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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 February 2007 (08.02.2007)

PCT

(10) International Publication Number
WO 2007/015266 A2

(51) International Patent Classification:
G06F 12/16 (2006.01) *G06F 7/24* (2006.01)

(21) International Application Number:
PCT/IN2006/000269

(22) International Filing Date: 31 July 2006 (31.07.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2057/DEL/2005 2 August 2005 (02.08.2005) IN

(71) Applicant and
(72) Inventor: **MADHOK, Ajay** [IN/IN]; Sector 43, Unitech Trade Centre, Gurgaon, Haryana, Gurgaon 122002 (IN).

(74) Agent: **JOTWANI, Dinesh**; 81 National Park, Lajpat Nagar 4, New Delhi 110 024 (IN).

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

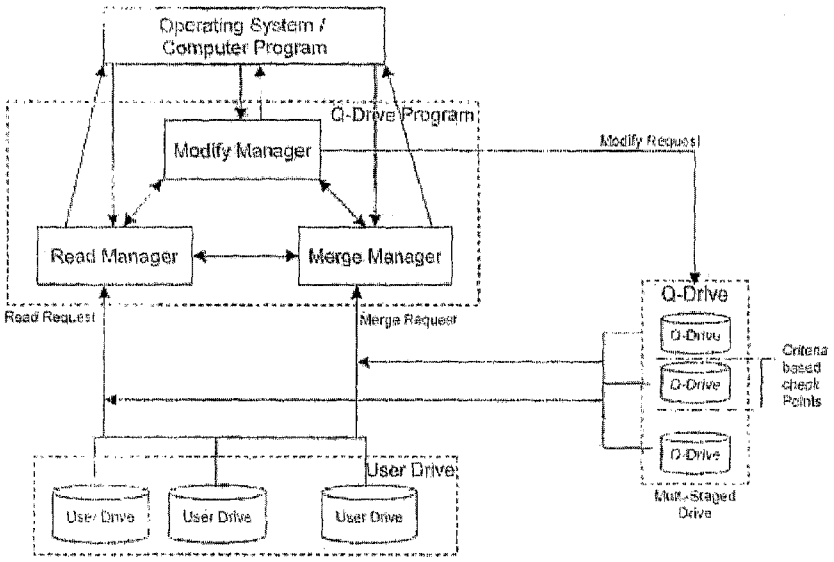
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT,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

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

Published:
— *without international search report and to be republished upon receipt of that report*

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

(54) Title: SYSTEM AND METHOD OF TIME BASED HIERARCHICAL STORAGE MANAGEMENT



(57) Abstract: The present invention is a method to prevent complete data loss by means of a time based hierarchical storage that allows any new or modified data to be incubated or staged on any differentiated drive(s), data storage area(s), device(s), etc. for a predefined period of time. The invention is a method to effect or commit changes made in the incubated drive(s) / device(s) etc. after expiration of a pre-definable quiescent period of pre-emptive quarantine of incubated data on being attested as free from the effect of malicious software(s), accidental defects, etc. The invention is a method to prevent accidental data loss by recovering changed data from the incubated drive(s), etc. Further, the invention is a method to seamlessly furnish requested data and related information regardless of the respective underlying drive(s) etc. The method also limits the data loss in case of known or unknown malicious software attack to the data in the incubation drive(s), device(s), only.

WO 2007/015266 A2

System and Method of time based hierarchical storage management

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention relates generally to computer data, systems and networks. In particular, the present invention is a method to prevent complete data loss in case of malicious software attacks or intentional or accidental modifications or deletions or corruption, by means of a time based hierarchical storage that allows any new or modified data to be incubated or staged on any logically or physically differentiated drive(s), data storage area(s), device(s), etc. for predefined period(s) of time.

2. Description of the Prior Art

As the use of computers and their interconnection becomes widespread, computer "malware" or "malicious software" like viruses, worms, trojan horses, spyware and adware are becoming dominant causes that plague and compromise the security and / or privacy of users. Malware is a term used to define a "malicious software" or a combination of these, that infiltrate a system, computer or otherwise, without the consent of the owner, usually with the intent of causing damage to the host system.

Obviously, because of the destructive / interfering nature of such malicious software, there is a need for eliminating them from computer systems and networks.

The need is reiterated by the findings of a recent survey (Source: America Online & National Cyber Security Alliance, 2005) that states that 68% of the users keep sensitive information on their computer.

Malicious software could enter any user's PC through any medium like internet download(s), email(s), CD-ROM, removable disk(s), etc. Another related survey suggests that a substantial percentage of data loss is caused due to viruses (16% of the emails, were infected by viruses in the year 2004 and upto about 7% of all data loss was due to virus). The prior art uses various malicious software detection programs to end the proliferation of malware. Malware checking application programs or Anti-virus software are currently available for checking malicious software on individual computers. The user needs to update anti-virus software on a regular basis to obtain new virus definitions. Again a recent survey (Source: America Online & National Cyber Security Alliance, 2005) suggested that 56% of the computer users either don't have or don't update their anti-virus definitions on a regular basis.

As the size of storage on computers is growing fast, the said activity of virus scan is increasingly taking a large amount of time. Another related

survey suggests that during normal usage most (over 98%) data remains unchanged between two successive sessions. Any data that has not changed is also typically not affected by malware and scanning only the changed data can be finished in a relatively smaller time.

Most of the computers today are protected from malware attack using Anti-virus solutions. Anti-virus software programs typically use of one of two techniques, described herein, for detecting malware. One comprises of examining the file for known viruses, employing methods to match virus "definitions" or "signatures" from a virus "dictionary" or "database", while the other comprises of detecting suspicious behavior (similar to what a virus typically exhibits) from any program. Anti-virus solution providers update the signature databases regularly for new malicious software found since the last update and provide means to download updates to user systems. Computers are still open for such attack if the virus database does not contain the virus signature (unknown virus) or user has not downloaded the most appropriate update.

Another approach for precaution against virus attacks or intentional / accidental data loss is based on simultaneous or periodic data back up. This is pivoted on either real-time mirroring or synchronous back up, or at chosen / regular time intervals with fixed / uncertain periodicity for back up. Non-automatic processes requiring human intervention for initiating back up often suffer from the lack of discipline needed to

sustain / maintain the cyclical repetitiveness of backing up data. Periodic data dump to a designated back up data storage area in physically or logically contiguous drives or devices or network nodes / areas is handicapped by the volume of data to be regularly backed up and the intervening changes in the main data. Any malware can propagate into the back up arena and users need to be cautious about the cleanliness of the data being backed up. The issue of volume of data is tackled by versioning control or incremental back up wherein only the changed computer data is backed up. Incremental back up can also be further narrowed down to back up of smaller data segment(s) or elements of data with, or without, corresponding log of change(s). Data chronicles or logs facilitate check-point restart or rollback but there are significant deficiencies. Micro level management at a physical hardware level increases complexity tremendously. In tackling bits and bytes microscopically, choice of data prioritization, classification, differential criticality etc. for various data types is minimal. Choices do not expand significantly in solutions that operate at an aggregate level of device(s). Thus a malware attack induced by a single computer file may cause other data to be also rolled back to any previous snapshot of the back up store, at an earlier point in time. A multiplicity of back up threads may be handling different distinct logical aggregations of data but outbound multi-thread back up, streaming data out of a user's computer system or drive(s), may not result in prioritized or synchronized data recovery. Further, the vulnerability of malware propagation always remains.

Also, most of the Anti-virus solutions offered today suffer from the drawback that any malware has to be recognized first: only thereafter can a user be protected against the associated threat. In the meantime, the (unknown) malicious software continues to inflict damage to many computer systems till its antidote is found and updated in the virus database(s) on user's system(s). Therefore, what is required is a system and method that works transparently and leverages the existing anti-virus solutions offered by different companies.

Therefore, it is an object of the invention to provide a system and method that overcomes deficiencies in the prior art.

SUMMARY

An object of the present invention is to a develop a method to prevent complete data loss in case of any malware attack or intentional or accidental modifications or deletions or corruption of data, by means of a time based hierarchical storage that allows any new or modified data to be incubated or staged on any logically or physically differentiated drive(s), data storage area(s), device(s), etc.

Another object of the present invention is to treat any new or modified data as uncertified from a malware linkage or safety perspective and in default caution to cause pre-emptive quarantine of such new / modified data to incubated drive(s), data storage area(s), device(s), etc. generically called Quarantine Drive(s) or Q-drive(s). Q-drives may have different safety index zones through which data may bypass / flow

through in sequential stages, akin to multiple security check points, based upon user defined parameters.

Another object of the present invention is to allow the user to specify a quiescent period during which incubated data remains relatively isolated from user drive(s), in the incubated drive(s), data storage area(s), device(s), etc. Changes made in the incubated drive(s) / device(s) etc. are committed to the user drive(s) after expiration of the quiescent period of pre-emptive quarantine of incubated data on being attested as free from the effect of malware, accidental defects, etc. The quiescent period phase lag may be for a single stage or more stages or different levels of safety index zones through which data may traverse.

Another object of the present invention is to permit different quiescent times to be defined for various types of data besides other parameters specified by users pertaining to relative prioritization or criticality of data, maintained on incubated drive(s), data storage area(s), device(s), etc. as a collection of transient computer files or file segments together with a chronicle log associated with each. Such transient files may be kept for archive purposes even after relevant data has traveled to and updated the user drive(s) after crossing 'multiple security gates'.

Another object of the present invention is to prevent accidental data loss by recovering changed data from incubated drive(s), data storage area(s), device(s), etc. - which is held for quiescent period(s) in

sequential / leap-forward quarantine stages for various different types of data as defined by users and may travel from one stage to another physically, or logically, or through modification of indexes or pointers or directories, etc. within the Quarantine-drive(s) or Q-drive(s).

Another object of the present invention is a method to seamlessly furnish requested data and related information regardless of the respective underlying drive(s) etc. while allowing the user to access or be presented with a view of any new or old or modified data, irrespective of whether the relevant data resides partly or fully on the user drive(s), or Q-drives(s), or any possible permutation or combination.

Another object of the present invention is to minimize or limit the data loss in case of known or unknown malicious software attack to the data in the Q-drive(s) only. Further, the detection of updates to malicious software cleaning programs and associated databases along with frequent execution of Anti-virus software programs helps in maintaining purity of data. Based upon user choice the data on Q-drive(s) can be scanned through multiple Anti-virus software programs also. In order to preserve / retain sterility of data, Q-drive(s) may exist on heterogeneous computer systems in a network or any other connectivity of heterogeneous computer(s) or processor(s) in tandem.

DEFINITIONS AND PRESUMPTIONS

File / Computer File:

A computer file is one of the most basic, logical forms of storage within a computer system. A computer file is typically identified, though not limited to, by unique names called the full path names or file names. Other attributes are also associated with the computer file based on the type of computer system it resides upon. The meta-data / attributes typically contain size information, time of modification, time of creation, permissions to access the computer file, etc. Computer files provide ways to store temporarily or permanently, user as well as program information.

File Operation:

Computer files residing in a computer system are used by users of the computer system through computer programs, which are activated either automatically or on user requests. These programs then perform various activities on the computer file. A file operation typically consists of a file create operation where the file is created, a file modify operation which involves addition or deletion of information within the file, file delete operation where the files are removed from the computer system when they are no longer required, file attribute change operations where the attributes of a file may be changed to acquire the respective result this may cause, etc.

User Drive(s):

Various computer storage types, like hard disks, floppy disks, flash memory, optical discs, magneto-optical discs, etc. are represented by some computer systems and computer programs as drives. These logical drives provide a logical distinction, apart from simplicity of usage of computer files residing on the computer system. The user drive is a logical entity which can be said to represent the logical drive or a section of a logical drive or a collection of these sections within and / or across logical drives, which contains the user related or user specified computer files.

Computer Network:

A computer network is the system / technology which enables one or more computers to communicate with each other. These networks could span across distances from a few centimeter to thousands of kilometers. Computer networks are widely used for sharing information between computer systems.

Malicious Software / Malware:

Malicious software, also referred to as malware or computer contaminants, are undesired computer programs which are intentionally or unintentionally brought into a computer system and may cause extensive damage or undesirable changes to computer files and user information residing within. These include computer viruses, worms, trojan horses, spyware, adware, etc. These contaminants usually enter into the computer system through user actions such as executing

contaminated programs, downloading infected e-mail, etc. The computer system may also be contaminated by other users with malicious intentions who may have gained access to the computer system.

Anti-virus Systems / Spyware Detection Systems:

Used synonymously within this document, Anti-virus systems, spyware Detection and removal systems etc, are computer programs which can repair a contaminated computer system and / or file by removing the contaminant or preventing access to the particular file in the case or a non repairable contaminant. The process of limiting the spread of an infection by preventing access to the contaminated resource(s) is also typically referred to as a quarantine procedure.

Such Anti-virus computer programs typically use two different techniques to accomplish this:

1: Examining computer files to look for known signatures of contaminants

2: Identifying suspicious behavior of a computer program, which could be any operation that the program has performed which is neither authorized by the user nor a part of the normal program behavior.

Most of such programs use both of these approaches, with some programs emphasizing on the dictionary approach.

Hierarchical / Incremental Storage:

A backup program is a computer program designed to store computer files at a different location from the original computer file, for the purpose of recovering from an intentional or unintentional damage to a computer file. Backup programs generally support full / incremental / hierarchical backups. Often, only computer file contents that are newer or changed, compared to the previously stored information, are stored, thereby dramatically increasing the speed of the backup process. Backup programs may also store information about every operation performed on the computer file. This procedure enhances the recovery of a computer file to a state prior to the time when a particular operation was performed on the computer file.

Q-drive / Quarantine Drive:

Q-drive or the Quarantine Drive, used synonymously in this document, refers to a logical storage area. This logical storage area may reside on any of the storage types like hard disks, floppy disks, flash memory, optical discs, magneto-optical discs, etc or even a location on a computer network or a computer or processor in tandem. The purpose of the Q-drive is to provide a mechanism to isolate file operations being performed on a computer file residing on the user drive and related meta-data for a period of time. Once the file operations and the information associated with the operation, are confirmed by the anti-virus / malware detection and removal programs as safe, these changes are still stored on the Q-drive for a specified time period, referred to as

Q-time. The purpose of Q-time is to accommodate for new virus / malware information updates. Typically there is a time difference between the birth of a virus or malware and the release of the removal information and updates to the anti-virus / malware removal programs by the respective vendors of these programs. Once the file operations are Q-time old and are certified to be contaminant free, these file operations and the information associated with the operation, are applied onto the computer file on the user drive. During the Q-time for a computer file, any file operation pertaining to the user file is processed to and from the Q-drive. At a simplistic level a Q-drive may be a physically or logically distinct singular drive. Alternately, it may be very widely distributed in compartmentalized multiplicity across various heterogeneous systems in tandem or in a network. Besides a time sequence hierarchy, it envelopes hierarchy ranging from a single stage to more stages or different levels of safety index zones through which data may physically or logically traverse while in incubation mode on the Q-drive(s).

Phrases & Words

The singular includes the plural and vice-versa, unless repugnant to the context. Phrases are gender neutral

Brief Description of the Drawings

The preferred embodiments of the invention will hereinafter be described in conjunction with the appended drawings provided to illustrate and not to limit the invention, wherein like designations denote like elements, and in which:

Figure 1 is a diagram that illustrates an overview of the system in accordance with one embodiment of the present invention.

Figure 2 is a flow chart that illustrates an overview of the system in accordance with one embodiment of the present invention.

Figure 3 is a flow chart that illustrates the procedure for furnishing data on every read request in accordance with an embodiment of the present invention.

Figure 4 is a flow chart that illustrates the procedure for executing every data modification request in accordance with an embodiment of the present invention.

Figure 5 is a flow chart that illustrates the procedure for executing every file delete request in accordance with an embodiment of the present invention.

Figure 6 is a flow chart that illustrates the procedure for executing every data or file restore request in accordance with an embodiment of the present invention.

Figure 7 is a flow chart that illustrates the procedure for executing manual or automated Malware scan request in accordance with an embodiment of the present invention.

Figure 8 is a flow chart that illustrates the procedure for presenting data for user's view in accordance with an embodiment of the present invention.

Figure 9 is a flow chart that illustrates the procedure for executing every merge request in accordance with an embodiment of the present invention.

Figure 10 is a flow chart that illustrates the procedure for executing every anti-malware software update request in accordance with an embodiment of the present invention.

While the invention is amenable to various modifications and alternative forms, specific embodiments of the invention are provided as examples in the drawings and detailed description. It should be understood that the drawings and detailed description are not intended to limit the invention to the particular form disclosed. Instead, the intention is to

cover all modifications, equivalents and alternatives failing within the spirit and scope of the invention as defined by the appended claims.

DETAILED DESCRIPTION

Figure 1 represents the interaction between the operating system or computer program(s), Q-drive Program, Q-drive and the User Drive on / across computer system(s).

Typically all requesting applications referencing / modifying any file data on the user device(s) / drive(s) route the request(s) through the operating system, which retrieves / writes the required file data from / to the user disk. Q-drive Program intercepts all such requests for the file data on either User Drive / Q-drive, and the respective operation Manager furnishes the request either from the User drive or Q-drive or both, depending on the nature of the request and the location of the requested file data. The file data stored on the Q-drive may be placed on any of the safety index zones depending on a set of defined criteria, and may traverse within these zones depending on same or another set of defined criteria.

The diagram illustrates the interaction for three such requests -

Read request: The request is intercepted by the Read Manager component of the Q-drive Program. The Read Manager retrieves the requested file data from the appropriate drive(s) and services the requesting computer program.

Modify / Write request: The request is intercepted by the Modify Manager component of the Q-drive Program. The Modify Manager

creates / appends to the modify Log depending on number of times the file has been accessed for any such modification. The Log can be used in restore or merge operations on the said computer file.

Merge request: The request is intercepted by the Merge Manager component of the Q-drive Program. The Merge Manager retrieves the requested file data from the appropriate drive(s) and after attesting the data using appropriate Anti-virus program(s), merges (and copies / transfers) to the User Drive(s).

Figure 2 is a flow chart that illustrates an overview of the system in accordance with one embodiment of the present invention.

File operations performed either by the computer user or a computer program are analyzed by the Q-drive computer program. The file operations are serviced based on the type of the file operation using the logic described in the following flow charts. The invention currently services commonly used file operations, but may be extended for other file operations. The Q-drive uses the Hierarchical / Incremental Storage procedure to save information about the file operations on the Q-drive. All file operations pertaining to a particular computer file are saved as logs on the Q-drive. These logs contain the information about the file operation like the operation type, time at which the operation was performed, file property changed affected by the operation, the actual

information within the computer file that was changed or added or deleted, etc.

Figure 3 is a flow chart that illustrates the procedure for furnishing data on every read request in accordance with an embodiment of the present invention. Typically read file operations, represent operations where a user or a computer program intends to retrieve information from a stored file on the computer system. The Q-drive computer program analyzes the read operation where it is presented by the name of the computer file to be read, along with the data offset of the information required and the length of the information required. The Q-drive computer program then checks for the existence of the file on the Q-drive. In case of the file being present only on the user drive the request is serviced from the user drive, else it is serviced from the Q-drive. The required information is read from the appropriate drive and serviced back to the requesting user or computer program. However, there may be cases where the read operation has been requested on a data offset and length that is spread between the Q-drive and the user drive. In this kind of a fragmented file operation, the Q-drive computer program reads the appropriate information from both the Q-drive and the user drive to service the file operation requested.

Figure 4 is a flow chart that illustrates the procedure for executing every data modification request in accordance with an embodiment of the present invention.

Typically modify file operations, represent operations where a user or a computer program intends to modify information present in a computer file, by adding new information to the computer file, or updating any existing information within the file or removing any unnecessary information within the computer file. The Q-drive computer program analyzes this request where it is presented with the name of the computer file to be read, along with the data offset of the information required and the length of the information required. The Q-drive computer program then checks if this is the first operation on the computer file. This case may arise in any of the following cases:

- The computer file existed on the user drive before the Q-drive program was initially activated on the computer system
- A new computer file is being created on the computer system.

In either case the Q-drive program logs the first entry on the Q-drive and saves the information pertaining to the file operation on the Q-drive. In the case of the computer file information already residing on the Q-drive, the Q-drive computer program adds the information pertaining to the file operation to the previously saved information about the computer file already present on the Q-drive. Any changes made by user, computer programs and malware are saved on the Q-drive as modify log information. Hence the file residing on the user drive is free from any malware contamination. Upon detection of malware initiated

modify operations these operations can be un-done to restore a contaminant free version of the computer file.

Figure 5 is a flow chart that illustrates the procedure for executing every file delete request in accordance with an embodiment of the present invention.

Typically delete file operations, represent operations where a user or a computer program intends to remove all information present in a computer file and often the computer file itself from the computer system. The Q-drive computer program analyzes this request where it is presented with the name of the computer file to be deleted. The Q-drive program updates the information previously present on the Q-drive to mark the file as deleted. In case of a new file, the Q-drive program first follows the procedure to log information about the new file as described in the modify operation. All information pertaining to the computer file present on the user drive is moved to the Q-drive. The computer file is then deleted from the user drive. It is important to note that the information about computer file though deleted from the user drive, still resides on the Q-drive. In the case of an accidental deletion by the user or malware initiated deletion, this information could be at a later point in time, used for restoring the file in its entirety or to any previous version of the file as described further in the description of the restore file operation.

Figure 6 is a flow chart that illustrates the procedure for executing every data or file restore request in accordance with one embodiment of the present invention.

Typically restore file operations, represent operations where a user or a computer program intends to un do any one or more file operations performed on the computer file. The Q-drive computer program analyzes this requested where it is presented with the name of the computer file to be restored and the previous time or file operation that the computer file has to be restored to. The Q-drive then checks if the file exists on the Q-drive in which case it has already logged information about any file operations that have been performed on the computer file since the first log on the Q-drive. The Q-drive computer program can then present the user or the computer program with the log information retained on the Q-drive. The computer file can then be restored to a previous version by un doing one or more of the file operations performed on it. The Q-drive computer program can not perform the restore operation on computer files, for which it does not have any file operation logs.

Figure 7 is a flow chart that illustrates the procedure for executing manual or automated Malware scan request in accordance with one embodiment of the present invention.

The Q-drive computer program periodically performs malware checking on all the log entries of all files residing on the Q-drive. This malware check is performed using the commonly available Anti-virus Systems /

spyware Detection Systems. The updates to these computer programs are performed by the procedure that the vendors for these computer programs recommend. Depending on the type of malware and the type of the detection and removal computer programs some malware contamination may be irreparable, in which case the Q-drive computer program deletes the particular log entry or entries that this infection is present in, to recover an un-contaminated version of the computer file. In case of a successful repair of the computer file, the log entries are cleaned and saved back on to the Q-drive. A check is also made for a Q-time age for the file operation log entries. File operation log entries which are not Q-time old are retained on the Q-drive. The logic behind the Q-time bases itself on the premise that there may be computer contaminants which are presently unknown and the updates to combat the contaminant may be provided by the Anti-virus Systems / spyware Detection Systems vendors with a certain delay after detection of the particular contaminant. The Q-time hence accommodates for the time taken by the Anti-virus Systems / spyware Detection Systems vendors to provide for an appropriate update to their computer programs to combat the contaminant. File operation log entries which are more than Q-time old and certified contaminant free by the Anti-virus Systems / spyware Detection Systems are merged to the Q-drive to the user drive by the Q-drive computer program. These log entries are then removed from the Q-drive to accommodate for newer file operations which may be performed on the computer file.

Figure 8 is a flow chart that illustrates the procedure for presenting data for user's view in accordance with one embodiment of the present invention.

Users and computer programs typically find a requirement to check the properties of a computer file, like the size of the computer file and etc. Since the information about the computer file may reside both on the user drive and the Q-drive, the Q-drive computer program services these requests by processing all the information available about the computer file on the user drive and the Q-drive and presenting the latest information pertaining to the computer file as though it were residing on the user drive itself.

Figure 9 is a flow chart that illustrates the procedure for executing every merge request in accordance with one embodiment of the present invention.

File merge refers to a merge request wherein the data on the Q-drive is merged (and transferred) to the User Drive(s). This can either be manual (or user triggered) or automated. In either case, an anti-virus check is invoked, post which if the data is slated clean from any kind of malware, it is moved / merged on to the User Drive(s) and the respective data is removed from the Q-drive, or alternately, the data is cleaned if found reparable or deleted, if not reparable.

Figure 10 is a flow chart that illustrates the procedure for executing every anti-malware software update request in accordance with one embodiment of the present invention.

The Q-drive computer program periodically checks for updates to Anti-virus Systems / spyware Detection Systems as recommended and suggested by the vendors. Upon detection of a new update the Q-drive program either applies the update by itself or requests the Anti-virus Systems / spyware Detection Systems to update their contaminant definitions and removal procedures. Computer users often are either ignorant of or neglect the update procedures recommended by the vendors of the malware detection and removal programs, hence the Q-drive computer program tries to keep the computer system up-to-date by performing periodic updates as required.

While the illustrative embodiments of the invention have been described, it will be clear that the invention is not limited to the aforesaid only. Numerous modifications, changes, variations, substitutions and equivalents will be apparent to those skilled in the art without departing from the spirit and scope of the invention as described in the claims.

CLAIMS

We claim:

1. A method to contain data loss to pre-defined pre-emptive isolation / incubation time period(s) in the event of a malware attack or intentional or accidental modifications or deletions or corruption, said method utilizing management of the existing logically or physically differentiated multi-staged storage device(s) and Anti-virus cleaning program(s), said method comprising the steps of:

directing and storing of file(s) that is / are created or modified by the user to the appropriate stage on a multi-staged Q-drive;

recording relevant details of the said file data and operations performed in the form of a log on the Q-drive;

running a periodic or manual Anti-virus scan over the said file data in the multi-staged Q-drive and in case of malware presence confirmation, cleaning the data if repairable or alternately restoring the said data to a prior known safe state; and

moving and merging the file data onto the User Drive or an appropriate stage on the Q-drive after the same has become older than 'defined time period' (Q-time) as per available log(s) and subject to Anti-virus checks and any other pre-defined criteria;

whereby in a worst case scenario only file data that is Q-time old is lost and the User Drive(s) remain(s) relatively immune from attack(s) by any known or unknown malicious software, or intentional or accidental modifications or deletions or corruption.

2. A method as recited in claim 1, wherein the malware cleaning programs are instructed to scan only the changed file data in a given period of time, as per the log in the Q-drive, said method further comprising steps of:

detecting updates to malware cleaning program or database;

processing the log of changes and identifying files for cleaning malware; and

invoking the Anti-virus program to detect and clean malware on only the changed data.

3. A method as recited in claim 2 to detect and apply updates to various anti-virus programs and associated databases.

4. A method as recited in claim 1, wherein moving and merging the file data onto the next logical stage on the multi-staged Q-drive is carried out optionally instead of merging to the User drive, based on the fulfillment of a predefined set of criteria.

5. A method as recited in claim 1, wherein the user is seamlessly furnished requested file data and related information regardless of the respective underlying drive(s).

6. A method as recited in claim 1 to prevent complete data loss by means of a time based hierarchical storage, wherein any modified data is incubated onto an appropriate indexed safety zone or stage or logical compartment on the Q-drive.

7. A method as recited in claim 6, wherein the safety zone within the Q-drive is based on defined criteria.

8. A method as recited in claim 7, wherein the next logical safety zone within the Q-drive is based on the fulfillment of defined criteria.

9. A method as recited in claim 1, further comprising transferring and copying the data to the User's drive or an appropriate stage on the Q-drive after expiration of the quiescent period of pre-emptive quarantine, on being attested as 'clean' by various Anti-virus program(s) and any other criteria.

10. A method as recited in claim 9, to define different quiescent times as criteria for copying / transferring data.

11. A method as recited in claim 1, wherein the said Q-drive exist on heterogeneous computer systems in the network or any other connectivity of heterogeneous computer(s) or processor(s) in tandem.

12. A system to contain data loss to pre-defined pre-emptive isolation / incubation time period(s) in the event of a malware attack or intentional or accidental modifications or deletions or corruption, said method utilizing management of the existing logically or physically differentiated multi-staged storage device(s) and Anti-virus cleaning program(s), said system comprising of:

a multi-staged Q-drive to store file(s) that is / are created or modified by the user, wherein the relevant details of the said file data and operations are recorded and with a periodic or manual Anti-virus check(s); and

a User Drive to move onto the said file data from the multi-staged Q-drive, after the same has become older than 'defined time period' (Q-time) as per available log(s) and subject to Anti-virus checks and any other pre-defined criteria;

whereby in a worst case scenario only file data that is Q-time old is lost and the User Drive(s) remain(s) relatively immune from attack(s) by any known or unknown malicious software, or intentional or accidental modifications or deletions or corruption.

13. A system as recited in claim 12, wherein the multi-staged Q-drive further comprises of an appropriate indexed safety zone or stage or logical compartment to prevent complete data loss by means of a time based hierarchical storage.

14. A system as recited in claim 13, wherein multi-staged Q-drive moves and merges the file data onto the next logical stage, based on the fulfillment of a predefined set of criteria.

15. A system as recited in claim 12, wherein the said Q-drive exist on heterogeneous computer systems in the network or any other connectivity of heterogeneous computer(s) or processor(s) in tandem.

16. A carrier medium comprising program instructions which are executable to:

direct and store file(s) that is / are created or modified by the user to the appropriate stage on a multi-staged Q-drive;

record relevant details of the said file data and operations performed In the form of a log on the Q-drive;

run a periodic or manual Anti-virus scan over the said file data in the multi-staged Q-drive and in case of malware presence confirmation, cleaning the data if repairable or

alternately restoring the said data to a prior known safe state; and

move and merge the file data onto the User Drive or an appropriate stage on the Q-drive after the same has become older than 'defined time period' (Q-time) as per available log(s) and subject to Anti-virus checks and any other pre-defined criteria.

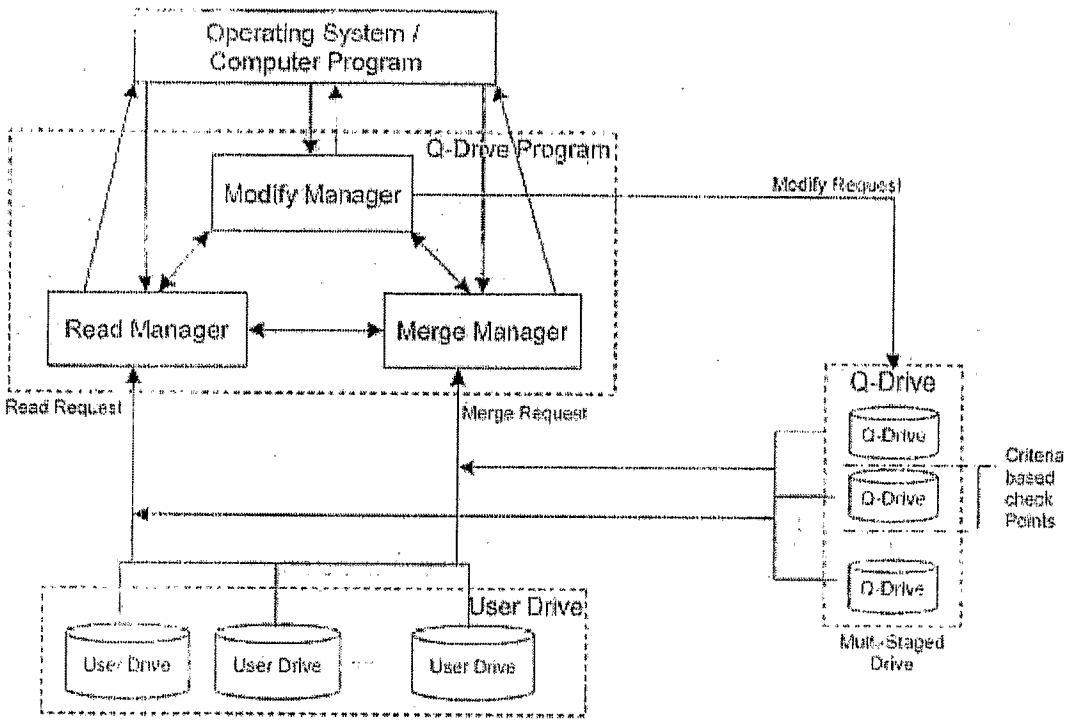

Operating System / Computer Program
Q-Drive Program
Modify Manager
Modify Request
Read Manager
Merge Manager
Read Request
Merge Request
Q-Drive
Q-Drive
Q-Drive
Q-Drive
Criteria based check Points
Multi-Staged Drive
User Drive
User Drive
User Drive
User Drive

Figure 1

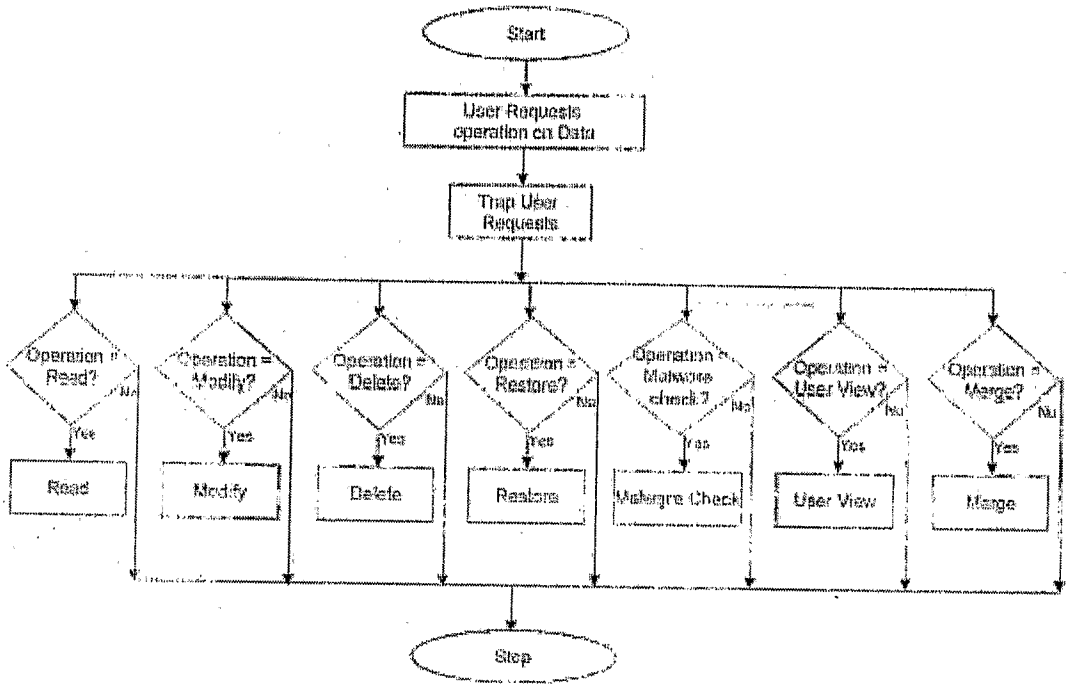

Start
User Requests operation on Data
Trap User Requests
Operation = Read?
Operation = Modify?
Operation = Delete?
Operation = Restore?
Operation = Malware check ?
Operation = User View?
Operation = Merge?
No
Yes
Read
Modify
Delete
Restore
Malware Check
User View
Merge
Stop

Figure 2

Read

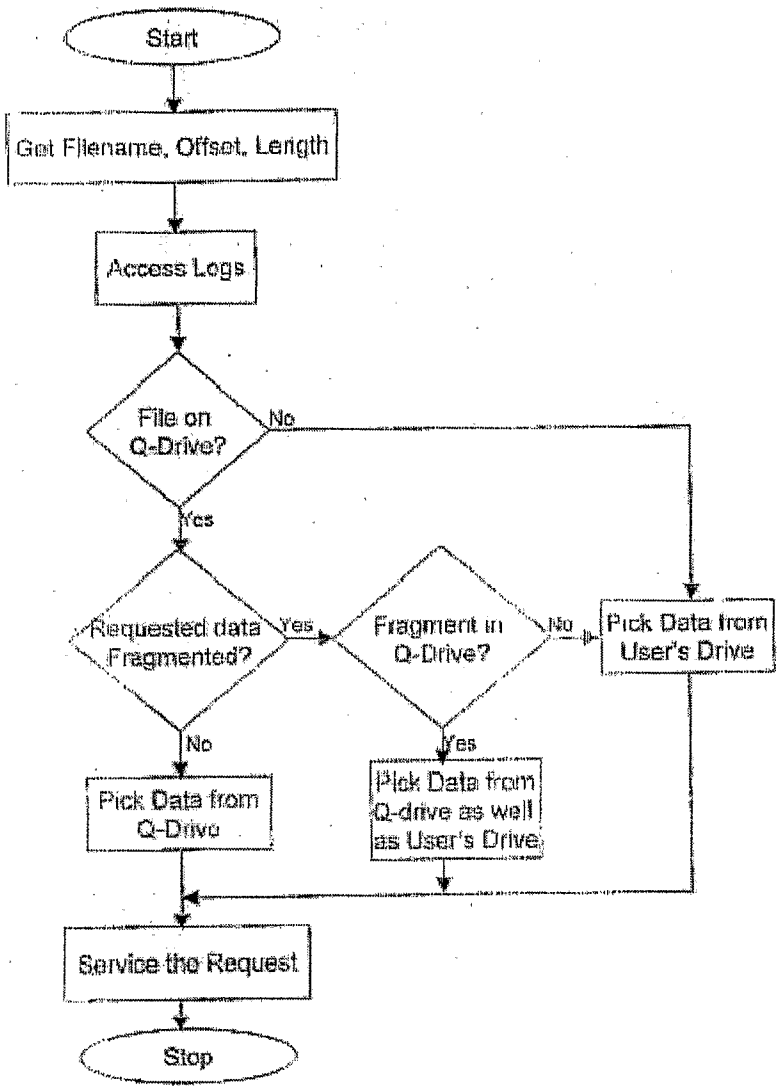


Figure 3

Modify

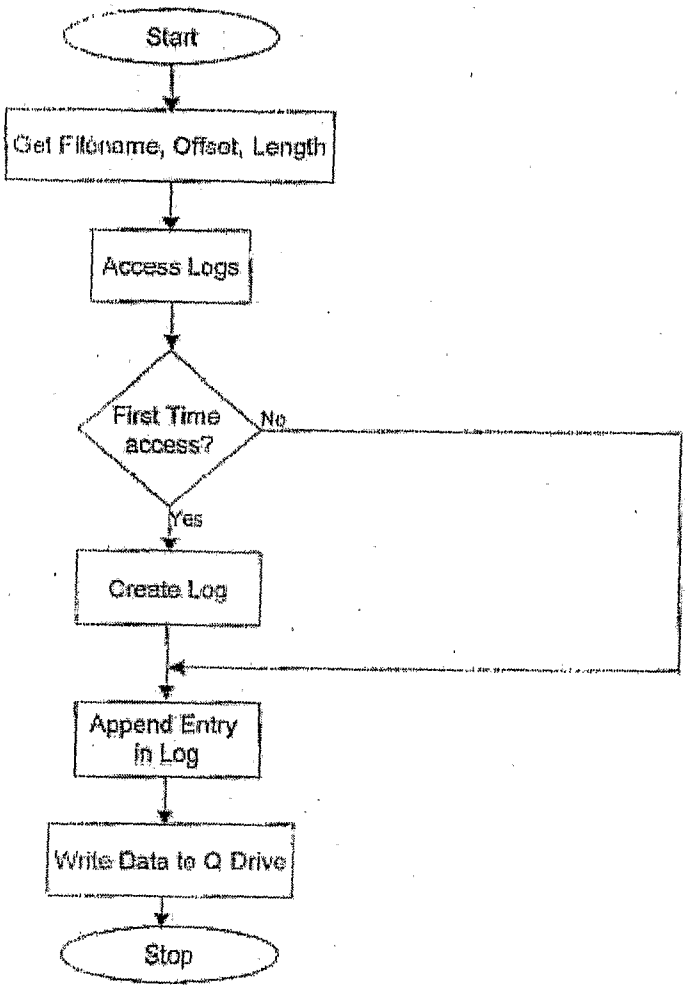


Figure 4

Delete

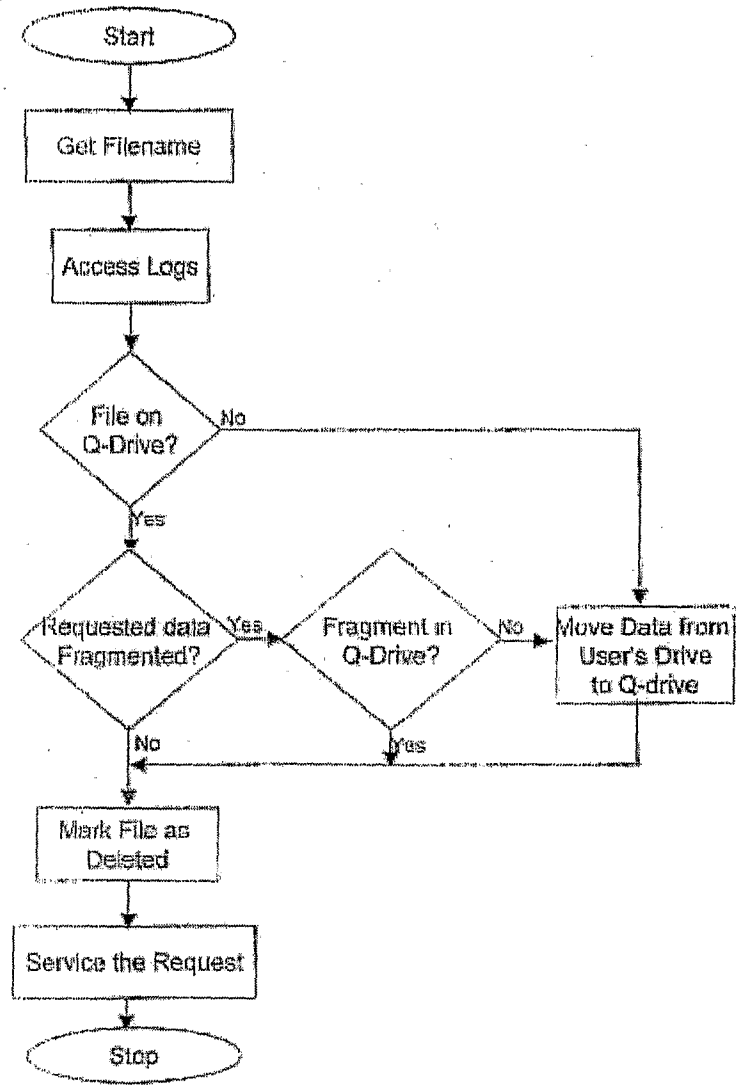


Figure 5

Restore

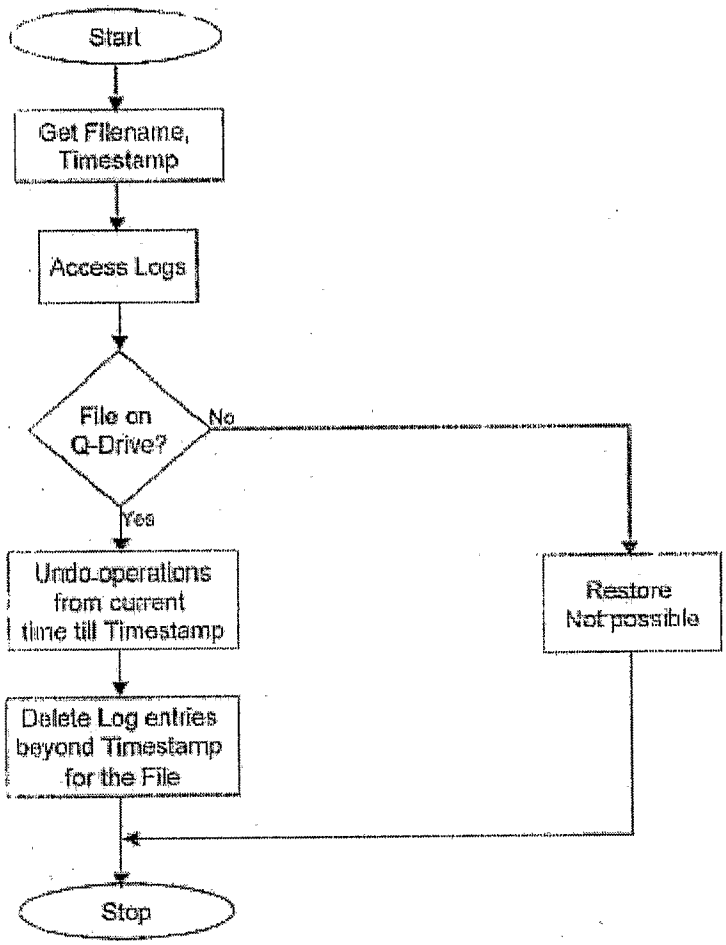


Figure 6

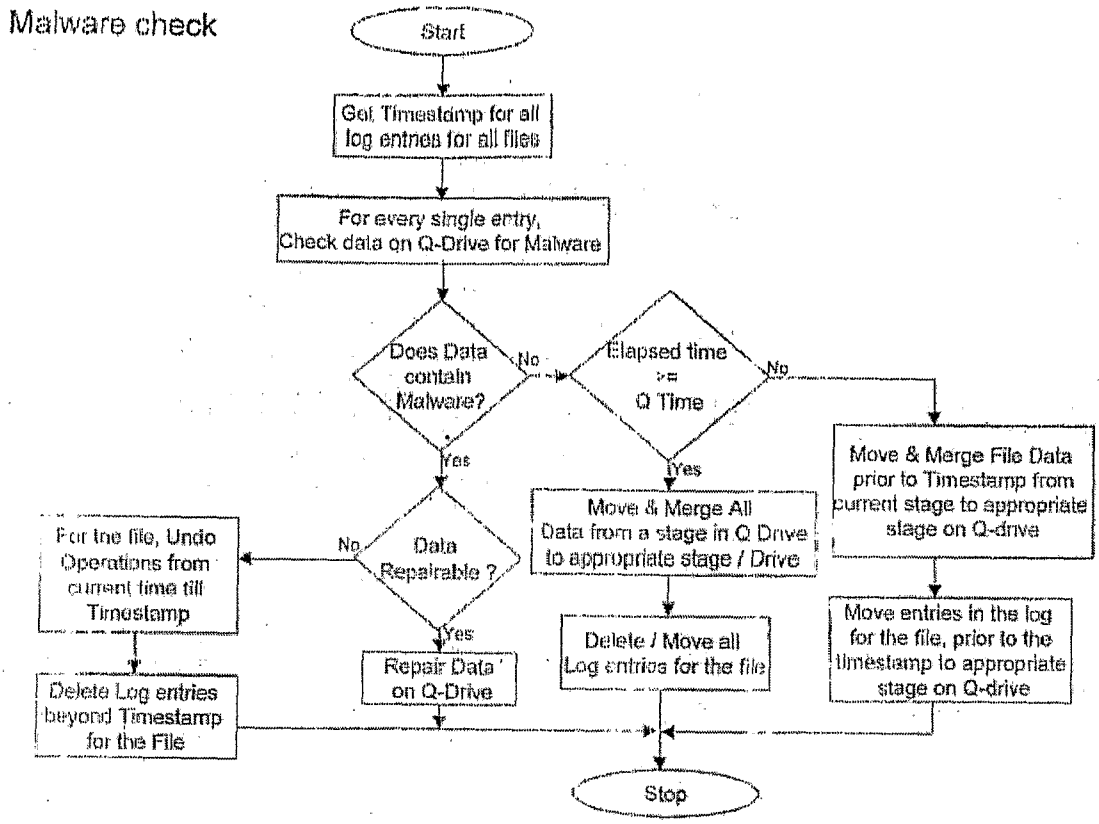

Malware check
Start
Get Timestamp for all log entries for all files
For every single entry, Check data on Q-Drive for Malware
Does Data contain Malware?
No
Yes
Elapsed time >= Q Time
No
Yes
Move & Merge File Data prior to Timestamp from current stage to appropriate stage on Q-drive
Move & Merge All Data from a stage in Q Drive to appropriate stage / Drive
Data Repairable ?
No
Yes
For the file, Undo Operations from current time till Timestamp
Repair Data on Q-Drive
Delete / Move all Log entries for the file
Move entries in the log for the file, prior to the timestamp to appropriate stage on Q-drive
Delete Log entries beyond Timestamp for the File
Stop

Figure 7

User View

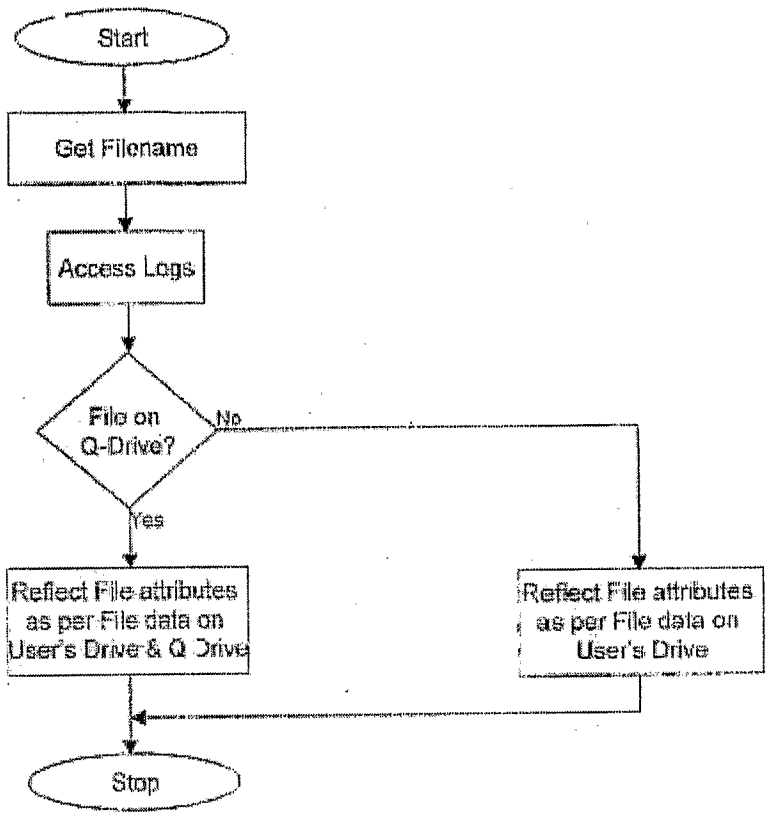


Figure 8

Merge

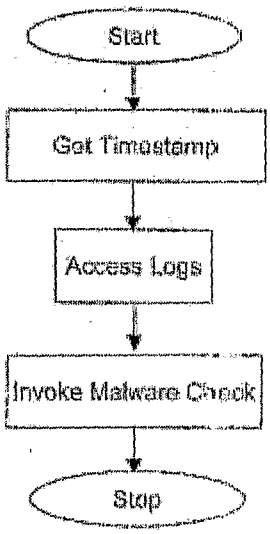


Figure 9

: Anti-Malware Software Updates

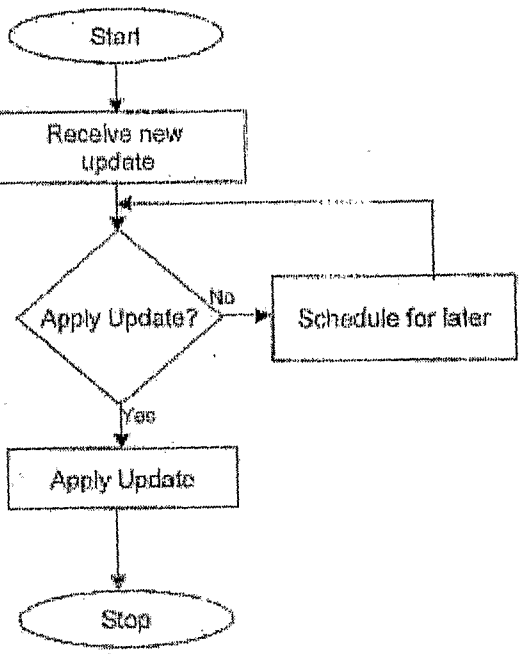


Figure 10