Method and System of Securely Accessing Cloud Storage Using Personal Mobile Device

Field of the Invention

This invention relates to a process or a system for accessing cloud network storage. More particularly, this invention relates to accessing cloud network storage activated by a mobile device. Still more particularly, this invention relates to mounting a virtual file system in a computer system to access data in the cloud network storage activated by the mobile device.

Prior Art

With the proliferation of information technology by the masses, there has been an explosive growth in the demand for storage to store anything from family photographs, videos, to personal confidential documents and so on. Usage of personal storage devices such as thumb drives, flash memory cards and portable hard disk drives are very common these days. With personal storage devices, there is a tendency to misplace and lose such storage devices together with the data stored on the storage device. Further there is also a limit on the amount of data that can be stored by such storage devices.

An alternative method of storing personal data is via cloud storage. Although cloud storage provides some benefits over personal storage devices such as ubiquitous accessibility of data, automatic backup of data and scalable storage space, accessing the files in the cloud is not as easy and convenient as plugging in a USB storage device on a computer and immediately have access to the files. Accessing files on the cloud storage typically entails the use of a web browser to log in to the cloud storage portal before the files can be accessed. It is not the most intuitive way to access data for most users who are more accustomed to accessing files on local file system or USB storage, using familiar file explorer user interface of the operating system. Furthermore, there is also concern about the security and privacy of data stored in the cloud.

The invention overcomes the above shortcomings by use of a mobile communication device in lieu of personal storage device to provide transparent and secured access to data in the cloud through a locally mounted virtual file system.

Summary of the Invention

The above and other problems are solved and an advance in the art is made by the method and system for accessing data stored in cloud network storage in accordance with the present invention. A first advantage of a method and system in accordance with this invention is accessing of data stored by a cloud network storage when activated by a personal mobile device. Hence, added security is provided. A second advantage of a method and system in accordance with this invention is the ease of accessing data since it is common that a user carries at least one mobile device. A third advantage of a method and system in accordance with this invention is that system allows the creation of virtual personal storage device where the files on the storage device are amalgamation of files stored remotely in multiple cloud storage services. The virtual personal storage device presents a consistent virtual layout of files and folders regardless of how data is actually stored in the cloud. The access of cloud data using the virtual file system allows existing PC applications such as document editor (e.g. MS Words) to continue to work transparently.

A system and method for accessing data stored in cloud network storage in accordance with an embodiment of this invention is provided in the following manner. The system resides in a computer system and receives a mount request acknowledgement from a mobile device. After a mount request acknowledgement is received from the mobile device, a virtual file system is mounted in the computer system. The system then generates a file operation request and transmits the file operation request to the mobile device. The system then requests meta data from the mobile device to enable it to perform file operation such as read and write. With the meta data, the system access the cloud network storage and retrieves data stored by the cloud network storage or writes data to the cloud network storage. The meta data may contain critical information including location of slices of files and transform matrix required for reconstruction of files, without which access to data is not possible. Data retrieved from or written to the cloud network storage is allowed access through the virtual file system.

In accordance with embodiments with this invention, the system detects whether a mobile device is within a certain proximity of the computer system. Upon detecting a mobile device is within the proximity, computer system generates a mount request and transmits the mount request to the mobile device.. In accordance with some of these embodiments, the computer system detects the proximity of the mobile device via Bluetooth connectivity.

In accordance with embodiments with this invention, the computer system generates a remote mount request and transmits the remote mount request to the mobile device. The remote mount request may comprise a user identification, a password and endpoint address and port of said computer system. In accordance with some of these embodiments, the remote mount request to the mobile device is via telephonic connection or network connection.

In accordance with embodiments of this invention, the system detects the mobile device is outside a certain proximity. After the system detects the mobile device is outside a certain proximity, the system removes the virtual file system from the computer system.

In accordance with an embodiment of this invention, the system receives a mount request from the mobile device via telephonic connection or a network connection.

In accordance with embodiments of this invention, the system detects a dismount request from the mobile device and removes the virtual file system from the computer system. Alternatively, the system detects a dismount request from the computer system and removes the virtual file system from the computer system.

In accordance with an embodiment of this invention, the computer system updates the data retrieved from the cloud network storage and transmits the updated data to the cloud network storage.

In accordance with an embodiment of this invention, the system updates the meta data and transmits the updated meta data to the mobile device. The system then receives a confirmation that the updated meta data is received by the mobile device.

Brief Description of the Drawings

The above and other features and advantages in accordance with this invention are described in the following detailed description and are shown in the following drawings:

Figure 1 illustrating a system connected to cloud network storage in accordance with an embodiment of this invention;

Figure 2 illustrating an exemplary processing system such as those in a computer system and network devices in accordance an embodiment of this invention;

Figure 3 illustrating a flow diagram of process performed by a system in the computer system to mount a virtual file system in the computer system in accordance with an embodiment of this invention;

Figure 4 illustrating a flow diagram of a process performed by the system to detect a mobile device in accordance with an embodiment of this invention;

Figure 5 illustrating a flow diagram of a process performed by the system to authenticate with the mobile device in accordance with an embodiment of this invention;

Figure 6 illustrating a flow diagram of a process performed by an application in the mobile device in accordance with an embodiment of this invention;

Figure 7 illustrating a flow diagram of a process performed by the system to establish connection with the mobile device in a remote location in accordance with an embodiment of this invention;

Figure 8 illustrating a flow diagram of a process performed by an application in the mobile device in accordance with an embodiment of this invention;

Figure 9 illustrating a flow diagram of a process performed by the system to dismount the virtual file system when mobile device is not within proximity in accordance with an embodiment of this invention; and

Figure 10 illustrating a flow diagram of a process performed by the system to dismount the virtual file system in accordance with an embodiment of this invention.

Detailed Description

This invention relates to a system in a computer system for accessing cloud network storage. More particularly, this invention relates to accessing cloud network storage activated by a mobile device. Still more particularly, this invention relates to mounting a virtual file system in the computer system to access data in the cloud network storage activated by the mobile device.

This invention relates to accessing data stored in cloud network storage. For purposes of this discussion, cloud network storage system is a group of processing devices communicatively connected over a network such as the Internet to share resources. In accordance with this invention, a user may not be a proprietor of the cloud network storage system and/or may not have control of cloud network resources and/or of accessibility of data stored by the cloud network resources. Further, a user in accordance with this invention may use resources from one or more cloud network storage systems.

Figure 1 illustrates an embodiment of this invention in which system 100 includes a computer system 170, a mobile device 150, and cloud network storage 110. Computer system 170 is a typical processing system such as a desktop computer, laptop computer, or other computer terminal that connects to cloud network storage 110 via a conventional wire connection, wireless connection or any other method. Computer system 170 executes

applications that perform the required processes in accordance with this invention. One skilled in the art will recognize that although only one computer system 170 is shown, any number of computer systems may be connected without departing from this invention. Furthermore, the computer system 170 may be connected to or within a cloud network storage 110 without departing from this invention.

Cloud network storage 110 includes network devices 120 and 125. Network devices 120 and 125 are processing systems that provide resources to computer system 170 over cloud network storage 110 and are connected to cloud network storage 110 via a conventional wire connection, wireless connection or any other method. Resources may include but are not limited to storage, processing time, and applications. Network devices 120 and 125 may be connected as separate systems in cloud network storage 110 or connected as parts of separate cloud network storages. As shown in Figure 1, network devices 120 are connected in first cloud network storage 115 and network devices 125 are connected in second cloud network storage 116. One skilled in the art will recognize that the exact number and configurations of network devices in a network; and the exact number and configurations of cloud computing networks in cloud network storage 110 are design choice left to those skilled in the art.

Mobile device 150 is a mobile hand phone, Personal Digital Assistant (PDA) or other device that can be connected to and/or communicate with computing system 170 through the Internet, WiFi, Bluetooth, IR data transmission, Radio Frequency, etc. Further, mobile device 150 may be any device that can be connected to and/or communicate with computing system 170 through telephonic means such as Public Switched Telephonic Network (PSTN). A complete description of mobile device 150 is omitted for brevity and only those processes that are performed in accordance with this invention are described.

Figure 2 illustrates an exemplary processing system 200 that represents the processing systems in computer system 170 that execute instructions to perform the processes described below in accordance with this invention. One skilled in the art will recognize that the instructions may be stored and/or performed as hardware, firmware, or software without departing from this invention. One skilled in the art will recognize that the exact configuration of each processing system may be different and the exact configuration executing processes in accordance with this invention may vary and processing system 200 shown in Figure 2 is provided by way of example only.

Processing system 200 includes Central Processing Unit (CPU) 205. CPU 205 is a processor, microprocessor, or any combination of processors and microprocessors that execute instructions to perform the processes in accordance with the present invention. CPU 205 connects to memory bus 210 and Input/Output (I/O) bus 215. Memory bus 210 connects CPU 205 to memories 220 and 225 to transmit data and instructions between the memories and CPU 205. I/O bus 215 connects CPU 205 to peripheral devices to transmit and receive data between CPU 205 and the peripheral devices. One skilled in the art will recognize that I/O bus 215 and memory bus 210 may be combined into one bus or subdivided into many other busses and the exact configuration is left to those skilled in the art.

A non-volatile memory 220, such as a Read Only Memory (ROM), is connected to memory bus 210. Non-volatile memory 220 stores instructions and data needed to operate various sub-systems of processing system 200 and to boot the system at start-up. One skilled in the art will recognize that any number of types of memory may be used to perform this function.

A volatile memory 225, such as Random Access Memory (RAM), is also connected to memory bus 210. Volatile memory 225 stores the instructions and data needed by CPU 205 to perform software instructions for processes such as the processes for providing a system in accordance with this invention. One skilled in the art will recognize that any number of types of memory may be used to provide volatile memory and the exact type used is left as a design choice to those skilled in the art.

I/O device 230, keyboard 235, display 240, memory 245, network interface 250, detection module 255 and any number of other peripheral devices connect to I/O bus 215 to exchange data with CPU 205 for use in applications being executed by CPU 205. I/O device 230 is any device that transmits and/or receives data from CPU 205. Keyboard 235 is a specific type of I/O device that receives user input and transmits the input to CPU 205. Display 240 receives display data from CPU 205 and display images on a screen for a user to see. Memory 245 is a device that transmits and receives data to and from CPU 205 for storing data to a media. Network interface 250 connects CPU 205 to a network for transmission of data to and from other processing systems. Network interface 250 may be any devices that connect computer system 170 to mobile devices and/or cloud computing network 110 via PSTN, WIFI, Bluetooth Personal Area Network, etc. Detection module 255 is a module that receives and detects signals broadcasted from mobile device 150. Some

examples of detection module 255 include, but are not limited to a Wi-Fi interface, Bluetooth interface, IR data transmission interface, Radio Frequency interface, Near Field Communication, capable of connecting computer system 170 to mobile device 150.

Figure 3 illustrates a flow diagram of process 300 performed by a system in computer system 170 in accordance with this invention. The system is provided by processes stored in software, firmware, or hardware that performs the processes described. Process 300 begins in step 310 in which computer system 170 monitors and detects for any mobile device 150. The detection of mobile device 150 will be described further with reference to figure 4 below.

In step 320, computer system 170 generates and transmits a mount request to mobile device 150. Computer system 170 then waits for an acknowledgement from mobile device mobile device 150 to allow access to mobile device 150. The acknowledgement may be a mount request acknowledgement from mobile device 150.

Upon receipt of the mount request acknowledgement from mobile device 150, a virtual file system is then mounted in computer system 170 in step 330 and ready for further file operations by user or application such as directory listing, file read, write and so on. For purposes of this discussion, mounting of new virtual file system may refer to creation of a new virtual file system, which is manifested as creation of a virtual drive, or a new mount point in the computer system and is performed in a conventional manner. Once the virtual file system is mounted, file I/O operations can be performed by computer system 170. The file I/O operations supported by the virtual file system are the same as the file I/O operation supported by native or other mounted file systems of the corresponding operating system. For example, in UNIX, file I/O operations include operations such as stat(), mknod(), mkdir(), rmdir(), rename(), read(), write().

When the system receives a file operation from a user through I/O device 230, keyboard 235 or other peripheral devices of computer system 170, the system will generate a file operation request and transmit the file operation request to mobile device 150 in step 340. Particularly, the system will attempt to retrieve and/or update the corresponding meta data to and from mobile device 150 to satisfy the file operations requested from the user. Meta data is information that allows computer system 170 to establish connection with and access data stored by cloud network storages. Meta data includes file information, size, location of file, etc. In particular, the file are slices of files and may further include transform

matrix required for reconstruction of files as described in PCT Application PCT/SG2011/000138 title "Method And System For Storing Data In A Cloud Network" filed on 4 April 2011 which is incorporated by reference as if set forth herewith. One skilled in the art will recognize that the meta data only need to assist in identifying the data content stored in the cloud network storage. The exact protocols or standards used are left as a design choice.

In step 350, the system receives meta data from mobile device 150. If the meta data is not available from mobile device 150, no file operation is possible. If the meta data for the file operation requested from the user is available, the file operation is carried out. For a file which requires read or write of file data, the data is read or written to the cloud network storage using the information provided by the meta data. One skilled in the art will recognize that the file operation may be performed in any known manner and the exact process of file operation is left as a design choice for the skilled in the art.

After receiving the meta data, process 300 then establishes connection with cloud network storage in step 360. Depending on the file operation requested from the user, data is then retrieved from or written to various cloud network storages using the meta data in step 370. In step 380, data retrieved from the cloud network storage or data written to the cloud network storage is then available for use through the virtual file system on display 240. Process 300 then ends after data step 380.

Once the mounted virtual file system is disconnected or a command to dismount the mounted virtual file system is received by the system either from mobile device 150 or from a user through I/O device 230, keyboard 235 or other peripheral devices of computer system 170, any modified or updated meta data due to file operation such as write() or mkdir() is sent to the mobile device. Any data being written to a file is also updated to the cloud network storage. The system will discard the meta data after the system successfully updates the meta data on the mobile device. Similarly, the data will also be discarded from computer system 170 after the system successfully updates or writes the data to the cloud network storage. A more detailed description of dismounting of virtue file system is described below.

Figure 4 illustrates a flow diagram of process 400 performed by the system in computer system 170 in accordance with this invention. Process 400 is an embodiment of a process for performing step 310 in process 300. Process 400 begins in step 410 by

monitoring for signals from a mobile device. If signals from a mobile device are received indicating a mobile device is within certain proximity in step 420, process 400 proceeds to step 320 of process 300 to generate and transmit a mount request to mobile device 150. One skilled in the art will recognise that the proximity in which a signal from a mobile device may be detected is dependent on the signal strength of the signal broadcasted from the wireless communication device in mobile device 150. The stronger the signal broadcasted from the wireless communication device in mobile device 150, the further the distance the detection module is able to detect the mobile device. If no signal is received from a mobile device indicating a mobile device is within certain proximity in step 420, process 400 repeats from step 410.

Figure 5 illustrates a flow diagram of process 500 performed by the system in computer system 170 in accordance with this invention. Process 500 is an embodiment of a process prior to performing step 340 in process 300. Process 500 begins with step 510 by determining whether authentication with the mobile device is required. In this step, computer system 170 waits for a challenge request from mobile device 150 for a certain period of time. If a challenge request is received from mobile device, authentication is required. The challenge request is a request for authentication information in order to access the meta data in mobile device 150 and may include, but is not limited to, a user identification and/or a password.

If authentication is not required, process 500 proceeds to step 330 in process 300. If authentication is required, process 500 proceeds to step 520 to prompt the user to enter the authentication information requested from mobile device 150 such as user identification and password. Alternatively, the authentication information requested from mobile device may be credential information such as an electronic certificate or any other type of data that may be used to authenticate the device. If a registry of computer system 170 contains the required information to authenticate with mobile device 150, the required information for authentication is retrieved and transmitted to the mobile device for authentication. One skilled in the art will recognise that other methods of authentication may be implemented without departing from the invention and the exact choice of authentication method is left to the skilled in the art.

In step 530, computer system 170 receives the authentication information from the user through I/O device 230, keyboard 235 or other peripheral devices of computer system 170. Computer system 170 then transmits the information to mobile device 150.

Process 500 then waits for an authentication success acknowledgement from mobile device indicating authentication is successful in step 540. If the authentication success acknowledgement is received, process 500 proceeds to step 340 in process 300. If authentication success acknowledgement is not received within a predetermined period, process 500 proceeds to step 560. In step 560, connection is terminated and process 500 proceeds to step 310 in process 300.

Figure 6 illustrates a flow diagram of process 600 performed by mobile device 150 in response to process 500. Process 600 begins with step 610 in which mobile device 150 generates and transmit a challenge request to computer system 170. The challenge request is a request for information in order to access the meta data in mobile device 150 and may include, but is not limited to, a user identification and/or a password.

In step 620, mobile device receives authentication information from computer system 170. In step 630, mobile device 150 determines if authentication information received from computer system is correct. In step 640, if information is correct, mobile device 170 transmits an authentication success acknowledgement to confirm authentication is successful in step 650. Process 600 ends after step 650. If authentication information is not correct, mobile device will terminate connection with computer system 170 at step 660. Process 600 then ends after step 660.

Figure 7 illustrates a flow diagram of process 700 performed by the system in computer system 170 in accordance with an embodiment of this invention. Process 700 illustrates a process that allows a user to initiate mounting of a new virtual file system from computer system 170. This process may be used to access mobile device 150 when mobile device is not within range of computer system 170. Process 700 begins with step 710 in which a remote mount request is generated. The remote mount request contains the required authentication information such as, but not limited to user identification and/or password and the computer system endpoint information such as endpoint address and port. With reference to process 300, one skilled in the art will recognise that since process 700 is used when mobile device 150 is not within certain proximity of computer system 170 steps 310 and 320 of process 300 will be overwritten by process 700. The remote mount request is then transmitted to the mobile device in step 720. In particular, the remote mount request can be sent to the mobile device by a Short Messaging Service (SMS) through a telephone

network or a notification service such as cloud to device messaging service provided by Google via the Internet.

If mobile device responds, through the computer system endpoint, and allows access, process 700 proceeds to step 340 in process 300. In particular, the mobile device sends an authentication success acknowledgement to the computer system at the specified endpoint address and port through telephonic network or the Internet. One skilled in the art will recognize that for those computer systems behind the Network Address Translation or firewall, common techniques such as an intermediate server is required to establish a reverse Secure Shell can be implemented.

If mobile device does not respond within a certain period of time or a signal indicating that access is not allowable, connection between computer system and mobile device is terminated in step 740. After step 740, process 700 proceeds to step 310 of process 300.

Figure 8 illustrates a flow diagram of process 800 performed by mobile device 150 in response to process 700. Process 800 begins with step 810 in which mobile device 150 receives a remote mount request from computer system 170. The remote mount request contains the required authentication information such as, but not limited to user identification and/or password and the computer system endpoint address and port. The remote mount request can be received by the mobile device through a Short Messaging Service (SMS) through a telephone network or a notification service such as cloud to device messaging service provided by Google via the Internet.

In step 820, mobile device 150 determines if authentication information in the remote mount request is correct. In step 830, if authentication information is correct, mobile device 150 transmits an authentication success acknowledgement to confirm authentication is successful in step 840. Process 800 ends after step 840. If authentication information is not correct, mobile device 150 will terminate connection with computer system 170 at step 850. Process 800 then ends after step 850.

Figure 9 illustrates a flow diagram of process 900 performed by the system in computer system 170 in accordance with this invention. Particularly, process 900 illustrates the monitoring of mobile device after mounting of the virtual file system. Process 900 begins with step 910 by determining whether mobile device is still within the determined

proximity. In step 920, if computer system 170 determines that mobile device is not within the determined proximity, process 900 proceeds to step 950 to dismount of virtual file system.

As the user may move away from computer system 170 from time to time, process 900 may optionally include steps 930 and 940. In step 930, a time out counter will be activated. In step 940, computer system 170 determines if mobile device is back within the proximity. If mobile device is back within proximity, process 900 repeats from step 910. If mobile device is not back within the proximity, process 900 proceeds to step 950 to dismount virtual file system. The time out counter is a timer to determine whether mobile device is back within the proximity within a certain time period. The time out counter is configurable. One skilled in the art will recognise that if the time out counter is configured to be shorter, security will be tightened as other unauthorized user would not be able to access the virtual file system in the absence of the owner or user of the mobile device. If the time out counter is configured to be longer, security may be compromised as the virtual file system may remain available for a period of time, when the owner or user is away from the computer system. The exact time period configured to the time out counter is left as a design choice.

If dismount of virtual file system is activated when mobile device 150 is not within the determined proximity, the dismount process is performed in the following manner. It is important to note that the meta data is updated continuously to mobile device 150 for any file operation that updates the file. For example, write operation, rename operation, etc. On-going file operations are allowed to continue to protect the integrity of the data after dismount of virtual file system is activated. Once the operations are completed, the meta data is updated and ready to be transmitted to mobile device 150. Due to the absence of mobile device 150, the updated meta data may be transmitted to mobile device 150 during the next mounting process. One skilled in the art will recognize that the updated meta data may also be transmitted to mobile device by a Short Messaging Service (SMS) through a telephone network or a notification service such as cloud to device messaging service provided by Google via the Internet without departing from the invention. Any data being written to a file is updated to the cloud network storage. The system will discard the meta data after the system successfully updates to the mobile device. Similarly, the data will also be discarded from computer system 170 after the system successfully updates to the cloud network storage. After the data and meta data are discarded from computer system 170, computer system 170 may generate and transmit a confirmation to mobile device that the

virtual file system has been dismounted and that all data and meta data associated with the mounted virtual file system have been removed via a Short Messaging Service (SMS) through a telephone network or a notification service such as cloud to device messaging service provided by Google via the Internet.

Figure 10 illustrates a flow diagram of process 1000 performed by the system in computer system 170 in accordance with this invention. Particularly, process 1000 illustrates the detection of a dismount request from computer system 170. Process 1000 begins with step 1010 to detect dismount request. In step 1020, if a dismount request is not detected, process 1000 repeats from step 1010. If a dismount request is detected, process 1000 proceeds to step 1030 to update the data and meta data for the last file operation.

In step 1040, changes in the data are transmitted to the cloud network storage. In step 1050, the updated meta data is transmitted to mobile device 150. In step 1060, all data and meta data associated with mounted virtual file system are discarded from the memory of computer system 170. For purposes of this discussion, discarding of data refers to removing of information, files, or data from the computer system.

In step 1070, computer system 170 generates and transmits a confirmation to mobile device that the virtual file system has been dismounted and that all data and meta data associated with the mounted virtual file system have been removed.

The above is a description of a manner for providing a system in a computer system for accessing cloud network storage. It is envisioned that those skilled in the art can and will design alternative systems that infringe upon this invention as set forth in the following claims.

CLAIMS

1. A system in a computer system for accessing a cloud network storage comprising:
instructions for directing a processing unit to:
receive a mount request acknowledgement from a mobile device,
mount a virtual file system in said computer system in response to receiving said mount request acknowledgement;
generate a file operation request;
transmit said file operation request to said mobile device;
receive meta data from said mobile device,
establish a connection to said cloud network storage using said meta data to retrieve data from or write data to said cloud network storage,
allow access to said data retrieved from or wrote to said cloud network storage through said virtual file system, and
a media readable by said processing unit that stores said instructions for directing said processing unit.

2. The system according to claim 1 further comprising:
instructions for directing said processing unit to:
detect said mobile device is within a certain proximity of said computer system;
generate a mount request; and
transmit said mount request to said mobile device.

3. The system according to claim 2 wherein said instructions to detect said mobile device is within a certain proximity of said computer system is via Bluetooth connectivity.

4. The system according to claim 2 further comprising:
instructions for directing said processing unit to:
receive a user identification and a password;
transmit said user identification and said password to mobile device.

5. The system according to claim 4 further comprising;
instructions for directing said processing unit to:
receive an authentication success acknowledgement from said mobile device.

6. The system according to claim 2 further comprising:

instructions for directing said processing unit to:

detect a dismount request from said mobile device, and

remove said virtual file system from said computer system in response to detecting said dismount request.

7. The system according to claim 6 further comprising:

instructions for directing said processing unit to:

update said data retrieved from said cloud network storage, and

transmit said updated data to said cloud network storage.

8. The system according to claim 6 further comprising:

instructions for directing said processing unit to:

update said meta data,

transmit said updated meta data to said mobile device, and

receive a confirmation that said updated meta data is received by said mobile device.

9. The system according to claim 2 further comprising:

instructions for directing said processing unit to:

detect said mobile device is outside a certain proximity.

10. The system according to claim 9 further comprising:

instructions for directing said processing unit to:

remove said virtual file system from said computer system in response to detecting said mobile device is outside said certain proximity.

11. The system according to claim 10 further comprising:

instructions for directing said processing unit to:

update said data retrieved from said cloud network storage, and

transmit said updated data to said cloud network storage.

12. The system according to claim 10 further comprising:

instructions for directing said processing unit to:

update said meta data,

transmit said updated meta data to said mobile device via telephonic means, and

receive a confirmation that said updated meta data is received by said mobile device.

13. The system according to claim 1 wherein said instructions to receive said mount request acknowledgement from said mobile device is via telephonic connection.

14. The system according to claim 1 wherein said instructions to receive said mount request acknowledgement from said mobile device is via network connection.

15. The system according to claim 1 further comprising:
instructions for directing said processing unit to:
generate a remote mount request; and
transmit said remote mount request to said mobile device.

16. The system according to claim 15 wherein said remote mount request comprises a user identification, a password and endpoint address and port of said computer system.

17. The system according to claim 15 wherein said instructions to transmit said remote mount request to said mobile device is via telephonic connection.

18. The system according to claim 15 wherein said instructions to transmit said remote mount request to said mobile device is via network connection.

19. The system according to 15 further comprising:
instructions for directing said processing unit to:
detect a dismount request from said mobile device, and
remove said virtual file system from said computer system in response to said dismount request.

20. The system according to claim 19 further comprising:
instructions for directing said processing unit to:
update said data retrieved from said cloud network storage, and
transmit said updated data to said cloud network storage.

21. The system according to claim 19 further comprising:
instructions for directing said processing unit to:

update said meta data,

transmit said updated meta data to said mobile device, and

receive a confirmation that said updated meta data is received by said mobile device.

22. A method for accessing a cloud network storage comprising:

receiving a mount request acknowledgement from a mobile device;

mounting a virtual file system in said computer system in response to receiving said mount request acknowledgement;

generating a file operation request;

transmitting said file operation request to said mobile device;

receiving meta data from said mobile device;

establishing a connection to said cloud network storage using said meta data to retrieve data from or write data to said cloud network storage; and

allowing access to said data retrieved from or wrote to said cloud network storage through said virtual file system.

23. The method according to claim 22 further comprising:

detecting said mobile device is within a certain proximity of said computer system;

generating a mount request; and

transmitting said mount request to said mobile device.

24. The method according to claim 23 wherein said step of detecting said mobile device is within a certain proximity of said computer system is performed via Bluetooth connectivity.

25. The method according to claim 23 further comprising:

receiving a user identification and a password; and

transmitting said user identification and said password to mobile device.

26. The method according to claim 25 further comprising;

receiving an authentication success acknowledgement from said mobile device.

27. The method according to claim 23 further comprising:

detecting a dismount request from said mobile device; and

removing said virtual file system from said computer system in response to said dismount request.

28. The method according to claim 27 further comprises:
updating said data retrieved from said cloud network storage;
transmitting said updated data retrieved to said cloud network storage.

29. The method according to claim 27 further comprises:
updating said meta data;
transmitting said updated meta data to said mobile device; and
receiving a confirmation that said updated meta data is received by said mobile device.

30. The method according to claim 23 further comprising:
detecting said mobile device is outside a certain proximity.

31. The method according to claim 30 further comprising:
removing said virtual file system from said computer system in response to said mobile device being outside said certain proximity.

32. The method according to claim 31 further comprising:
updating said data retrieved from said cloud network storage; and
transmitting said updated data to said cloud network storage.

33. The method according to claim 31 further comprising:
updating said meta data;
transmitting said updated meta data to said mobile device via telephonic means; and
receiving a confirmation that said updated meta data is received by said mobile device.

34. The method according to claim 22 wherein said step of receiving said mount request acknowledgement is via telephonic connection.

35. The method according to claim 22 wherein said step of receiving said mount request acknowledgement is via network connection.

36. The method according to claim 22 further comprising:
generating a remote mount request; and

transmitting said remote mount request to said mobile device.

37. The method according to claim 36 wherein said remote mount request comprises a user identification, a password and endpoint address and port of said computer system.

38. The method according to claim 36 wherein said step of transmitting said remote mount request to said mobile device is via telephonic connection.

39. The method according to claim 36 wherein said step of transmitting said remote mount request to said mobile device is via network connection.

40. The method according to claim 36 further comprising:

detecting a dismount request from said mobile device; and

removing said virtual file system from said computer system in response to said dismount request.

41. The method according to claim 40 further comprising:

updating said data retrieved from said cloud network storage;

transmitting said updated data to said cloud network storage; and

receiving a confirmation that said updated data retrieved from said cloud network storage is received by said cloud network storage.

42. The method according to claim 40 further comprising:

updating said meta data;

transmitting said updated meta data to said mobile device; and

receiving a confirmation that said updated meta data is received by said mobile device.

43. A system in a computer system for accessing a cloud network storage comprising:

circuitry configured to receive a mount request acknowledgement from a mobile device;

circuitry configured to mount a virtual file system in said computer system in response to receiving said mount request acknowledgement;

circuitry configured to generate a file operation request;

circuitry configured to transmit said file operation request to said mobile device;

circuitry configured to receive meta data from said mobile device;

circuitry configured to establish a connection to said cloud network storage using said meta data to retrieve data from or write data to said cloud network storage; and

circuitry configured to allow access to said data retrieved from or wrote to said cloud network storage through said virtual file system.

44. The system according to claim 43 further comprising:

circuitry configured to detect said mobile device is within a certain proximity of said computer system;

circuitry configured to generate a mount request; and

circuitry configured to transmit said mount request to said mobile device.

45. The system according to claim 44 wherein said circuitry configured to detect said mobile device is within a certain proximity of said computer system is via Bluetooth connectivity.

46. The system according to claim 44 further comprising:

circuitry configured to receive a user identification and a password; and

circuitry configured to transmit said user identification and said password to mobile device.

47. The system according to claim 46 further comprising;

circuitry configured to receive an authentication success acknowledgement from said mobile device.

48. The system according to claim 44 further comprising:

circuitry configured to detect a dismount request from said mobile device; and

circuitry configured to remove said virtual file system from said computer system in response to said dismount request.

49. The system according to claim 48 further comprising:

circuitry configured to update said data retrieved from said cloud network storage; and

circuitry configured for transmit said updated data to said cloud network storage.

50. The system according to claim 48 further comprising:

circuitry configured to update said meta data;

circuitry configured to transmit said updated meta data to said mobile device; and

circuitry configured to receive a confirmation that said updated meta data is received by said mobile device.

51. The system according to claim 44 further comprising:

circuitry configured to detect said mobile device is outside a certain proximity.

52. The system according to claim 51 further comprising:

circuitry configured to remove said virtual file system from said computer system in response to detection that said mobile device is outside said certain proximity.

53. The system according to claim 52 further comprising:

circuitry configured to update said data retrieved from said cloud network storage; and

circuitry configured to transmit said updated data to said cloud network storage.

54. The system according to claim 52 further comprising:

circuitry configured to update said meta data;

circuitry configured to transmit said updated meta data to said mobile device via telephonic means; and

circuitry configured to receive a confirmation that said updated meta data is received by said mobile device.

55. The system according to claim 43 wherein said circuitry configured to receive said mount request acknowledgement is via telephonic connection.

56. The system according to claim 43 wherein said circuitry configured to receive said mount request acknowledgement is via network connection.

57. The system according to claim 43 further comprising:

circuitry configured to generate a remote mount request; and

circuitry configured to transmit said remote mount request to said mobile device.

58. The system according to claim 57 wherein said remote mount request comprises a user identification, a password and endpoint address and port of said computer system.

59. The system according to claim 57 wherein said circuitry configured to transmit said remote mount request to said mobile device is via telephonic connection.

60. The system according to claim 57 wherein said circuitry configured to transmit said remote mount request to said mobile device is via network connection.

61. The system according to claim 60 further comprising:

circuitry configured to detect a dismount request from said mobile device; and

circuitry configured to remove said virtual file system from said computer system in response to said dismount request.

62. The system according to claim 61 further comprising:

circuitry configured to update said data retrieved from said cloud network storage; and

circuitry configured to transmit said updated data to said cloud network storage.

63. The system according to claim 61 further comprising:

circuitry configured to update said meta data;

circuitry configured to transmit said updated meta data to said mobile device; and

circuitry configured to receive a confirmation that said updated meta data is received by said mobile device.