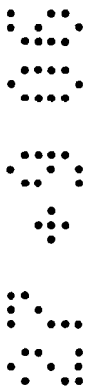
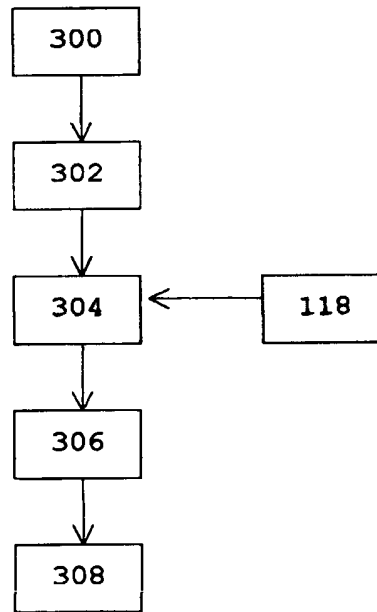


Figure 4

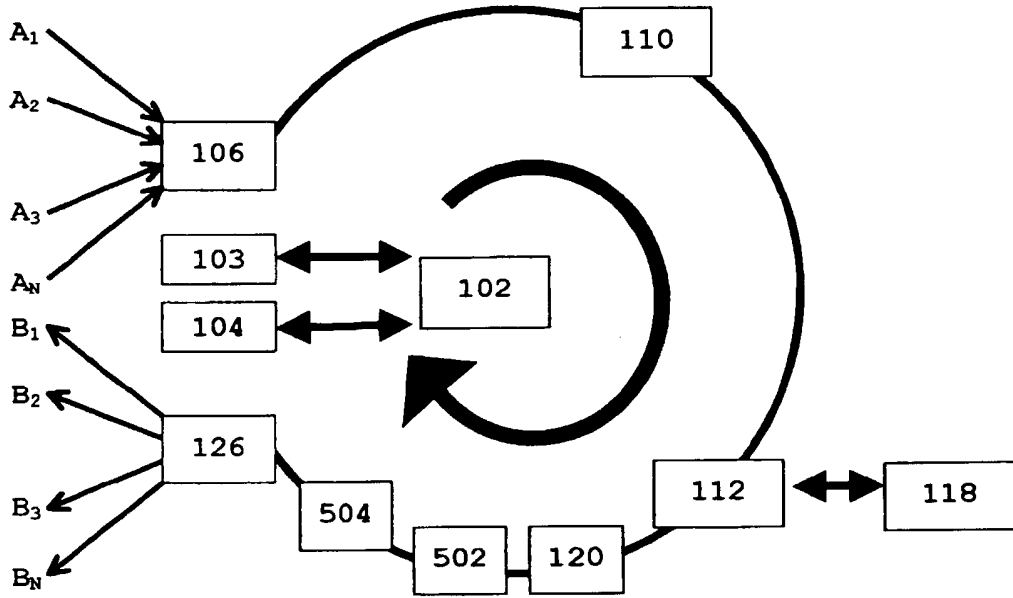


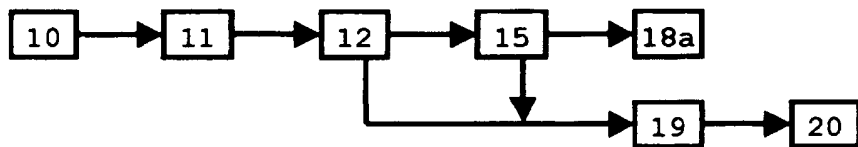
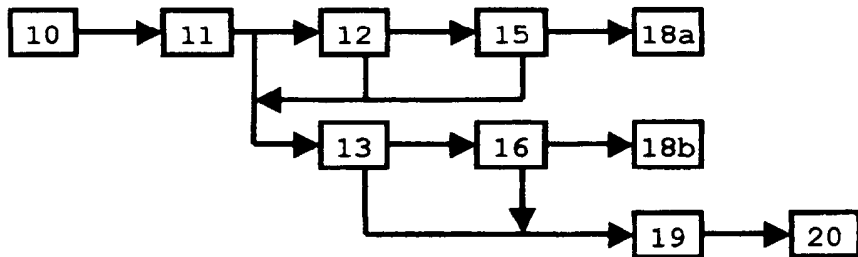
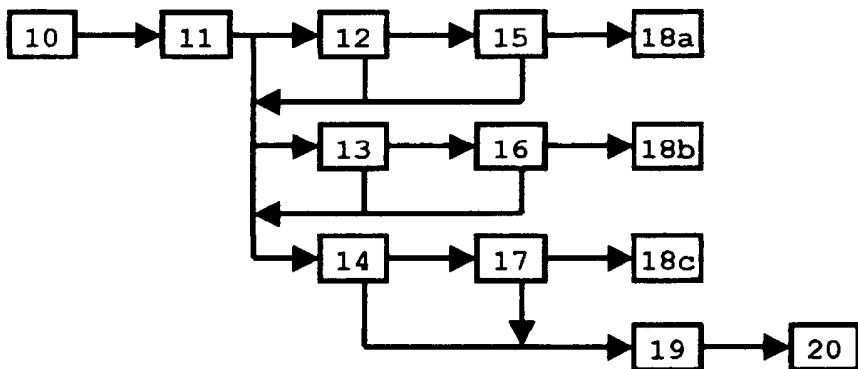
Figure 5aFigure 5bFigure 5c

Figure 6

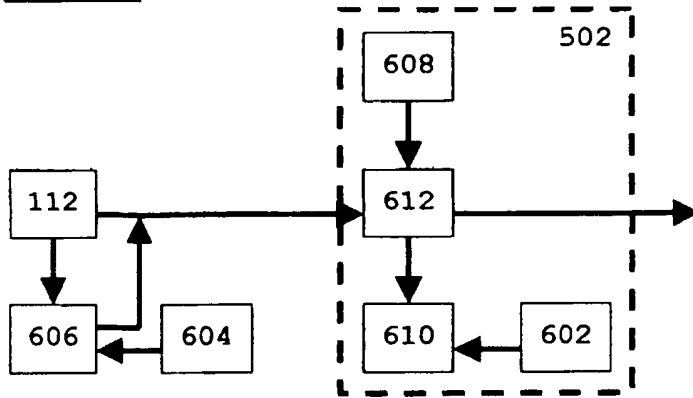
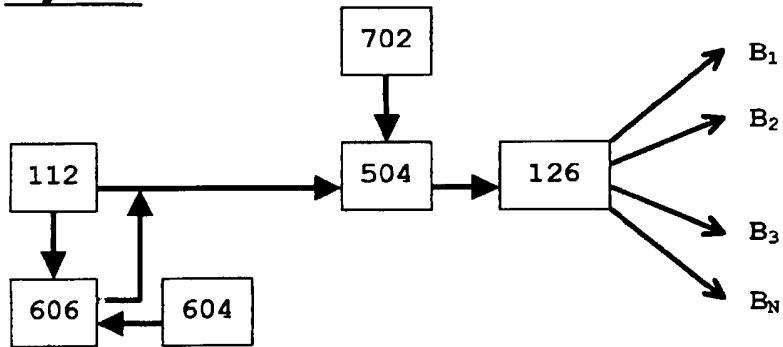


Figure 7



## Platform for Intelligent Message Management

### Technical Field

This invention is related to a Platform for Intelligent Message Management (PIMM). It is particularly directed to the filtering of digital messages, within set end-user parameters, in network environments encompassing large numbers of message addresses and message Domains, a message Domain being the logical grouping of users.

Furthermore, the present invention is directed to synchronisation of Domain information for authentication and identification of users for the purposes of security of access to messages.

### Background Art

With the advent of the Internet, email has become prevalent in digital communications. For example, email messages are exchanged on a daily basis to conduct business, to maintain personal contacts, to send and receive files, etc.

Unfortunately, undesired email messages have also become prevalent with increased email traffic. Often, these email messages are unsolicited advertisements, which are often referred to as "junk mail" or "spam"; worse, they may contain viruses, or other malicious content, such as 'spyware.'

Demand for Email Anti Virus, Anti Spam, Content Filtering and Mail Forwarding solutions for corporate users and Internet Service Providers, who in turn offer these services to home and residential users, has been rapidly increasing over the last five years. This is primarily in response to a newer kind of Email virus that gains control of its infected host digital computer and propagates itself further via Email (e.g SMTP and similar protocols), or through the web (e.g HTTP; HTTPS; FTP and similar protocols).

Software applications exist, which remove some of the spam or junk mail from a recipient's email account, thereby reducing clutter in the recipient's email account. Some of these applications remove email messages that contain a particular text or content (e.g., large image files, etc.) that may indicate that the email message is spam or junk mail. Email messages that are determined to be spam or junk mail are then either removed (e.g., permanently deleted) or stored in a designated folder (e.g., "trash" folder, "junk mail" folder, etc.). Unfortunately, some of the algorithms used to detect spam or junk mail may be quite complicated, cumbersome and at worst, ineffective.

Filtering of Email data on entry to a corporate or Internet service provider network can therefore be time and cost intensive in terms of hardware, personnel, and data loss should infection occur. During periods following the release of a new variant of virus, these issues are further exacerbated at the xSP level (an xSP may be, for example, an Internet Service Provider, a Managed Service Provider, or an Application Service Provider) because there are a large number of Email domains to be filtered, and these change on a daily basis (an Email domain being a logical grouping of Email users, such as @HOTMAIL.COM, for example).

5

10

15

Email also exposes family members within a home user environment to content and advertisements, not virus related, that may be unacceptable and / or inappropriate for their age group, or personal morals and values. With more than one mailbox being given to the home user as part of their service, specifically to allow family access to Email from a single home digital computer, there are conflicting requirements on the level of filtering required.

20

Moreover the nature of current anti-virus, anti-spam and Email content filtering solutions for corporate and xSPs allows for limited individual configuration by end-users and limited integration with third party application software.

25

WO02/28127 provides for a centralized, preprocessing electronic messaging solution that performs value-added tasks to electronic messages on behalf of the ISP or the end user, before these messages are delivered to the destination email server. The service can detect and detain damaging or unwanted messages, such as spam, viruses or other junk email messages, and route electronic messages from various sources covering a variety of topics to wired and wireless destinations, apart from the intended recipient email address, in various formats.

30

Currently available Email security and anti-virus solutions are possessed of critical shortcomings; specifically they do not offer:

35

- 1) capability for end-users directly to control individual security settings over multiple and/or individual mail boxes within an assigned Email sub-domain;
- 2) capability for the domain owner on behalf of the Email users within that domain or sub-domains to directly control individual security settings over multiple, individual mail boxes within an assigned Email domain and sub-domain;



3) capability for end-users directly to control individual content filtering settings over multiple, individual mailboxes within an assigned Email domain and sub-domain;

4) capability for end-users directly to control individual Spam acceptance or rejection criteria over multiple, individual mail boxes within an assigned Email domain and sub-domain;

5) capability for integrating fully within an existing secure Email filtered environment by providing direct domain synchronisation services to third party Email filtering solutions and third party databases containing user information; or

6) capability for integrating fully within an existing secure Email filtered environment by providing cost-effective pre-filtering facilities to third party Email filtering solutions, and subsequent Email redirection or quarantine options.

Third party databases containing user information may typically include those supporting Lightweight Directory Access Protocol (LDAP), which is an Internet protocol that email and other programs use to look up information from a server. LDAP deployments typically use Domain Name System (DNS) names for structuring the simplest levels of the hierarchy. Further into the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else which represents a given tree entry, or multiple entries. Other formats include ActiveDirectory.

Whilst large numbers of communications are disseminated via the Internet using Simple Mail Transfer Protocol (SMTP), 'messages' may also be transmitted via email as non-text attachments, for example: Fax-to-email image attachments in some image format, e.g. tif; Scanned attachments of meeting reports, agenda, legal documents, meeting notes, etc. In addition, more recently, 'messages' are communicated by a number of other digital formats other than email. These currently include: IM for text and image messaging computer to computer; SMS for text messaging via mobile devices; VoIP for communication via telephony; MMS for transmission of images, which could in future be document images as camera resolution improves; 3GP for transmission of video (e.g. via 3GP etc), which could in future be video-phone style information exchange or video voicemail; and Fax, for transmission of documents.

Moreover, some messages will clearly have a higher degree of importance than others, depending on who the sender is or the content, or both. Similarly, some messages, whilst not falling into the category of spam, may have a low priority.

Archiving an email or message (e.g IM in MSN, or SMS) in a useful manner is a major challenge, technically and operationally. Technically, it is a complex task to implement, particularly as the volume of email to be archived often exceeds GB's of data in total. The management of this archive consumes a large amount of business resources that could be more intelligently deployed in other areas. Operationally, locating an archived email or message that was sent or received within an organisation can be difficult. Emails or messages often contain vast amounts of corporate information to which various employees or interested parties of a business need access. In addition, legislation relating to emails presents a significant compliance issue for businesses, and courts now treat email as they would any other form of corporate information. This means that a business must be able to retrieve email from many years ago upon request.

In U.S. Patent Application Publication No. 2004/0267886 an email message is filtered to determine whether or not it is an undesired email message (e.g., "spam," "junk mail," etc.) that originates from an undesirable domain, such as, for example, a domain designated as originating from an undesirable geographic location. In some embodiments, upon determining that the email message originates from an undesirable domain, the email message is deleted (e.g., permanently removed, moved to a designated folder, marked for follow up, etc.). In other embodiments, upon determining that the email message originates from an undesirable domain, the email message is further filtered to determine whether or not the email message includes attributes that indicate that the email message should not be discarded.

In U.S. Patent Application Publication No. 2005/0080856 an e-mail filtering method and system that categorize received e-mail messages based on information about the sender is disclosed. Data about the sender is contained in the message and is used to identify the actual sender of the message using a signature combining pieces of information from the message header or derived from information in the message header. This and other information about the message is then sent by each member of an e-mail network to one or more central databases (in one embodiment, the information will also be stored at a database associated with the recipient's e-mail program and filtering software) which stores the information and compiles statistics about e-mails sent by the sender to indicate the likelihood that the e-mail is unsolicited and determine the reputation of the sender (a good reputation indicates the sender does not send unwanted messages while a bad reputation indicates the sender sends unsolicited e-mail messages). Information from the central database is then sent to recipients in order to determine the likelihood that a received e-mail message is spam (information may also be obtained from the local database associated with the recipient's e-mail

program and filtering software). This need has been met by an e-mail filtering method and system that categorize received e-mail messages based on information about the sender. A sender of a message may be either the individual sending the message or the machine(s) that forwarded the message. The sender may be identified in various ways based on single or combined pieces of information in the message header. For instance, the sender could be identified by an e-mail address, a single IP address, a range of IP addresses, an IP address used with a certain domain name, a range of IP address combined with a certain domain name, etc.

10 Disclosure of Invention

In a first aspect the present invention is a digital message filtering system that comprises a database module containing one or more configuration options relating to one or more end-users and a scanning engine module connected to the database module. The behaviour of the scanning engine module is modified on a message-by-message basis according to the configuration options for the end-users. The digital message may be IM for text and image messaging computer to computer, SMS for text messaging via mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax. The digital message filtering system may additionally include a set-up process so that a third party database may be synchronized as appropriate with the database module.

In a second aspect the present invention is a message filtering system that comprises a database module containing one or more configuration options relating to one or more end-users, a scanning engine module connected to the database module, and either or both of a message archiving system and a message prioritization system also connected to the database module. The behaviour of the scanning engine module, the message archiving system and the message prioritization system are modified on a message-by-message basis according to the configuration options for the end-users. The message filtering system may additionally include a set-up process so that a third party database may be synchronized as appropriate with the database module. The scanning engine module may additionally include a pre-filtering engine. The message may be an Email, or it may be IM for text and image messaging computer to computer, SMS for text messaging via mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax.

In a third aspect the present invention is a message filtering system that comprises a database module containing one or more configuration options relating to one or more end-users, a set-up process so that a third party user database may be synchronized as appropriate with the database module,

and a scanning engine module connected to said database module comprising a pre-filtering engine. The behaviour of the scanning engine module is modified on a message-by-message basis according to the configuration options for the end-users. The message may be an Email, or it may be IM for text and image messaging computer to computer, SMS for text messaging via mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax.

According to the present invention the sender or recipient of a message may be end-user of the message filtering system.

10 In a fourth aspect the present invention is a pre-filter able to identify a digital message that is not capable of carrying an unwanted or undesirable component prior to full scanning of the message by the standard filtering software. If the message is not capable of carrying unwanted or undesirable components, then it is not passed to the standard filtering software, but if  
15 it is, then it is passed to the standard filtering software for further analysis.

In a fifth aspect the present invention is a message archiving system comprising a message stream, an auto-archiving engine, a database and an auto-archive database. The message archiving system is characterised in that  
20 its behaviour is determined by settings in the database so that if a particular message in the message stream falls within criteria specified in the database a copy of the message is added to the auto-archive database.

In a sixth aspect the present invention is a message prioritisation system comprising a message stream, prioritisation module, a database and one or  
25 more delivery streams. The message prioritisation system is characterised in that its behaviour is determined by settings in the database so that if a particular message in the message stream falls within criteria specified in the database a delivery stream  $B_1, B_2, B_3 \dots B_N$  is chosen.

30 In a seventh aspect the present invention is a method for pre-filtering digital messages is disclosed which involves the steps of: (a) identifying a digital message that is not capable of carrying an unwanted or undesirable component prior to full scanning of said message by filtering software; (b) passing the message so identified to a data stream not requiring full scanning of said message by filtering software; and (c) passing other  
35 messages not identified in step (a) as not capable of carrying an unwanted or undesirable component to a module able to do a full scan of said message.

In an eighth aspect the present invention is a method for archiving messages which involves the steps of: (a) receiving a message from a message stream (120); (b) comparing the message to criteria in a database (610); and (c)

copying the message to an auto-archive database if the message falls within the criteria.

In a ninth aspect the present invention is a method for prioritising messages which involves the steps of: (a) receiving a message from a message stream  
5 (120); (b) comparing the message to criteria in a database (610); and (c) delivering the message to a delivery stream  $B_1, B_2, B_3 \dots B_N$  if the message falls within criteria.

In a tenth aspect the present invention is a method for filtering digital messages which involves the steps of: (a) receiving a message for an end-  
10 user; (b) identifying configuration options related to the end-user held in a user database module; (c) modifying a behaviour of a scanning engine module according to the configuration options; and (d) scanning and filtering the message according to the configuration options. The digital message may be IM for text and image messaging computer to computer, SMS for text messaging via  
15 mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax. The digital message filtering system may additionally include a set-up process so that a third party database may be synchronized as appropriate with the database module.

In an eleventh aspect the present invention is a method for filtering digital  
20 messages which involves the steps of: (a) receiving a message for an end-user; (b) identifying configuration options related to the end-user held in a user database module; (c) modifying a behaviour of a scanning engine module according to the configuration options; and (d) scanning and filtering the message according to the configuration options. The method also includes  
25 either or both of archiving and prioritizing the message. The method may additionally include a set-up process so that a third party database may be synchronized as appropriate with the database module. The scanning engine module may additionally include a pre-filtering engine. The message may be an Email, or it may be IM for text and image messaging computer to computer, SMS  
30 for text messaging via mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax.

In a twelfth aspect the present invention is a method for filtering digital messages which involves the steps of: (a) receiving a message for an end-  
user; (b) identifying configuration options related to the end-user held in a  
user database module; (c) modifying a behaviour of a scanning engine module  
35 according to the configuration options; (d) pre-filtering the message as described above; (e) scanning and filtering the message according to the configuration options; (f) synchronizing a third party user database as appropriate with the user database by means of a set-up process.

In a thirteenth aspect the present invention is a method of synchronising which comprises the steps: (a) accessing a first field in a third party database; (b) accessing a corresponding field in the user database; (c) determining whether data in this field of the third party database is newer than data in the corresponding field in the user database; and (d) replacing the data in the corresponding field in the user database with the data in the first field in the third party database if the first field in the third party database is newer than data in the corresponding field in the user database.

**Brief Description of Drawings**

10 For a more complete explanation of the present invention and the technical advantages thereof, reference is now made to the following description and the accompanying drawing in which:

Figure 1 shows a schematic of the data flows in a platform for intelligent message management according to one aspect of the present invention;

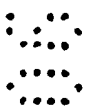
15 Figure 2 shows a schematic of the data flows in a scanning engine of the present invention;

Figures 3a and 3b show schematics of the data flows of the present invention when implemented to divert a service provider's messages via PIMM;

20 Figure 4 shows a schematic of the data flows in a platform for intelligent message management according to a further aspect of the present invention;

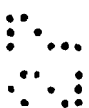
Figure 5 shows the essential features of a pre-filter module of the present invention in a schematic form;

Figure 6 shows the essential features of an auto-archiving module of the invention in a schematic form; and

25  Figure 7 shows a schematic of a prioritisation process of the present invention in a schematic form.

**Best Mode for Carrying Out the Invention**

Embodiments of the present invention and their technical advantages may be better understood by referring to Figures 1 - 7.

30  The present invention is exemplified in the following embodiments, in which a number of 'daemons' or discrete sections with composite functions and scanning engines for dedicated tasks are combined. This application suite will be referred to as the Platform for Intelligent Message Management, or PIMM, in the following.

Referring now to Figure 1, which shows a schematic of one embodiment of the present invention, module 106 receives messages from incoming data stream 108 which are processed and passed onto data queue 110 prior to processing by scanning engine 112. Processed messages are transferred via outbound data queue 120 to relay module 126 and thence to outgoing data stream 122.

In operation, listener 106 receives messages from an incoming data stream 108 and is preferably capable of accepting and acting on externally held data that may modify its behaviour on a message-by-message basis. Listener module 106 may be, for example and without limitation, a High Performance Port listener, for SMTP, POP3, IMAP4 or other protocols (see Table 1). Preferably these messages are decoded and unpacked and pass into data queue 110 prior to processing by the scanning engine 112.

CIFS	DHCP	DNS
FTP	Hotline@	HTTP
ICP@	IP	IRC
Kerberos@	Mail	MUDs@
NNTP	NTP	PKIX@
PPP	PPTP@	RADIUS@
RTSP	RWhois	SIP
SMB@	SNMP	SOAP@
SSH	SSL-TLS	TCP@
UDP@	WebDAV@	X11

Table 1 - Commonly used protocols

The overall behaviour of PIMM on a message-by-message basis is controlled by information contained in a secure data store, or user database 102. User database 102 is customer-specific and is an information store for end-user data. Its function is to hold information set by the end-user's preference options, and provides configuration for the behaviour of PIMM.

Referring again to Figure 1, end-user preference options may be set via an end-user interface 103, and an optional set-up process 104. End-user interface 103 provides access for the end-user to set configuration options, for example, over a corporate network, or the general Internet. In a preferred embodiment, access is via a web site. In a further preferred embodiment, access is via a secure means of communication, preferably involving a Secure Sockets Layer. In a further preferred embodiment, access is via a further protocol from hand held and mobile devices, preferably involving a secure communications protocol. When a new user is added by the customer, set-up process 104 automatically adds default information to 102,

including for example, login and password details, which services within PIMM the user is subscribed to, and so on.

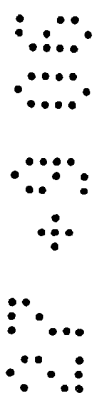
The scanning engine 112, performs anti virus, anti spam, and content control filtering services for inbound messages and file attachments and also  
5 provides further pre-filtering services of the kind disclosed above (see Figure 1) using third party software solutions and/or services on-server or off-server, with the ability to quarantine any infected message for virus, or with the ability to process any message according to pre-determined parameters. For example the message may be checked for the presence of a  
10 virus, so that messages that cannot contain a virus are not processed further. In this context, "pre-filtering" is defined as the capability to exclude or reroute message traffic either detected as unwanted by the database engine 102 or by third party services.

Scanning engine 112 is connected with a single master server that feeds all  
15 message servers for all services. The scanning engine 112 also receives updates of anti virus signatures and the like, via proprietary or third party update service 118.

Referring now to Figure 2, which shows a schematic of scanning engine 112, data from queue 110 passes through a pre-filtering engine 200, and, depending  
20 on the action of the pre-filtering engine 200 may subsequently pass through one or more of the following: an anti virus engine 202, an anti spam filtering engine 212, and a content-filtering engine 222. Filtered messages are passed either to quarantine (208, 220, or 230), or waste bin 210, and acceptable messages passed on to 120.

25 Pre-filtering engine 200 can if required provide redirection to third party software solutions and/or services on- or off-server, or the built-in capabilities afforded by 102. This typically operates using a defined rule set to determine the status of the message, for example i, the probable infection status of inbound message to the antivirus engine, or third party  
30 antivirus scanning engine within 112; for example ii, content control settings of the message to an individual user to the content control engine; for example iii, age control settings of the message to an individual user to the content control engine.

Anti virus engine 202, used either stand alone, or using unique  
35 synchronisation technology to integrate third party anti virus software solutions, provides antivirus filtering for the message and for any file attachment if the message is an email. Information regarding the filtering options performed on the message is provided by the user database, for example via an Application Programming Interface. Protection against viruses





may typically be provided by Known Virus Protection **204**, for example by examining signatures and detecting known viruses by name, and/or Outbreak Virus Detection **206**, for example by heuristic analysis to proactively stop new viruses. When a virus is detected it can be moved to quarantine **208** or a waste bin **210**.

Anti spam filtering engine **212** which uses heuristics and Bayesian model methodologies combined with individual word probabilities. The antis spam Engine, used either stand alone, or using unique synchronisation technology to integrate third party antis spam software solutions, provides user level preference spam filtering for the message and for any file attachment if the message is an email. Information regarding the filtering options performed on messages is provided by Application Programming Interface access to the user database. Typically it provides a Message Structure Analysis **214** that analyses, for example, the structure of a message, its reputation and travel path, performs heuristic rule-based checks **216** by checking against a knowledge base and heuristic and/or Bayesian content analysis, and is able to detect hoaxes and phishing, and uses White and Black Lists of global, domain and user lists **218** based on list entries. Messages are allowed or blocked based on sender, domain, hosts, etc. Detected spam is moved to quarantine **220** for further predetermined action or routing of messages depending on the content of the message, or a it is passed to waste bin **210**, or the subject line of the message is changed and the message allowed through.

Content-filtering engine **222** integrated with the external database enables individual message box preferences for content filtering to be set. It typically provides Message Server Protection **224** that detects and stops oversized attachments, mailbombs, etc, an Attachment Type Control List **226** that blocks selectable file types such as .mp3, video and executables, a Custom Rules Control **228** which uses custom rules to block specific subjects, message content or file names. Detected content message is moved to quarantine **230** or a waste bin **210**, or the subject line of the message is changed and the message allowed through.

The scanning engine **112** is preferably able to place undesired messages in quarantine queues **208**, **220**, and **230** and the software suite allows for a secure folder structure for the placement of quarantined messages. If required, the system may provide an alert to the user, the sender, or the systems administrator, (for example if the content is considered as not being acceptable or is inappropriate) via alert service **116**. This alert is passed to an outbound queue **120**.

Associated with the operation of the scanning engine, is a reporting mechanism **123** (not shown), which provides a summary by end-user as defined in **102** of, for example, quarantined and/or deleted messages. All reports, notifications and clean messages go via **120** and **126** to the customers message server.

A virus in quarantine queue **208** may be released or deleted according to user level or domain level defined settings.

Spam in quarantine queue **220** may be released or deleted according to user level or domain level protocols; in addition, when releasing quarantined messages a user can select to remember a particular message as being not spam. Any further similar message would be recognised by **212** to not be spam.

Messages having content that is considered as not being acceptable or is inappropriate, or which has special characteristics specified in **102**, may be released, forwarded, modified or deleted from quarantine queue **230** according to user level or domain level protocols; in addition notification can be made to an administrator or user. A message that originates from certain URL's or domain names according to spam blacklists is treated similarly.

Referring again to Figure 1, relay module **126** enables delivery to end-user message systems or third party application software on completion of antivirus, anti-spam, and content filtering checking. Relay module **126** transmits filtered Emails not quarantined or deleted to an outgoing data stream **122**. Optionally, a standard or customizable banner **124** may be added to the message (not shown). Clean processed messages are passed to an outbound queue **120** to enable delivery of Message data. In a preferred embodiment PIMM additionally comprises an outbound queue for clean processed message **120**. Should message not be delivered, it is retained in **120**, and stored or forwarded for a defined period of time. Relay module **126** may be for example and without limitation a high performance relay module for SMTP, POP3, IMAP4 or other protocols (see Table 1).

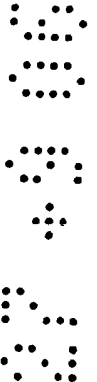
Each stage of the process requires information from **102** to determine the action the message is to be subjected to.

In a further aspect of the invention, the sender of a message may be an end-user of PIMM. In this case, the outgoing message passes into data queue **110** and the message is processed as described above according to settings in user database **102** before the message is passed to outbound data queue **120**.

Typically the spam filter is not applied to outbound messages as they are considered to be real messages.

If the intended recipient of the message is not an end-user of PIMM, the message is passed via relay module 126 to outgoing data stream 122 as described above. This may also be the case if the intended recipient of the message is an end-user of PIMM, in which case it will pass via the internet  
5 to listener 106 via incoming data stream 108. The message will be again processed by PIMM, but this time according to the user database settings for the recipient. Alternatively, the message may be diverted from 120 to 106, and processed again, but this time according to the recipients' settings in the user database, as described above.

10 A preferred embodiment of the present invention where the customer is a third-party service provider may be understood by reference to Figure 3a, which shows a schematic of data flows during message processing. When the third-party service provider subscribes to the PIMM service, information on database 302 concerning the third-party service message server is altered so  
15 that incoming message from a message sender 300 is sent to PIMM 304. Scanning engine 112 processes each message in data queue 110 according to the data in 102 as described in the foregoing. If the message has not been passed to 208, 210, 220, or 230, then it is sent to the third-party service message server 306, and thence to end-user messagebox 308. Such a PIMM system, typically  
20 located externally to the third-party service provider's servers, is able to process message data from multiple third-party service providers; in each case the records on database 302 concerning the third-party service provider are adjusted so that all messages for its customers are diverted to PIMM 304,  
25 processed, and sent to each third-party service provider's message server as appropriate. Of course, each third-party service provider will have multiple end-users; many, if not most of these will be grouped into specific groups, domains and sub-domains, allowing a domain, or sub-domain, administrator to set default settings for the end-users within their respective domains or sub-domains. This is achieved via set-up process 104 mounted on the server  
30 of the third-party service provider, so that, for example, when a new user subscribes to the third-party service provider, automatic synchronization from the third-party service provider to PIMM could instantly add a new user or domain to the PIMM user database 102. As soon as the user is added, the user may login to PIMM through the interface 103 running from the PIMM  
35 service mounted on a third party server. 103 has a separate sign-in and logon to authenticate users, and allows them to set their own settings at a Service Providers view (for some or all) or at the end-user view for personal settings. The end-user may also change the settings relating to the priority of various messages. For example, the end-user may request that an SMS  
40 message be sent to his mobile device should he receive a message from his boss. A domain owner or corporate customer of the xSP providing the PIMM



services may also define on behalf of its end users certain settings, whether individually, by group, or for all end users.

In a further preferred embodiment, a user interface 105 (not shown) allows end-users to modify their settings and preferences, and operates in a manner substantially identical to 103, as described above. However, according to this embodiment 105 connects to, and interchanges data with, 104, and both 104 and 105 are mounted on the third-party service provider's server. This end-user information held on 104 is synchronised as appropriate with the user database 102. Thus when a new user subscribes to a Service Provider, automatic synchronization from the Service Provider to PIMM could instantly add a new user or domain to the PIMM user database (configuration database). As soon as the user is added, the user could login through the web interface 103 as described above. Synchronisation between information held by the third-party service provider on 104 and the end-user database 102 on the PIMM service mounted on a third party server may happen at a frequency set by the needs of the third-party service provider. Both 104 and 105 may be mounted on different servers. Access to 105 may be via a corporate network, or the general Internet, and allows the third-party service provider to set configuration options on individual messageboxes within an assigned Email Domain or sub Domain, on behalf of the end-users. In a preferred embodiment, access is via a means of communication, such as via a web site. In a further preferred embodiment, access is via a secure means of communication, preferably involving a Secure Sockets Layer. In a further preferred embodiment, access is via a further protocol from hand held and mobile devices, preferably involving a Secure Communications Protocol. In a further preferred embodiment, access is via remote control or neurological implants.

In a particularly preferred embodiment the third-party service provider is an xSP. According to this embodiment, shown in Figure 3b, database 302 is a DNS server containing, for example, MX records. When an xSP subscribes to the PIMM service, information on DNS server 302 concerning the xSP's message server, for example MX records, is altered so that incoming message from a message sender 300 is sent to PIMM 304, mounted on a third-party service provider. Scanning engine 112 processes each message in data queue 110 according to the data in 102 as described in the foregoing. If the message has not been passed to 208, 210, 220, or 230, then it is sent to the xSP message server 306, and thence to end-user mailbox 308. Such an externally-mounted PIMM system is able to process Message data from multiple xSPs; in each case an xSP's DNS records are adjusted so that all messages for its customers are diverted to PIMM 304, processed, and sent to each xSP's message server as appropriate. Each xSP will have multiple end-users; many, if not

most of these will be grouped into specific domains and sub-domains, allowing a domain, or sub-domain, administrator to set default settings for the end-users within their respective domains or sub-domains. This is achieved via set-up process 104 mounted on the xSP's server, so that, for example, when a  
5 new user subscribes to the xSP, automatic synchronization from the xSP to PIMM could instantly add a new user or domain to the PIMM user database 102. As soon as the user is added, the user may login to PIMM through the interface 103 running from the PIMM service mounted on a third party server. 103 has a separate sign-in and logon to authenticate users, and allows them  
10 to set their own settings at a Service Providers view (for some or all) or at the end-user view for personal settings.

The approach disclosed above and shown in Figures 3a and 3b may be applied to any digital message stream to route the message to PIMM rather than the message service provider's servers. Thus the digital message may be IM for  
15 text and image messaging computer to computer, SMS for text messaging via mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax. Each method of routing will be specific to the protocol being utilized, and requires for example a BlackBerry server to route via its carrier to PIMM for processing, thereafter  
20 routing back to carrier to Blackberry recipient clean message. Similarly for any form of pda or wireless technology.

Information about an end-user's preference in relation to message handling may be stored on a variety of databases. For example, LDAP, Lightweight Directory Access Protocol, is an Internet protocol that email and other  
25 programs use to look up information from a server. Other formats include ActiveDirectory. Other main database formats are mostly based on the SQL standards, including Oracle, MS SQL, MySQL etc. These kinds of databases offer a high degree of flexibility, as they do not have a predefined form and may therefore be used for specialized systems.

30 In SQL terms when databases are kept in synchrony automatically this is called "database replication". This can be one way, with a master and one or more slaves, or both-ways, which means neither is a master or slave.

35 When using one-way synchronization, updates/changes/additions are made in the master and automatically updated in the slave database. When using both-ways updates/changes/additions can be made on either of the databases and updates are replicated/synchronised to the other(s).

40 In one embodiment user database 102 takes advantage of this flexibility and is written in an SQL format. Similarly, the third party database with which PIMM synchronises data may be written in an SQL format. In one embodiment of the present invention, the database at the third-party/customer end is the

master and changes are synchronised/replicated to user database 102. From a technical perspective, the user database 102 could also be the master, or there could be a both-ways mechanism if the third-party database also supports this.

5 Synchronizing LDAP, ActiveDirectory and SQL-based database formats requires different "modules" to read from a source database and update data in the target database. This is easiest with LDAP and active directory as these formats are mainly predefined, whereas SQL formats are more flexible.

10 For the synchronization fields from the source must be linked to the fields at the target database. For example in the source there might be a field which is called "Name1" and "Name2" where these may be called "FirstName" and "LastName" in the target database. Linking these fields together is what the specific module, based on the source type, does.

15 The kind of information stored might include information on people, organizational units, printers, documents, groups of people or anything else which represents a given tree entry, or multiple entries. This kind of information can be viewed as a group of settings/information just like the user database of PIMM. Instead of having to make separate changes in two systems, for example first in an external LDAP system and then secondly in  
20 user database 102, third party database synchronization can be used. As part of the synchronization mechanism there is a part that can detect changes in an LDAP structure/database to keep the user database up-to-date.

25 Other databases that may synchronise with the user database might include those owned and operated by cellular telephone service providers, whereby a user of such a service may set certain parameters regarding the delivery of a message to the user's cellular device. For example, the user may only wish to receive messages from certain senders whilst, for example, in a meeting. Using his cellular device the user can set the appropriate setting that updates the cellular telephone service provider's database, and synchronises  
30 subsequently with the PIMM user database.

35 Thus the third party database that is able to synchronise with the user database of PIMM can be any third party database containing information about PIMM end-users that can update corresponding information on the PIMM user database.

Thus external databases for example that have information about an end-user that could be related to the end-users preferences on PIMM, but which the end user does not want manually to enter into PIMM, but which if it were to be modified on PIMM by the end user would also be changed on this external database through a synchronisation process, or which if the end user changes

by accessing this external database by a different means, will also lead to an update on PIMM.

The benefit of this for the user, is that changes need to be made only once whatever digital message service the end user may be using, be it Email, SMS, IM, VM and so on.

A key aspect of PIMM is that only one update of Master server 118 with information about spam, worms, viruses errant scripts and the like is required, thereby reducing the volume of update traffic from an end-user's computer to antivirus, antispam, etc, and ensuring that these security measures are implemented across a user network regardless of the habits of the end-user.

These modules within the suite, according to the invention allow, for example:

- 1) End-users to directly apply individual security control over multiple, and/or individual message box within an assigned address, domain and sub-domain by accepting configuration from the web interface as described, and referencing that information on an individual message basis for processing.
- 2) End-users to directly control individual content filtering control over multiple, and/or individual message boxes within an assigned address, domain and sub-domain. Using the scanning engine, with end-user configuration supplied via the user database from the web interface, individual content rules are applied on a message-by-message basis. Differing content rules can be applied to each message box within an assigned message domain and sub domain.
- 3) End-users to directly control individual Spam acceptance or rejection criteria control over multiple, and/or individual message boxes within an assigned message domains and sub-domain. Using the scanning engine, with end-user configuration supplied via the user database from the web interface, individual spam acceptance or rejection criteria rules are applied on a message-by-message basis. Differing Spam acceptance or rejection criteria rules can be applied to each message box within an assigned message domain and sub domain.
- 4) Super-users or administrators can control the entire domain for all end-user message boxes, or to groups of end-users according to business function or seniority.
- 5) Capability for integrating fully within an existing secure message filtered environment by providing pre-filtering facilities to third party message filtering solutions, and subsequent message redirection or quarantine options (208, 220, 230). The pre-filter module allows pre-filtering

capabilities and redirection via **202**, **212**, **222** to either the end-user message system, existing third party software or managed service solutions for anti virus, anti-spam and content control services, or to quarantine for infected messages.

- 5 6) capability for integrating fully within an existing secure message filtered environment by providing cost-effective pre-filtering facilities to third party message filtering solutions, and subsequent message redirection or quarantine options.

Whilst the foregoing disclosure is refers to digital messages, it is to be understood that this includes a variety of message protocols, including for 10 Email protocols such as SMTP, POP3 and IMAP4. It is also to be understood that the message includes those messages that can be transmitted via Email as non-text attachments, for example: Fax-to-Email image attachments in some image format, e.g. tif; Scanned attachments of meeting reports, agenda, legal 15 documents, meeting notes, etc. In this case, listener module **106** would include an OCR capability prior to content analysis. Further, it is to be understood that listener module **106** and output module **126** be able to handle multi-protocol inputs/outputs for digital message management to allow various capabilities for content analysis of non-text based messages including: voice 20 recognition (for data streams comprising voice rather than text, or for filtering 3GP streams), and or other streaming technology; image processing (for filtering MMS streams), etc; OCR (for fax and other attachments), text to voice, and voice to text, etc. The message includes those communicated by a number of other digital formats other than message, including IM for text 25 and image messaging computer to computer; SMS for text messaging via mobile devices; VoIP for communication via telephony; MMS for transmission of images, which could in future be document images as camera resolution improves; 3GP for transmission of video, which could in future be video-phone style information exchange or video voicemail; and Fax, for transmission of 30 documents. Various protocols for message transmission are to be understood to be included within the scope of the present invention, including G3 and WAP. It is to be further understood that the platform for intelligent message management described above in Figure 1 is capable of handling any message in a digital format including those messages and protocols disclosed below (eg 35 via a neural interface).

Referring now to Figure 4, which shows a schematic of a further embodiment of PIMM capable of handling a wide range of digital messages, module **106** of Figure 1 is able to process a series of data streams **A<sub>1</sub>**, **A<sub>2</sub>**, ... **A<sub>N</sub>** which represent different message types and protocols (see Table 1). These may be, 40 for example and without limitation an SMTP stream, an SMS stream, a MMS



stream, a fax stream, a voip stream, an IM stream. These messages, after conversion into a suitable digital format where necessary are transferred to data stream 110 and thence to filter module 112. The filter module includes pre-filter processes and full virus, spam and content control filters as disclosed above in Figure 3. The behaviour of these filters is set and controlled by a user database 102. Depending on the settings in the user database and the behaviour of the filters, messages may be sent to one or more of a quarantine store (for example, to 208, 220, 230 of Figure 3), a waste bin (for example, to 210 of Figure 3) or a message stream (for example 120 of Figure 3). Optional embodiments of this aspect of the invention include an archiving module 502, and a prioritisation module 504. Messages that have been prioritised or archived are passed to module 126, and following suitable format inter-conversion are subsequently be passed to an appropriate delivery stream  $B_1, B_2, \dots B_n$ . These delivery streams may be, for example and without limitation, an smtp stream, an SMS or MMS stream, a fax stream, a voip stream, an IM stream or another output data stream, as appropriate based on and on settings in the user database, so that a user may receive them. End-user preference options may be set via an end-user interface 103, and an optional set-up process 104 as described above for Figure 1.

In a further aspect of the invention, the sender of an message may be an end-user of PIMM. In this case, the outgoing message passes into data queue 110 and the message is processed as described above according to settings in user database 102 before the message is passed to outbound data queue 120. Typically, for outgoing messages, the spam filter is not applied as these are considered to be real messages.

If the intended recipient of the message is not an end-user of PIMM, the message is passed via relay module 126 to outgoing data stream 122 as described above. This may also be the case if the intended recipient of the message is an end-user of PIMM, in which case it will pass to listener 106 via incoming data stream 108. The message will be again processed by PIMM, but this time according to the user database settings for the recipient. Alternatively, the message may be diverted from 120 to 106, and processed again, but this time according to the recipients' settings in the user database, as described above.

Referring now to Figure 5a, which shows in schematic form an embodiment of pre-filter 200, incoming messages from a sender 10 are passed to an incoming message queue 11 and thence to pre-filter 12. The pre-filter is able to detect messages that are not capable of carrying an unwanted component. The unwanted component may be, for example and without limitation, a virus, spam

or other unwanted content. If the message is so identified, then it is passed to outgoing message queue 19; otherwise it is passed to a standard filter 15. The standard filter may be, for example and without limitation, an antivirus, anti-spam or content filter. If, after analysis by standard filter 15, it is found to be carrying an unwanted component, it is passed to quarantine 18a; otherwise it is passed to outgoing message queue 19 and thence to recipient 20.

Referring now to Figure 5b, which shows in schematic form a further embodiment of pre-filter 200, having two pre-filters, incoming messages from a sender 10 are passed to an incoming message 11 queue and thence to pre-filter 12 or pre-filter 13. The pre-filter is able to detect messages that are not capable of carrying an unwanted component. The unwanted component may be, for example and without limitation, a virus, spam or other unwanted content. If the message is so identified, then it is passed to a second pre-filter 13 able to detect messages that are not capable of carrying an unwanted component; otherwise it is passed to a standard filter 15. The standard filter may be, for example and without limitation, an antivirus, anti-spam or content filter. If, after analysis by standard filter 15, it is found to be carrying an unwanted component, it is passed to quarantine 18a; if not, it is passed to second pre-filter 13. If the message is identified by second pre-filter 13 as being incapable of carrying an unwanted component, then it is passed to outgoing message queue 19; otherwise it is passed to a standard filter 16. The standard filter may be, for example and without limitation, an antivirus, anti-spam or content filter. Typically, if first pre-filter 12 is able to detect messages incapable of carrying a virus, second pre-filter 13 is able to detect a message unable to carry spam. If, after analysis by standard filter 16, it is found to be carrying an unwanted component, it is passed to quarantine 18b; otherwise it is passed to outgoing message queue 19 and thence to recipient 20.

Referring now to Figure 5c, which shows in schematic form a further embodiment of pre-filter 200, having one or more pre-filters 12, 13 or 14, incoming messages from a sender 10 are passed to an incoming message 11 queue and thence to one of the pre-filters. Typically, these may be a virus pre-filter, a spam pre-filter and a content pre-filter. Preferably the message is passed first to antivirus pre-filter 12, then antis spam pre-filter 13, and finally to content pre-filter 14. This order is preferable, because if the virus pre-filter is missed, it is possible that a message containing a virus may be passed to the outgoing message stream. After pre-filtering, the message is passed to the virus filter 15 if virus pre-filter 12 determines it

likely contains a virus, otherwise it is passed to spam pre-filter 13. Similarly, a message from spam pre-filter 13 is passed to the spam filter 16 if the pre-filter determines that the message is likely to be spam, otherwise it is passed to content pre-filter 14. If the content pre-filter  
5 determines that content filtering is likely needed, it is passed to content filter 17; otherwise the message is passed to the outgoing message queue 19 and thence to recipient 20. If any of the standard filters determine that the message is carrying an unwanted component, it is passed to the appropriate quarantine 18a, 18b, or 18c. The exact data flows may be specified by a user  
10 database (not shown; see the disclosure concerning Figure 1).

The pre-filtering system of the present invention performs a simple technical analysis of the message to see what sort of message it is. The analysis determines, for example, whether the message come from a trusted source, whether it contains harmful links/code, what kind of structure the message  
15 has, and whether it has attachments and of what type.

The pre-filtering system of the present invention will determine if the message needs subsequent spam, virus and or content filtering. Thus a message having an .exe file attachment to a message will certainly need virus-scanning, whilst a message with only two lines of text, which forms the bulk  
20 of the message, or for example, from a trusted source, or with a url link of a trusted HTTP site embedded in the message, will not necessarily need to be checked by an antivirus, spam or content engine.

Messages that do not need further analysis by the more complex virus/spam/content filters disclosed by the prior art are thus not processed  
25 further. This reduces the number of messages passed to the virus/spam/content filters, which serves to reduce the processing overhead of the message filtering system of the present invention, and also reduces the (license or subscriber) cost of utilising third party virus/spam/content filters where a fee is charged by the virus/spam/content filter authors per message, or per user (by message address, message alias, or frequency of messages scanned) as  
30 identified from the message being filtered. This enables faster delivery of messages to the user, reduces amount of hardware infrastructure necessary to scan messages that do not need to be scanned, resulting in lower costs for the organisation and users using the invention.

35 Thus application of the rules in a pre-filter of the present invention is differentiated in substance from simply applying the rules within the virus, spam and content filters: the rules are simpler, the processor overhead is lowered, and the licence cost of using third party filters is reduced.

The present invention aims to detect messages that do not require further  
40 analysis by an antivirus module, an anti-spam module or a content-filtering

module. The approach the pre-filter uses is to examine a message and assess for the absence of certain characteristics in a message.

In one aspect, if the pre-filter identifies messages, for example, having:

- (a) attachments;
- 5 (b) IFRAME or other embedded elements that will download when the message is opened, and which could download malicious code from the internet, or have privacy or other security implications;
- (c) a link to a website that could cause a virus to be downloaded;
- (d) a message originator blacklisted as a virus distribution server or user;

10 then the pre-filter passes the message to a standard antivirus filter for further analysis. If the message does not have these components, then the message can be passed onto the user inbox, or to a second pre-filter for spam, to a third for content and so on.

15 In a further aspect, if the pre-filter identifies messages in which for example:

- (a) the originator state is a known source of spam;
- (b) the sending program is probably bulk rather than personal;
- (c) the structure of the message is poor and may contain 'lazy' html;
- (d) a message originator blacklisted as a spam distribution server or user;

20 then the pre-filter passes the message to a standard antispam filter for further analysis. If the message does not have these components, then the message can be passed onto a further content filter, or to the user inbox.

25 In a further aspect, if the pre-filter identifies messages having attachments, then the pre-filter passes the message to a standard content filter.

Whilst the foregoing discloses separate pre-filters for each type of unwanted content, it is to be understood that this is partly for clarity; the pre-filter functions may also be merged into one module to further increase the speed of the pre-filtering process.

30 The pre-filtering module disclosed above can be used in a pre-processing step in conjunction with conventional third-party software for anti-virus, antispam and content filtering programs. This offers significant advantages in reducing the number of messages to be processed, particularly in a commercial environment where the majority of messages might be considered to be not requiring anti-virus, antispam and content filtering.

35 However the pre-filtering module may also be part of a bigger system.

Referring now to Figure 6, which shows the essential features of the auto-archiving module 502 of the present invention in a schematic form, a processed message, which may be, for example, from filter module 112 disclosed above, is received by auto-archiving engine 612 from message stream 5 120. The behaviour of the auto-archiving module is determined by settings in a database 608 or where the auto-archiving module is part of an integrated system of the type shown in Figures 1 and 4, through the user database 102, as described above, so that if a particular message falls within the criteria specified in the database, either at the individual user level or at an 10 administrator level, a copy of the message is added to auto-archive database 610. Access to the database may be via a web portal 602, accessible by the end user, whether individual or administrator level. For regulatory compliance, a compliance officer may set the auto-archiving parameters within the user database and the auto-archived messages are stored in a secure 15 database, potentially on an external regulatory database. Thus this aspect of the invention includes standard auto-archiving and 'bespoke', customer-specific archiving capabilities.

Preferences may be set by a user / administrator to specify how emails should be archived or automatically stored. Where the end user is for example an 20 individual who is a private customer of a commercial ISP, the scope for auto-archiving may simply be according to sender or subject line, and non-relevant messages are not auto-archived in this way. For example, to auto-archive anything from an end-user's lawyer or banker. The auto-archiving database may include mechanisms for allowing rapid access to stored messages by, for 25 example, subject, content, sender or date. The auto-archiving database may also permit compression of messages to save space. In a more commercial environment, where the end customer is a business or organisation, the auto-archiving may also be done for individual users within the organisation in this simple way according to header, date, sender, or subject line, or it may 30 be by more complex content analysis. At a user level in an organisation or in a non-commercial environment, incoming messages may also be auto-archived by user-determined priority. For example, this may be simply according to respondent (sender), file type, subject line, key word, sound, image or another determined criteria search. The database may be searchable, either at the user level, or at the domain level by a user / administrator.

35 Additionally, incoming messages may also be auto-archived by administrator-specified criteria, to provide compliance with current and evolving regulatory requirements to help achieve compliance, for example for US companies to comply with Sarbanes Oxley, for UK patient confidentiality requirements HIPPPAA, for EMEA finance companies Basel II and so on. Thus, 40 access and retrieval of the stored messages carry different access levels, to

help secure privacy of the user and/or to protect corporate information by an administrator. The data may be retrieved based on any message feature or content, such as respondent (sender), file type, subject line, key word, sound, image or another determined criteria search. Typically the data in a compliance data-base is read-only, and only modifiable by a compliance officer.

Archiving engine 502 may also generate useful summaries of emails and attachments as each message passes through the engine, provide management reports, etc and store that information in a database. The summary can then be used subsequently to locate emails based on content, recipient and so on.

It is important that any messages that are released from quarantine 606 via instructions given via user interface 604, or where the auto-archiving module is part of an integrated system of the type shown in Figures 1 and 4, through the user database 102 via interface 103, are also copied and stored in the auto-archive database.

A further feature for the platform for intelligent message management shown in Figure 4 is to extend these archiving capabilities to all message formats, to permit congruence of multiple-format digital information flows through a single portal. This means that all messages may be stored in a single place, in a format enabling uniform access and control over all messages. Storing of this uniform format is done on fault redundant systems with an effective search tool to interrogate and easily find stored messages, based on, for example, sender, recipient, content, and any other detail as may be specified to enable effective retrieval of required messages.

Referring now to Figure 7, which shows the essential features of the prioritisation module of the present invention in a schematic form, a message stream 120 carrying a processed message, which may be, for example, from filter module 112 disclosed above, is received by prioritisation module 504. The behaviour of the prioritisation module is determined by settings in a database 702 or where the prioritisation module is part of an integrated system of the type shown in Figures 1 and 4, through the user database 102, as described above, and depending on the settings in the user database, an outgoing delivery stream  $B_1, B_2, B_3 \dots B_N$  is chosen. The outgoing delivery may be for example and without limitation, an email message delivery, an SMS/text message, a MMS/multimedia message, a voice mail, a fax delivery, a pda/mobile delivery and so on, and the user determines which message stream is preferred for certain messages. For example, the user may elect to receive a text alert to a mobile device when a message from the user's lawyer is received. The xSP can then, at a fee, enable the end user to receive the message on the device of choice.

30  
35  
40

It is important that messages released from quarantine **606** via instructions given via user interface **604**, or where the prioritisation module is part of an integrated system of the type shown in Figures **1** and **4**, through the user database **102** via interface **103**, are also dealt with by the prioritisation module.

Messages may be prioritized, for example, according to sender, content or subject line, thus identifying to the user the immediacy of receipt and notification of receipt by end user, or administrator determined importance.

The action taken for high priority messages may include the following:

forwarding a copy of the message to a user-specified device; forwarding a copy of the message to a mobile service provider and 'pushing' an alert message to a mobile device to alert the user to 'pull' the copy message from the mobile service provider; forwarding the message to a Personal Assistant for action; alerting the user on receipt of a file type, such as .tif, a fax; forwarding the message to a distribution list; renewing an insurance premium in response to a communication; booking an airline ticket in response to a communication; acting on share information; acting on a virus alert.

The user may specify which device, devices or persons (such as another messaging protocol) he wishes messages to be sent, and these would include: a cell-phone; fax; VoIP; Pda.

Some delivery devices and actions may require format conversion or communication with an end-point web interface.

Action taken for low priority messages may include auto-archiving and the removal of the message as pre determined by the user and / or network administrator from the delivery queue, for example, messages from a particular sender may not be spam, but not be deemed worthy of receipt by the end user or administrator, such as messages from an ex-employee, or specific communication from a previous business or personal relationship.

Prioritization of emails and messages as described above could be further extended to allow scheduling of responses.

Thus, for example, high-priority messages should be responded within one hour, medium priority messages within one day, and low priority messages are essentially for information only. Reporting can be managed, and should response not be with pre determined parameters held in a database, further action can automatically be initiated, such as the message or message is forwarded to other personnel, a distribution list, a named contact, or other device, pda, mobile phone etc. and then that message be subject to predetermined priority levels and further actions as appropriate by the end user / administrator.

Priority information from content analysis can be further extended to include project-specific information to allow data to be automatically entered into tools such as Microsoft Project Manager, Outlook, or other scheduling, calendar systems, or Customer Relationship Management (CRM) systems. For example, sending out meeting or action reminder messages at scheduled times.

Additionally, failure to respond to messages within the required time could lead to the generation of alert messages and summary reporting.

Scheduling features may also include a reminder service according to parameters set by the user or administrator. For example, by SMS, SMTP message, VOIP, or other communications protocol as the end user may use.

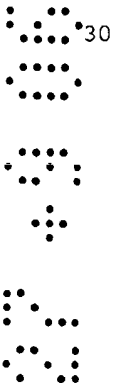
The prioritisation service may be applied to outbound messages also; for example, large messages may be sent overnight.

Although the foregoing disclosure contains many specificities, these should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments of this invention.

### Industrial Applicability

The foregoing describes a digital message filtering system that comprises a database module containing one or more configuration options relating to one or more end-users and a scanning engine module connected to the database module. The behaviour of the scanning engine module is modified on a message-by-message basis according to the configuration options for the end-users.

The digital message may be IM for text and image messaging computer to computer, SMS for text messaging via mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax. The digital message filtering system may additionally include a set-up process so that a third party database may be synchronized as appropriate with the database module. A message archiving system and a message prioritization system may also be also be part of the message filtering system, and the behaviour of the message archiving system and the message prioritization system may also be modified on a message-by-message basis according to the configuration options for the end-users. The message filtering system may additionally include a pre-filtering engine.





Claims

1. A message archiving system comprising:

- (a) a message stream (120);
- (b) an auto-archiving engine (612);
- 5 (c) a database (608); and
- (d) an auto-archive database (610);

characterised in that a behaviour of said auto-archiving module is determined by settings in said database so that if a particular message in said message stream falls within criteria specified in said database  
10 a copy of said message is added to said auto-archive database.

2. The message archiving system of claim 1 wherein said criteria comply with a regulatory code.

3. The message archiving system of claim 2 wherein said regulatory code is selected from the group consisting of: Sarbanes Oxley, HIPPPAA, and Basel  
15 II.

4. The message archiving system of claim 1 wherein said auto-archive database is a secure database.

5. The message archiving system of claim 4 wherein data stored in said database is read-only.

20 6. The message archiving system of claim 1 wherein said auto-archive database is external to said system.

7. The message archiving system of claim 1 wherein said auto-archiving database comprises a mechanism to compress messages.

8. The message archiving system of claim 1 wherein said message stream  
25 comprises messages of any format.

9. The message archiving system of claim 8 wherein said auto-archiving database additionally comprises a mechanism to convert multiple-format digital information to a uniform format.

10. The message archiving system of claim 8 wherein said auto-archiving  
30 database comprises a mechanism to search said auto-archiving database.

11. The message archiving system of claim 10 wherein said search is at a user level.

12. The message archiving system of claim 10 wherein said search is at a domain level.



13. The message archiving system of claim 1 wherein said auto-archiving database comprises a mechanism to allow access to stored messages according to different access permissions.
14. The message archiving system of claim 13 wherein said auto-archiving database comprises a mechanism to allow rapid access to stored messages by subject, content, sender or date.
15. The message archiving system of claim 13 wherein said auto-archiving database comprises a mechanism to allow access based on any message feature or content.
16. The message archiving system of claim 15 wherein said message feature or content is selected from the group consisting of: sender, file type, subject line, key word, sound, and image.
17. The message archiving system of claim 1 wherein said auto-archiving engine additionally comprises a mechanism to generate a summary of messages that have passed through the system.
18. The message archiving system of claim 17 wherein said summary is used subsequently to locate emails based on content, recipient and so on.
19. The message archiving system of claims 1-18 wherein said database is a user database (102).
20. The message archiving system of claim 19 wherein said criteria are set by a user.
21. The message archiving system of claim 20 wherein said criteria are selected from the group consisting of: sender, subject line, file type, key word, key sound, and key image.
22. The message archiving system of claim 20 wherein said user is a business or organisation
23. The message archiving system of claim 22 wherein said criteria apply to all individual users within said business or organisation.
24. The message archiving system of claim 20 wherein said criteria are set by an administrator.
25. A message filtering system, comprising a database module (102) containing one or more configuration options relating to one or more end-users, a scanning engine module (112) connected to said database module (102) and a message archiving system of claims 1-24, wherein said one or more configuration options for said one or more end-users modify the scanning engine module (112) behaviour and the message archiving system on a message by message basis.

26. The message filtering system of claim 25 additionally comprising a message prioritisation system.

27. The message filtering system of claims 25 and 26 wherein said scanning engine module comprises a pre-filtering engine.

5 28. The message filtering system of claims 25 and 26 additionally comprising a set-up process (104), wherein a third party user database is synchronized as appropriate with the user database.

29. The message filtering system of claims 25-28 wherein said message is an Email message.

10 30. The message filtering system of claims 25-28 wherein said message comprises a message selected from the group consisting of: IM for text and image messaging computer to computer, SMS for text messaging via mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax.

15 31. The message filtering system of claims 25-30 wherein a sender of a message is end-user of PIMM.

32. The message filtering system of claims 25-31 wherein a recipient of a message is end-user of PIMM.

20 33. The message filtering system of claim 25-32 in which said prioritisation system comprises:

- (a) a message stream (120);
- (b) prioritisation module (504); and
- (c) one or more delivery streams ( $B_1, B_2, B_3 \dots B_N$ )

25 characterised in that a behaviour of said auto-archiving module is determined by settings in said database module (102) so that if a particular message in said message stream falls within criteria specified in said database a delivery stream  $B_1, B_2, B_3 \dots B_N$  is chosen.

30 34. The message filtering system of claim 33 wherein said delivery stream comprises a delivery stream selected from the group consisting of: an email message delivery, an SMS/text message delivery, a MMS/multimedia message delivery, a fax delivery, a voice mail delivery, and pda/mobile delivery.

35 35. The message filtering system of claim 33 wherein said criteria are selected from the group consisting of: sender, message content, and subject line.

36. The message filtering system of claim 33 wherein a particular message in said message stream falls within criteria specified in said user database, said message is accorded a priority.

37. The message filtering system of claim 36 wherein said chosen delivery stream is to a device selected for said priority and specified in said database.

5 38. The message filtering system of claim 36 wherein if said priority is high the delivery stream chosen is a message stream to a mobile service provider.

10 39. The message filtering system of claim 36 wherein if said priority is high the delivery stream chosen is a message stream to a mobile service provider, said mobile service provider 'pushing' an alert message to a mobile device whereby a recipient of said alert message 'pulls' a copy of said particular message from the mobile service provider.

40. The message filtering system of claim 33 wherein a particular message in said message stream falls within criteria specified in said user database, said message is accorded a low priority.

15 41. The message filtering system of claim 40 wherein if said priority is low the delivery stream chosen is a stream to the message archiving system of claim X and the message is not delivered.

20 42. The message filtering system of claim 40 wherein if said priority is low and said message is from a particular sender no delivery stream chosen and the message is not delivered.

43. The message filtering system of claim 33 wherein said message stream comprises messages of any format.

25 44. The message filtering system of claim 43 wherein said prioritisation engine additionally comprises a mechanism to inter-convert multiple-format digital information.

45. The message filtering system of claims 25-44 wherein said criteria are set by a user.

30 46. The message filtering system of claim 25-45 additionally comprising a set-up process (104), wherein a third party user database is synchronized as appropriate with the user database.

35 48. The message filtering system of claims 46 or 47 for which information on a database (302) concerning a third party's message server (306) has been altered so that incoming messages from a message sender (300) is sent to said filtering system (304).

49. The message filtering system of claim 48 wherein said third party is an xSP or corporate organization.

50. The message filtering system of claim 48 wherein said xSP database contains subscription data for a new end-user to said xSP.

51. The message filtering system of claim 48 wherein said clean message is sent to a message server of said xSP, and thence to said end-user mailbox (308).

52. The message filtering system of claim 48 wherein said xSP has multiple end-users, and wherein said end-users are grouped according to specific domains and subdomains.

53. The message filtering system of claim 49 wherein default settings for said end-users may be set by an administrator of said domain or subdomain.

54. The message filtering system of claims 48-53 wherein said message is an Email message.

55. The message filtering system of claims 48-53 wherein said message comprises a message selected from the group consisting of: IM for text and image messaging computer to computer, SMS for text messaging via mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax.

56. The message filtering system of claims 46-55 wherein a sender of a message is end-user of PIMM.

57. The message filtering system of claims 46-55 wherein a recipient of a message is end-user of PIMM.

58. The message filtering system of claims 46-57 further characterized in that said scanning engine module (112) comprises at least one of:  
(a) an antivirus filter module (202);  
(b) an anti-spam filter module (212); and  
(c) a content control filtering module (222).

59. The message filtering system of claim 58 additionally comprising a quarantine queue (208, 220, 230) for secure holding of mail for each of said at least one of: said antivirus filter module (202), said anti-spam filter module (212) and said content control filtering module (222).

60. The message filtering system of claim 59 wherein messages may be released, forwarded, modified or deleted from said quarantine queue according to user level or domain level protocols held in said database.

61. The message filtering system of claim 58 further characterized in that said content control filtering module (222) comprises:  
(a) a first module (224) able to detect messages having attachments of a size greater than that specified in said database;  
(b) a second module (226) able to detect messages having attachments of specific file types specified in said database; and

(c) a third module (228) able to detect messages having specific subjects, message content or attachment file names specified in said database.

5 62. The message filtering system of claim 58 wherein said antivirus filter module (202) providing antivirus filtering for message and file attachments and whose behavior is determined by settings contained within said database module (112), comprises:

- 10 (a) a first module (204) able to detect messages having virus infection by examining signatures and detect known viruses by name; and  
(b) a second module (206) able to detect messages having virus infection by heuristic analysis of said message.

15 63. The message filtering system of claim 58 wherein said antispam filter module (212) for message and whose behaviour is determined by settings contained within a database module (112) and set by a user, or administrator on behalf of a user or group of users, comprises:

- 20 (a) a first module (214) able to analyze the structure of a message, its reputation and travel path  
(b) a second module (216) able to perform heuristic rule-based checks against a knowledge base and perform heuristic and/or Bayesian content analysis using heuristics and Bayesian model methodologies combined with individual word probabilities  
(c) a third module (218) able to detect hoaxes and phishing, and using White and Black Lists on global, domain and user level.

25 64. The message filtering system of claims 46-55 wherein said third party database and said user database have a format compatible with LDAP.

65. The message filtering system of claims 46-55 wherein said third party database and said user database have a format compatible with ActiveDirectory.

30 66. The message filtering system of claims 46-55 wherein said third party database and said user database have an SQL format.

67. The message filtering system of claims 46-55 wherein said third party database is a master and said user database is a slave.

68. The message filtering system of claims 46-55 wherein said third party database is a slave and said user database is a master.

35 69. The message filtering system of claims 46-55 wherein said third party database and said user database use both-ways synchronisation.

70. The message filtering system of claims 46-55 wherein said third party database contains information including information on people, organizational units, printers, documents, or groups of people.

71. A method for archiving messages comprising the steps of:  
    (a) receiving a message from a message stream (120);  
    (b) comparing said message to criteria in a database (610); and  
    (c) copying a message to an auto-archive database (610) if said message  
5       falls within said criteria.
72. The method of claim 71 wherein said criteria comply with a regulatory  
code.
73. The method of claim 72 wherein said regulatory code is selected from the  
group consisting of: Sarbanes Oxley, HIPPA, and Basel II.
- 10 74. The method of claim 71 wherein said auto-archive database is a secure  
database.
75. The method of claim 74 wherein data stored in said auto-archive database  
is read-only.
76. The method of claim 71 additionally comprising the step of comprising  
15 said message if said message falls within said criteria.
77. The method of claim 71 wherein said message stream comprises messages of  
any format.
78. The method of claim 77 additionally comprising the step of converting  
multiple-format digital information to a uniform format if said message  
20 falls within said criteria.
79. The method of claim 77 additionally comprising the step of searching  
said auto-archiving database.
80. The method of claim 79 wherein said search is at a user level.
81. The method of claim 80 wherein said search is at a domain level.
- 25 82. The method of claim 71 additionally comprising the step of allowing  
access to said auto-archiving database according to different access  
permissions.
83. The method of claim 82 wherein access is according to subject, content,  
sender or date.
- 30 84. The method of claim 82 wherein access is according to any message  
feature or content.
85. The method of claim 84 wherein said message feature or content is  
selected from the group consisting of: sender, file type, subject line,  
key word, sound, and image.
- 35 86. The method of claim 71 additionally comprising the step of generating a  
summary of messages that have passed through the system.

87. The method of claim 86 wherein said summary is used subsequently to locate emails based on content, recipient and so on.

88. The method of claims 71-87 wherein said database is a user database (102).

5 89. The method of claim 88 wherein said criteria are set by a user.

90. The method of claim 89 wherein said criteria are selected from the group consisting of: sender, subject line, file type, key word, key sound, and key image.

91. The method of claim 90 wherein said user is a business or organisation

10 92. The method of claim 91 wherein said criteria apply to all individual users within said business or organisation.

93. The method of claim 90 wherein said criteria are set by an administrator.

94. A method for filtering messages comprising the steps:

15 (a) receiving a message for an end-user;

(b) identifying one or more configuration options related to said end-user held in a user database module;


(c) modifying a behaviour of a scanning engine module according to said one or more configuration options;

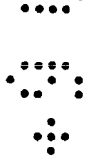
20 (d) scanning and filtering said message according to said configuration options; and

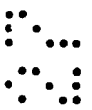
(e) archiving said message according to the method of claim 84-106 wherein said database is the user database module (102).

25 95. The method of claim 94 additionally comprising the step of prioritising said message.

96. The method of claims 94-95 additionally comprising synchronizing a third party user database as appropriate with the user database according to a set-up process.

 30 97. The message filtering system of claims 94-96 wherein said message is an Email message.

 35 98. The message filtering system of claims 94-96 wherein said message comprises a message selected from the group consisting of: IM for text and image messaging computer to computer, SMS for text messaging via mobile devices, VoIP for communication via telephony, MMS for transmission of images, 3GP for transmission of video, and Fax.

 99. The method of claims 94-96 additionally comprising pre-filtering said message according to the steps:



- (a) identifying a digital message that is not capable of carrying an unwanted or undesirable component prior to full scanning of said message by filtering software;
- (b) passing said message identified as not capable of carrying an unwanted or undesirable component to a data stream not requiring full scanning of said message by filtering software;
- (c) passing other messages not identified in step (a) as not capable of carrying an unwanted or undesirable component to a module able to do a full scan of said message.

10 100. The method of claim 99 wherein said unwanted or undesirable component is a virus and wherein said step of identifying a digital message that is not capable of carrying a virus comprises:

- (a) detecting the presence of an attachment to said message;
- (b) detecting an embedded element (for example iFrame /ActiveX code) able to download potentially malicious code from the internet when said message is received, or opened;
- (c) detecting whether or not said message had a link to a website that could cause a virus to be downloaded;
- (d) detecting whether or not an originator of said message is blacklisted as a virus distribution server or user.

101. The method of claim 99 wherein said unwanted or undesirable component is spam and wherein said step of identifying a digital message that is not capable of carrying spam comprises:

- (a) detecting whether or not the originator state is a known source of spam;
- (b) detecting whether or not the sending program is probably bulk rather than personal;
- (c) detecting whether or not the structure of the message is poor and may contain lazy html.

30 102. The method of claim 99 wherein said unwanted or undesirable component is message content and wherein said step of identifying a digital message that is not capable of carrying spam comprises: detecting the presence of an attachment to said message.

103. The method of claim 99 wherein said step of passing said message identified as not capable of carrying an unwanted or undesirable component to a data stream not requiring full scanning of said message by filtering software additionally comprises passing said message via said data stream to the filter of claim 3.

104. The method of claim 99 wherein if said message is not capable of carrying an unwanted or undesirable component to a data stream not

requiring full scanning of said message by filtering software additionally comprises passing said message via said data stream to the filter of claim 4.

5 105. The method of any of claims 99 to 104 wherein if said message is not capable of carrying an unwanted or undesirable component to a data stream not requiring full scanning of said message by filtering software additionally comprises passing said message via said data stream to a user inbox.

10 106. The method of claim 95 wherein said step of prioritising said message comprises the steps of:  
(a) receiving a message from a message stream (120);  
(b) comparing said message to criteria in said database;  
(c) delivering said message to a delivery stream  $B_1, B_2, B_3 \dots B_N$  if said message in said message falls within criteria.

15 107. The method of claim 106 wherein said delivery stream comprises a delivery stream selected from the group consisting of: an email message delivery, an SMS/text message delivery, a MMS/multimedia message delivery, a fax delivery, a voice mail delivery, and pda/mobile delivery.

20 107. The method of claim 106 wherein said criteria are selected from the group consisting of: sender, message content, and subject line.

109. The method of claim 106 wherein said step of comparing said message to criteria in a database comprises according a priority to said message if said message falls within said criteria.

25 110. The method of claim 109 wherein said step of delivering said message to a delivery stream comprises selecting a deliverer stream for said priority as specified in said database.

111. The method of claim 109 wherein if said priority is high the delivery stream selected is a delivery stream to a mobile service provider.

30 112. The method of claim 111 wherein comprising the additional steps of:  
(a) 'pushing' an alert message from said mobile service provider to a mobile device;  
(b) 'pulling' a copy of said particular message from the mobile service provider by a recipient.

35 113. The method of claim 106 wherein a particular message in said message stream falls within criteria specified in said user database, said message is accorded a low priority.

114. The method of claim 113 wherein the delivery stream chosen is a stream to a message archiving system and the message is not delivered.

115. The method of claim 109 wherein if said priority is low and said message is from a particular sender no delivery stream is chosen and the message is not delivered.

116. The method of claim 106 wherein said message stream comprises messages of any format.

117. The method of claim 116 additionally comprising the step of inter-converting wherein said multiple-format digital information.

118. The method of claim 106 additionally comprising the step of allowing a user to set said criteria.

119. The method of claim 96 wherein said step of synchronising comprises the steps:

(a) accessing a first field in said third party database;

(b) accessing a corresponding field in said user database

(c) determining whether data in said first field in said third party database is newer than data in said corresponding field in said user database; and

(d) replacing said data in said corresponding field in said user database with said data in said first field in said third party database if said first field in said third party database is newer than data in said corresponding field in said user database.

120. The method of claim 119 additionally comprising the step of replacing said data in said first field in said third party database with said data in said corresponding field in said user database if said first field in said third party database is older than data in said corresponding field in said user database.

121. The method of claim 119 and 120 in which said third party database has a format selected from the group consisting of: LDAP, ActiveDirectory, Oracle, MS SQL, and MySQL.

122. The method of claim 119 and 120 in which said user database has a format selected from the group consisting of: LDAP, ActiveDirectory, Oracle, MS SQL, and MySQL.

123. The message filtering system of claim 27 wherein said pre-filter is able to identify a digital message that is not capable of carrying an unwanted or undesirable component prior to full scanning of said message by filtering software wherein if said message is not capable of carrying said unwanted or undesirable component said message is not passed to a module able to do a full scan of said message and if said message is

capable of carrying said unwanted or undesirable component said message is passed to a module able to do a full scan of said message.

124. The pre-filter of claim 123 wherein said unwanted or undesirable component is a virus and wherein said pre-filter comprises one or more of the following component modules:

- (a) a module able to detect the presence of an attachment to said message;
- (b) a module able to detect an embedded element (for example iFrame /ActiveX code) able to download potentially malicious code from the internet when said message is received, or opened;
- (c) a module able to detect whether or not said message had a link to a website that could cause a virus to be downloaded;
- (d) a module able to detect whether or not an originator of said message is blacklisted as a virus distribution server or user.

125. The pre-filter of claim 123 wherein said unwanted or undesirable component is spam and wherein said pre-filter comprises one or more of the following component modules:

- (a) a module able to detect whether or not the originator state is a known source of spam;
- (b) a module able to detect whether or not the sending program is probably bulk rather than personal;
- (c) a module able to detect whether or not the structure of the message is poor and may contain lazy html.

126. The pre-filter of claim 123 wherein said unwanted or undesirable component is message content and wherein said pre-filter comprises a module able to detect the presence of an attachment to said message.

127. A pre-filter comprising the filter of claim 124 wherein if said message is not capable of carrying a virus said message is passed to the filter of claim 3.

128. The pre-filter of claim 127 wherein if said message is not capable of carrying spam said message is passed to the filter of claim 4.

129. The pre-filter of claims 124-128 wherein if said message is not capable of carrying said unwanted or undesirable component it is passed to a user inbox.



For Innovation

39

Application No: GB0618187.9

Examiner: Kalim Yasseen

Claims searched: 1-129

Date of search: 19 December 2006

### Patents Act 1977: Search Report under Section 17

#### Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-25.	WO2004/003704 A2 (PRGRS) see whole document especially page 7 line 3 to page 9 line 32
X	1-25	US2004/0133645 A1 (MASSANELLI) see whole document especially paragraphs 26-45
X	1-25	US2004/0254988 A1 (RODRIGUEZ) see whole document especially paragraphs 12, 35, 36
X	1-25	EP1509014 A2 (SOPHOS) see whole document especially paragraph 18

#### Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

#### Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC<sup>X</sup>:

Worldwide search of patent documents classified in the following areas of the IPC

H04L

The following online and other databases have been used in the preparation of this search report

Online: EPODOC, WPI