

CLIENT SIDE DEVICE ACCESSING DATA DURING COMMUNICATION DISTRUPTIONS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present application claims priority to U.S. Non-Provisional Patent Application 14/203,265, filed March 10, 2014 which is a continuation-in-part of U.S. Non-Provisional Patent Application 12/581,533, filed on October 19, 2009, which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

[0002] The invention relates to systems and methods of providing centralized client-side data storage and retrieval on a local network. More particularly, the invention relates to systems and methods of converting data having multiple formats to a predefined format and providing centralized client-side data storage and retrieval of the converted data.

BACKGROUND OF THE INVENTION

[0003] Client terminals having software applications that access data stored on remote servers are well-known. The client terminals access the Internet or other remote networks to obtain web-based application data that is stored on remote servers. During communication outages, the client terminals are not able to access the remote servers hosting the web-based data. Thus, communication outages may cause client terminal users to experience productivity loss, data loss, or other losses.

[0004] Client terminals may include applications that store data on the respective client terminal devices and provide off-line access to the stored data. Known client terminal devices store the data in a format that is defined by the application that generates the data. Known systems require each application to generate and store data in a separate database on the client terminal device. Each separate database is distributed and is accessible only to the application that generated the data. In other words, known systems do not grant data access to other applications running on the client terminal devices that did not generate the data.

Various other drawbacks exist with these known systems and with other systems known in the prior art.

SUMMARY OF THE INVENTION

[0005] Various aspects of the invention overcome at least some of these and other drawbacks of existing systems. The invention advantageously discloses a method and system for providing a plurality of client terminal devices with connectivity to a central device during off-line operation.

[0006] In one embodiment, the invention provides a local communication device that locally stores data obtained from a plurality of sources, including a remote server, a local server and a client terminal device. The remote server is associated with an external network and the local server is associated with an internal network. The client terminal device communicates with the remote server over the external network and communicates with the local server over the internal network. The local communication device includes a software agent that communicates with the local server, the remote server and the client terminal device to gather the data from the local server, the remote server and the client terminal device and provides access to the data during time periods when a data connection is disrupted between the client terminal device and the local server or the remote server. The local communication device further includes a storage module that is adapted to store the gathered data to at least one memory device and a conversion module that generates a predefined format for the gathered data.

[0007] In another embodiment of the invention, the invention provides a local communication device that locally stores data obtained from a plurality of sources, including a remote server, a local server and a client terminal device. The remote server is associated with an external network and the local server is associated with an internal network. The client terminal device communicates with the remote server over the external network and

communicates with the local server over the internal network. The local communication device includes a software agent that communicates with the local server, the remote server and the client terminal device to gather the data from the local server, the remote server and the client terminal device and provides access to the data during time periods when a data connection is disrupted between the client terminal device and the local server or the remote server. The local communication device further includes a database module that generates and manages at least one database, a storage module that is adapted to store the gathered data to the at least one database, a conversion module that generates a predefined format for the gathered data and a synchronizing module that maintains a data version tag for the data stored in the at least one database.

[0008] In yet another embodiment of the invention, a method of facilitating off-line connectivity to a central database is provided. A local communication device stores the data transmitted between selected sources and the client terminal devices and monitors whether the client terminal devices are communicating with the selected sources. When the client terminal devices become decoupled from the selected sources, the local communication device establishes a data connection with the client terminal devices, transmits data to the client terminal devices, and assigns a synchronization start identifier, one or more synchronization intermediate identifiers and a synchronization completed identifier to facilitate data transfer with the selected sources. The local communication device monitors whether a data connection is re-established between the client terminal devices and the selected sources and re-establishes a data connection between the client terminal devices and the selected sources when the client terminal devices are coupled to the selected sources.

[0009] Data is transmitted between selected sources and client terminal devices and the data is stored to a local communication device. If a communication channel between the client terminal devices and the selected sources is disrupted, then a data connection is established

between the client terminal devices and the local communication device. During the network outage, data is transmitting between the local communication device and the client terminal devices. The local communication device and the selected sources synchronize the stored data to provide the latest retrieved data. The client terminal devices are coupled to the selected sources upon determining that the data connection is re-established between the client terminal devices and the selected sources and any data that is entered during offline operation may be synchronized to the selected data source.

[0010] The invention provides numerous advantages over and/or avoids many drawbacks of conventional systems. These and other features and advantages of the invention will be apparent through the detailed description of the embodiments and the drawings attached hereto. It is also understood that both the foregoing general description and the following detailed description are exemplary and not restrictive of the scope of the invention. Numerous other features and advantages of the invention should become apparent upon a reading of the following detailed description when taken in conjunction with the accompanying drawings, a brief description of which is included below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] A more complete understanding of the present invention, and the attendant advantages and features thereof, will be more readily understood by reference to the following detailed description when considered in conjunction with the accompanying drawings wherein:

[0012] FIG. 1 illustrates a system diagram according to one embodiment of the invention.

[0013] FIG. 2 illustrates an exemplary embodiment of the system of FIG. 1 operating in an environment where external communications paths couple the local devices and the external network devices.

[0014] FIG. 3 illustrates an exemplary embodiment of the system of FIG. 1 operating in an environment where external communications paths are decoupled between the local devices and the external network devices and internal communications paths couple the local devices with the local communications device.

[0015] FIG. 4 illustrates a system for transferring data between a remote server and a local communication device according to one embodiment of the invention.

[0016] FIG. 5 illustrates a flow chart for providing a plurality of client terminal devices with off-line connectivity to a central database.

DETAILED DESCRIPTION OF THE INVENTION

[0017] The invention provides systems and methods of employing a local communication device that performs centralized client-side data storage and retrieval. The local communication device may be coupled to a plurality of sources, including external networks, internal networks and client terminal devices, among other sources. The local communication device receives data from and transmits data to the plurality of sources and converts the data to preselected formats prior to storage. For example, the local communication device may receive data in any format including MS Word format, MS Excel format, PDF format, or any other format. Prior to storage, the local communication device may convert the received data to preselected formats including Health Level Seven (HL7), Extensible Markup Language (XML), American National Standards Institute (ANSI) standards, viewable format through MEDIOS proprietary application or other preselected formats.

[0018] By contrast, known systems employ distributed architectures that include client terminal devices having individual applications that generate distributed databases on the corresponding client terminal device. The distributed databases are stored at the client

terminal devices and are accessible only by the individual applications that generate the distributed database. Thus, known systems are deficient at least because the data stored in the distributed database is segmented, non-centralized, non-portable and is available only to the corresponding individual applications.

[0019] While specific embodiments of the invention are discussed herein and are illustrated in the drawings appended hereto, the invention encompasses a broader spectrum than the specific subject matter described and illustrated. As would be appreciated by those skilled in the art, the embodiments described herein provide but a few examples of the broad scope of the invention. There is no intention to limit the scope of the invention only to the embodiments described.

[0020] Computer networks offer great potential for automating information retrieval and storage. FIG. 1 illustrates an example of the system architecture 100 according to one embodiment of the invention. Client terminal devices 102a-102n (hereinafter identified collectively as 102) may be coupled to one or more local servers 104a-104n (hereinafter identified collectively as 104) and/or to one or more remote servers 130a-130n (hereinafter identified collectively as 130) via a wired network, a wireless network, a combination of the foregoing and/or other networks, such as a local area network 106 and an external network 125. A local communication device 110 may be provided to capture and store data communications between the client terminal devices 102, the local servers 104 and the remote servers 130 and other components.

[0021] The local communication device 110 may be of modular construction to facilitate adding, deleting, updating and/or amending modules therein and/or features within modules. Modules may include a software agent 112, a storage module 114, a scheduling module 116, a database module 118, a switching module 120, a synchronizing module 121, a conversion module 122, an alert module 123 or other modules. It should be readily understood that a

greater or lesser number of modules might be used. One skilled in the art will readily appreciate that the invention may be implemented using individual modules, a single module that incorporates the features of two or more separately described modules, individual software programs, and/or a single software program.

[0022] The software agent 112 may request data from the plurality of sources with or without end user awareness of the data requests. For example, the software agent 112 may capture data exchanges that occur during communications between the client terminal devices 102 and the remote servers 130, wherein the data exchanges are routed through the external network 125, such as the Internet. The software agent 112 may capture the data exchanges in substantially real-time or at predefined intervals. Alternatively, the software agent 112 may trigger capturing the data exchanges based on availability of system resources, such as bandwidth or other system resources. A storage module 114 may be provided to direct the captured data to a desired memory device for storage.

[0023] The software agent 112 may include applications that perform the data capture on sources that are coupled to the local communication device 110. The sources may include the client terminal devices 102, the local servers 104, and the remote servers 130, among other sources. For sources that request security credentials (e.g., passwords, digital certificates, etc.) prior to granting access to the data, the software agent 112 may perform authentication prior to requesting the data transfer to the local communication device 110. Alternatively, the software agent 112 may await a user log-in with the security credentials prior to requesting data transfer to the local communication device 110. Local communication device 110 provides access to the data independent of the geographical location or time periods when a data connection is disrupted between the client terminal devices 102 and local communication device 110 or between local communication device 110 and remote servers 130.

[0024] If users are not authenticated, then the users may be invited to submit requested information or take other action. If the user is authenticated, then the selected sources may perform other processing. For example, the selected sources may load data or other information (e.g., download) to the client terminal devices 102 that an authorized user may be permitted to access, but has not yet received from the selected sources.

[0025] With regard to user authentication, one of several different authentication schemes may be employed, and would be appreciated by those skilled in the art. For example, the user may be asked to input an alphanumeric code. Alternatively, the user may be asked to provide biometric information (i.e., a thumbprint through a fingerprint scanner) or other suitable identifying information. One of ordinary skill in the art will readily recognize that other authentication schemes may be employed.

[0026] The local communication device 110 may operate as a redundancy device that stores data accessed or data sought to be accessed by the plurality of sources. FIG. 2 illustrates an exemplary embodiment of the system of FIG. 1 operating under conditions where external communication paths 202 couple the remote server 130 to the client terminal devices 102, the local server 104 and/or the local communication devices 110. During operation, the client terminal devices 102 and the local server 104 transmit and receive data from the remote server 130. The local communication device 110 may communicate with the remote server 130 to duplicate and locally store data received from the remote server 130.

[0027] Referring to FIG. 1, the software agent 112 may instruct the local communication device 110 to continuously store the requested data. Alternatively, the software agent 112 may instruct the local communication device 110 to update the requested data at predefined schedules or automatically upon availability. A scheduling module 116 may be provided in the local communication device 110 to establish the predefined schedules to include periodic

schedules, random schedules, scheduling based on system resources, or other predefined schedules.

[0028] The local communication device 110 may include a database module 118 that generates and manages a central database 124. The central database 124 may be accessed by one or more sources, including the client terminal devices 102, the local servers 104 and the remote servers 130. The central database 124 may be structured to mirror the data structure of the selected sources, including the client terminal devices 102, the local servers 104 and the remote servers 130.

[0029] According to one embodiment, the local communication device 110 may include a switching module 120 that operates to switch a data connection for the client terminal devices 102 between the selected sources and the central database 124. The operation of switching the data connection for the client terminal devices 102 between the selected sources and the central database 124 may be transparent to users of the client terminal devices 102.

Alternatively, the operation of switching data connections for the client terminal devices 102 between the selected sources and the central database 124 may be initiated by users of the client terminal devices.

[0030] The switching module 120 may include a feature that determines the communication status of the client terminal devices 102. The feature may detect whether the client terminal devices 102 are operating online or offline, relative to the external network 125. Additionally, the switching module 120 may detect a type of network connection for the client terminal devices 102, such as a wired connection, a wireless connection or other network connection. If the client terminal devices 102 are determined to be operating offline relative to the external network 125, then the client terminal devices 102 may be coupled to the corresponding local communication device 110.

[0031] FIG. 3 illustrates an exemplary embodiment of the system of FIG. 1 operating in an environment where external communication paths 202 are decoupled between the local devices and the external network devices. Under this condition, internal communication paths 302 are provided to couple the local communications device 110 with the client terminal devices 102 and the local server 104. Since the local communication device 110 locally stores a duplicate of the data stored at the remote server 130, users that are accessing the client terminal devices 102 and the local server 104 do not experience a service disruption when the external communication paths 202 are decoupled.

[0032] Regarding transparent switching, the switching module 120 of FIG. 1 may detect trigger events to automatically initiate switching the data connections between the selected sources and the central database 124. The trigger events may include detecting time periods when communication channels to the selected sources are not available, among other trigger events.

[0033] Regarding user-initiated switching, the switching module 120 may respond to a manually initiated trigger to switch the data connections between the selected sources and the central database 124. The manually initiated trigger may include enabling users to activate a command at the client terminal devices 102 when communication channels to the selected sources are not available, among other manually initiated triggers.

[0034] The local communication device 110 may include a synchronizing module 121 that maintains data version tags for the data stored at the selected sources and the central database 124. The data version tags may be used at the selected sources and the central database 124 to identify the data that is stored most recent in time. According to one embodiment, the synchronizing module 121 may analyze the data version tag and determine whether to replicate data from the selected sources to the central database 124 or from the central database 124 to the selected sources. In this way, the synchronizing module 121 prevents the

client terminal devices 102 from accessing expired data. According to one embodiment, the synchronizing module 121 may determine whether the selected sources or the central database 124 is maintaining the most recent data version tag by analyzing which of the selected sources or the central database 124 performed the last save function. Additionally, the remote server 130 may be configured to synchronize a plurality of local communication devices 110 that are spread across multiple networks. The synchronization module 121 may employ a success/fail transaction protocol that ensures data is successfully transferred without any loss of connectivity.

[0035] According to one embodiment, the synchronization module 121 may apply a transaction based, encryption and decryption synchronization algorithm to perform data transfers in predefined stages. The predefined stages may include a start point, breakpoints and a commit point. By performing data transfers using stages, the initial data transfer may be completed even if a data transfer communication is interrupted during transmission. The synchronization module 121 identifies a start point to the beginning of a selected data transfer. After identifying the start point, the synchronization module 121 may assign intermediate breakpoints to the transferred data. The breakpoints are provided to recover data transfer operations if an interruption occurs before the data transfer is complete. For example, after experiencing a data transfer interruption, the data transfer operation may begin from a previously identified successful breakpoint. In other words, the synchronization module 121 enables the data transfer operation to recover from a breakpoint or intermediate transfer point, rather than from the start point or the beginning of the data transfer. When the last breakpoint is successfully traversed, the synchronization module 121 assigns an identification number to the data transfer. Additionally, the synchronization module 121 may classify the data transfer as authentic and complete.

[0036] In another embodiment, synchronization module 121 is adapted to monitor a broadcast system that is operated over the network device and into the external network over a predefined protocol. A predefined logical port automatically resolves conflicts of data and, via a series of algorithms, and automatically reestablishes synchronization from the local network and a set of one or more external servers.

[0037] FIG. 4 illustrates a system for performing data transfer. The remote server 130 and the local communication device 110 begin a synchronization process over communication channel 402 using a plurality of intermediate breakpoints or synchronization intermediate identifiers (403a-403n). According to one embodiment, breakpoint 1 (403a) and breakpoint 2 (403b) are established between the remote server 130 and the local communication device 110. During the data transmission, the remote server 130 and the local communication device 110 transmit status information over communication channel 404.

[0038] According to one embodiment, the data transmission may occur without experiencing a data transfer interruption. For a synchronization transfer between the remote server 130 and the local communication device 110, the synchronization module 121 may identify a Start Point 1 or start identifier at 01/01/Yr1, 03:00:00 SERVER TIME and data transfer may begin over communication channel 402. The data transfer may traverse BREAKPOINT 1 (403a) at 01/01/Yr1, 03:03:00 SERVER TIME and may traverse BREAKPOINT 2 (403b) at 01/01/Yr1, 03:06:00 SERVER TIME and be successfully completed. Upon success completion, the synchronization module 121 may establish a COMMIT POINT and assign a synchronization complete identification number ID:0001:01/01/Yr1, 03:06:00 SERVER TIME. The data transfer may be considered complete and authenticated upon assignment of identification number ID:0001.

[0039] Alternatively, the data transmission may occur with a data transfer interruption. For a synchronization transfer between the remote server 130 and the local communication device

110, the synchronization module 121 may identify a Start Point 1 at 01/01/Yr1, 03:00:00 SERVER TIME and data transfer may begin over communication channel 402. The data transfer may traverse BREAKPOINT 1 (403a) at 01/01/Yr1, 03:03:00 SERVER TIME and may experience an INTERRUPTION at 01/01/Yr1, 03:04:30 SERVER TIME, such as if the server encounters bandwidth loss. The synchronization module 121 may initiate a rollback to BREAKPOINT 1 at 01/01/Yr1, 03:04:35 SERVER TIME. Upon reestablishment of bandwidth at 01/01/Yr1, 03:20:30 SERVER TIME, the synchronization module 121 may begin the data transfer at BREAKPOINT 1 at 01/01/Yr1, 03:20:35 and may traverse BREAKPOINT 2 at 01/01/Yr1, 03:23:35 SERVER TIME and be successfully completed. Upon success completion, the synchronization module 121 may establish a COMMIT POINT, assign identification number ID:0002:01/01/Yr1, 03:23:35 SERVER TIME. The data transfer may be considered completed authenticated upon assignment of identification number ID:0002.

[0040] Referring to FIG. 1, the local communication device 110 may include a conversion module 122 that converts the received data to preselected formats including Health Level Seven (HL7), Extensible Markup Language (XML), American National Standards Institute (ANSI) standards, or other preselected formats prior to storage. Other standards that enable interoperability may be employed, such as but not limited to CCD, DICOM, HIPAA, and HITSP. The ANSI compliant file may be denoted as a Vessel Data Exchange (VDE) file.

[0041] The data that is stored in the central database 124 may be searched using a variety of techniques. According to one embodiment, the search may be performed using a structured query language (SQL) that uses SQL statements to perform tasks on the database 124, such as retrieving data from the database 124.

[0042] The local communication device 110 may include an alert module 123 that generates notifications and/or alerts in real-time. The generated notifications and/or alerts may be delivered in real-time to notify users of the status of the network connectivity.

[0043] The client terminal devices 102 may include any number of different types of client terminal devices, such as medical devices, medical equipment, personal computers, laptops, smart terminals, personal digital assistants (PDAs), mobile devices, cell phones, Web TV systems, video game consoles, and devices that combine the functionality of one or more of the foregoing or other client terminal devices. The client terminal devices 102 may include processors, RAM, USB interfaces, telephone interfaces, satellite interface, microphones, speakers, a stylus, a computer mouse, a wide area network interface, a local area network interface, hard disks, wireless communication interfaces, DVD/CD reader/burners, a keyboard, a flat touch-screen display, and a display, among other components.

[0044] According to one embodiment, the client terminal devices 102 may include a touch-sensitive display screen, a handset, speakers and input buttons, among other features. Select functions may be implemented on the client terminal devices 102 by positioning an indicator over selected icons and manipulating an input receiving device such as a touch-sensitive display screen, a mouse, a keyboard, a voice recognition system or other input receiving devices. The client terminal devices 102 may include a video input device to permit audio-visual communication with other client terminal devices 102, such as to permit dictation by medical personnel. The client terminal devices 102 may communicate with the remote servers 130, the local servers 104, other client terminal devices 102 and/or other systems.

[0045] Users may access the client terminal devices 102 to communicate with the selected sources, including the client terminal devices 102, the local servers 104 and the remote servers 130. Data requests that originate from the client terminal devices 102 may be broadcast to selected sources and the local communication device 110 in substantially in real-

time if the client terminal devices 102 are coupled to networks 106,125. Alternatively, communications from the client terminal devices 102 may be delayed for an amount of time if, for example, a selected client terminal device 102 is not connected to the local area network 106. For example, the data connection between the client terminal device 102 and the local server 104 or the remote server 130 may be disrupted due to a large latency, a delayed connection, or a severed connection, among other disruptions.

[0046] According to one embodiment of the invention, any requests that are made while the client terminal devices 102 are not connected to the local area network 106 may be stored and propagated from/to the offline client terminal device 102 when the selected sources, the local communication device 110 and the target client terminal device 102 are re-connected to networks 106/125. For example, if the target client terminal device 102 is not connected to network 106, then requests remain in the corresponding client terminal device 102 for dissemination to the local communication device 110 or the selected sources when the target client terminal devices 102 are re-connected to networks 106/125.

[0047] FIG. 5 illustrates a method 500 of providing a plurality of client terminal devices with off-line connectivity to a central database. Data is transmitted between the selected sources and the client terminal device 102 in operation 501, wherein data communication is performed via networks 106/125. For example, the network 125 may include the Internet. Data communication between the client terminal devices 120 and the selected sources may occur substantially in real-time if the client terminal devices 102 are connected to the networks 106/125. In operation 503, data is transmitted between the selected sources and the local communication device 110, wherein the data communication is performed via network 106/125. One of ordinary skill in the art will appreciate that communications may be conducted in various ways and among various devices.

[0048] A determination is made in operation 505 whether the client terminal devices 102 remain in communication with the selected sources. If the client terminal device 102 and the selected sources remain in communication, then the system returns to operation 501. If the client terminal device 102 and the selected sources are no longer in communication, then the client terminal device 102 is coupled to the local communication device 110 in operation 507. In operation 509, data is transmitted between the client terminal devices 102 and the local communication device 110, wherein the data communication is performed via network 106. One of ordinary skill in the art will appreciate that communications may be conducted in various ways and among various devices.

[0049] A determination is made in operation 511 whether the connection between the client terminal devices 102 and the selected sources is restored. If the connection between the client terminal device 102 and the selected sources is not restored, then the system returns to operation 507. If the connection between the client terminal device 102 and the selected sources is restored, then the system synchronizes data between the local communication device and the selected sources in operation 513 and the system returns to operation 501.

[0050] In another embodiment, the technology includes a distributed system with one or multiple locations with an optionally defined central hub. The information on each of the nodes is accessed locally by users in that network and is not limited by the connectivity to any of the other nodes. The information is readily available on all nodes as needed on a continuous or scheduled basis with an algorithm that decides how to synchronize. The synchronization can be made either ubiquitous (e.g., complete) so that each node has the same information, or the synchronization can be selective, in which case it only transfers the minimum data needed to operate, plus any additional data selected. The nodes could be stationed on mobile devices such as a network of mobile phones or mobile vessels such as, for example, but not limited to, a truck, a tank, a boat or an airplane. As a second layer of

data transfer, in addition to the database, the file system is also transferred by default in selective mode (e.g., it only transfers the minimum needed to operate). The system is self-maintained and possesses an updated mechanism. It also has a disaster recovery mechanism allowing for the system to fully recover itself with a very short recovery time objective (RTO) and recovery point objective (RPO).

[0051] Transfer Technology

Communications from or to the nodes can occur via Transmission Control/Internet Protocol (TCP/IP) using TCP and User Datagram Protocol (UDP) transport protocols. The specific port numbers can be configured at the time of setup. Packages can be compressed using, for example, the ZLib filter which uses the DEFLATE algorithm.

[0052] Ubiquitous Database Transfer

Database data can be stored in any standard relational database including, but not limited to, MySQL, PostgreSQL Lite, and MICROSOFT SQL. The database is configured to report binary logs to a pre-defined local location. A daemon reads each bin-log entry and broadcasts to each enabled node. The bin-log is assigned a globally unique ID and then each node attempts to execute the selected bin-log entry one at a time. Each bin-log entry contains one or multiple SQL statements. The statements can be executed in real-time and in case of two statements attempting to affect the same row, the latest insert prevails. Each node manages time by setting a Network Time Protocol (NTP) with predefined time settings.

[0053] Execution and Error Resolution

The system can be configured to handle errors in different ways. For example, a Latest Entry Prevails method handles errors by default, by executing all queries and the latest query affecting the same row prevails. Thus, if a conflict arises, each transaction is inserted and a latest inserted occurrence would prevail. In a Priority Node method, a node can be

configured to have priority over other nodes. Therefore, if two statements affect the same row within a pre-configured time, the priority node would prevail.

[0054] Error Handling

Based on the conflict resolution strategy, the outcome could be handled in several ways. For example:

- Stop Execution: If an error statement is detected, synchronization is disabled until manual intervention. This ensures full data integrity across the nodes.
- Do nothing: Ignore entries that generate an error and continue to the next statement.
- A conflict resolution mechanism can be used where transactions are merged across one or more remote servers 130.

[0055] Selective Database (DB) Transfer

The use of Selective DB can be accomplished with any relational database including, for example, MySQL, Postgres, SQLite and MSSQL as well as any Non-SQL protocols such as Elastic, MongoDB, CouchDB or Cassandra. The disclosure is not limited to a specific type of relational database. An atomic record is first established. An atomic record is defined as the core entity in the system needed for business operation, and then all dependent entities attached are automatically encapsulated within the atomic record. The record can then be transferred over TCP/IP to one or all nodes. The record can be transferred via a serialized object. The serialized object can be compressed using a ZLib filter based on the DEFLATE strategy. The receiving end un-compresses the serialized string and serializes the object, re-populating with the latest version of the entity and dependent entities. Thus, no conflict resolution is needed as every entry is inserted as it comes based on the Latest Entry Prevails. Transfer control assurance can be configured to either confirm the receipt of the object or

attempt to resend it if it failed to receive it. This option can be disabled to not expect a confirmation-of-receipt to minimize package size.

[0056] Selective Files Transfer

Separate from the DB data, the files needed to operate the business logic are identified by the application at runtime by flagging each file with its creation location. All files can be scanned at any preselected intervals, (e.g., scanned every 1-minute) to detect any changes. If another node is requesting the use of the file, then this file is flagged in the requesting node. The flag is transferred to all the nodes via the DB replication. Following this, the file is transferred to any of the requesting nodes. The file can be compressed using ZLib based on the DEFLATE strategy, although other compression protocols may be used. The files can also be deleted from any node where the file is not flagged as being required by the business application.

[0057] Self-Maintain and Update Mechanism

The system can install all required updates as flagged by a central server using the LINUX-based Advanced Packaging Tool (APT) package manager. This includes all operating system (OS) layer updates as well as any other required package needed for operation as flagged by configuration on a central server. The application layer is updated by a remote control script that can be written in, for example, BASH, PERL and PYTHON, which retrieves all the required files needed for the application and transfers them to the nodes. Upon completion of this process, each of the nodes sends a notification to all the other nodes using the DB replication and then self-stop replication. The update takes place by backing up the current application and then replacing all files with the new files. The replication is then restored and a notification is sent to the other nodes. In case of an error, the system remains in maintenance mode and awaits manual intervention. All other nodes continue to operate normally.

[0058] Disaster Recovery Mechanism Strategy

In case of a disaster, the system is reinstalled and flagged as a “fresh” DB. Upon the start of replication, the required data to operate is transferred from the other nodes to take the system to the latest level of data.

[0059] Recovery Point Objective (RPO)

RPO is determined by the bandwidth available at the time of the disaster. The last sequence broadcasted from the node to the other nodes becomes the recovery point objective.

[0060] Recovery Time Objective

Recovery time objective is determined by the bandwidth available after the disaster. The fastest the connection, the faster the RPO will be reached.

[0061] Break-Glass Mechanism

In case of a disaster or for any trigger previously configured by the business application, the system can issue a Quality of Service (QoS) upgrade request via Simple Network Management Protocol (SNMP) or any other pre-established mechanism to upgrade the QoS and therefore speed up data transfer.

[0062] A set of devices and peripherals can be connected to any of terminals devices 102 to collect biometrics data, financial data and/or medical data. The data may be stored locally in terminal device 102, transferred to local server 104 and/or replicated to each of the nodes.

The connection from the devices to the terminals can be any standard connection protocol, for example, USB, Serial, BLUETOOTH, Wi-Fi or Network TCP/IP. The data can be transferred using one or more of many different formats such as, for example, HL7, CSV or XML. Biometric data may be collected via the use of one or more traditional data collection methods including but not limited to fingerprint, palm scan, retina scan, and/or facial recognition. Financial data may be collected with the use of one or more scanning techniques

such as but not limited to magnetic cards, smart chip cards, BLUETOOTH identifiers and/or barcode ID's. Medical data may be collected with the use of a wide array of medical devices including but not limited to EKG devices, pulse detectors, blood pressure monitors, oximetry sensors, weight and height scales, X-Ray Devices (both digital and film-based), blood analyzers, urine analyzers, stool analyzers, ultrasound devices and Doppler devices, among others.

[0063] The invention can be realized in hardware, software, or a combination of hardware and software. Any kind of computing system, or other apparatus adapted for carrying out the methods described herein, is suited to perform the functions described herein.

[0064] A typical combination of hardware and software could be a specialized computer system having one or more processing elements and a computer program stored on a storage medium that, when loaded and executed, controls the computer system such that it carries out the methods described herein. The invention can also be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which, when loaded in a computing system is able to carry out these methods. Storage medium refers to any volatile or non-volatile storage device.

[0065] Computer program or application in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after either or both of the following a) conversion to another language, code or notation; b) reproduction in a different material form.

[0066] It will be appreciated by persons skilled in the art that the invention is not limited to what has been particularly shown and described herein above. In addition, unless mention was made above to the contrary, it should be noted that all of the accompanying drawings are

not to scale. A variety of modifications and variations are possible in light of the above teachings without departing from the scope and spirit of the invention, which is limited only by the following claims.

CLAIMS

What is claimed is:

1. A local communication device that locally stores data obtained from a plurality of sources, the local communication device being in communication with a local server that is associated with a local network, the local server also associated with an external network, and at least one client terminal device that communicates with the local server over an internal network, the local server synchronizing with a set of at least one or more remote servers over the external network, the local communication device comprising:

a software agent that communicates with the local server, the set of at least one or more remote servers and the at least one client terminal device to gather the data from the local server, the set of at least one or more remote servers and the at least one client terminal device, wherein the local communication device provides access to the data independent of geographical location or time periods when a data connection is disrupted between the at least one client terminal device and the local device, or between the local device and the set of at least one or more remote servers;

a storage module that is adapted to store the gathered data to at least one memory device;

a conversion module that generates a predefined format for the gathered data; and

a synchronizing module that applies a transaction-based encryption/decryption synchronization algorithm to transfer data at predefined stages between at least two of the local server, the set of at least one or more remote servers and the at least one client terminal device.

2. The local communication device of claim 1, wherein the data transfer is ubiquitous.

3. The local communication device of claim 1, wherein the data transfer is selective.

4. The local communication device of claim 1, wherein the at least one client terminal device is located on a mobile device.

5. The local communication device of claim 4, wherein the mobile device is located on a mobile vessel.

6. The local communication device of claim 1, further comprising a biometrics data collection device configured to collect one or more of biometrics data, financial data or medical data.
7. The local communication device of claim 6, wherein the biometrics data is stored in the at least one client terminal device.
8. The local communication device of claim 6, wherein the biometrics data is stored in the local server.
9. The local communication device of claim 1, wherein the synchronization module further comprises a conflict resolution mechanism configured to merge multiple transactions into a single transaction across the set of at least one or more remote servers.
10. A method of providing at least one client terminal device with off-line connectivity to a central database, the method comprising:
 - storing data transmitted between selected sources and the at least one client terminal device;
 - monitoring whether the at least one client terminal device is communicating with the selected sources;
 - establishing a data connection with the at least one client terminal device when the at least one client terminal device becomes decoupled from the selected sources;
 - transmitting data to the at least one client terminal device;
 - applying a transaction-based encryption/decryption synchronization algorithm to transfer data at predefined stages between the selected sources;
 - monitoring whether a data connection is re-established between the at least one client terminal device and the selected sources; and
 - re-establishing a data connection between the at least one client terminal device and the selected sources when the at least one client terminal device becomes coupled to the selected sources.
11. The method of claim 10, wherein transmitting the data to the at least one client terminal device is a ubiquitous data transfer.

12. The method of claim 10, wherein transmitting the data to the at least one client terminal device is a selective data transfer.
13. The method of claim 10, wherein the at least one client terminal device is located on a mobile device.
14. The method of claim 13, wherein the mobile device is located on a mobile vessel.
15. The method of claim 10, further comprising collecting biometrics data and storing the biometrics data in the at least one client terminal device.
16. The method of claim 10, further comprising merging multiple transactions into a single transaction across the selected sources in order to resolve conflicts.
17. The method according to claim 10, further comprising providing predefined schedules for storing the data that is transmitted between the selected sources and the client terminal devices.
18. The method according to claim 17, wherein providing predefined schedules includes storing the data based at least on one of periodic intervals, random intervals or system triggered intervals.
19. The method according to claim 10, wherein re-establishing a data connection between the client terminal devices and the selected sources is performed automatically.
20. The method of claim 10, further comprising configuring one or more particular client terminal devices to have priority over other client terminal devices such that selective data can be transmitted from the selected sources to the one or more particular client terminal devices before data is transmitted to the other client terminal devices.
21. The local communication device of claim 1, further comprising an alert module configured to generate one or more alerts in real-time, the one or more alerts configured to notify users of a status of the data connection.

22. The local communication device of claim 21, wherein the one or more alerts includes a request to the local server to automatically disable the synchronization in order to prevent replication of an error.