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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 March 2008 (20.03.2008)

PCT

(10) International Publication Number
WO 2008/032304 A2

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/IL2007/000874

(22) International Filing Date: 17 July 2007 (17.07.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/519,971 13 September 2006 (13.09.2006) US

(71) Applicant *(for all designated States except US)*: **NICE SYSTEMS LTD.** [IL/IL]; Hapninah 8, 43107 Raanana (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BEN-AMI, Hadas** [IL/IL]; Halotem 7A, 42493 Netanya (IL). **PORTMAN, Leon** [IL/IL]; Hazofim 12, 75832 Rishon Lezion (IL). **HOFFMAN, Dvir** [IL/IL]; Haeshel 7A, 44235 Kfar Saba (IL). **FISHER, Oren** [IL/IL]; Aharon Becker 1A, 69643 Tel Aviv (IL).

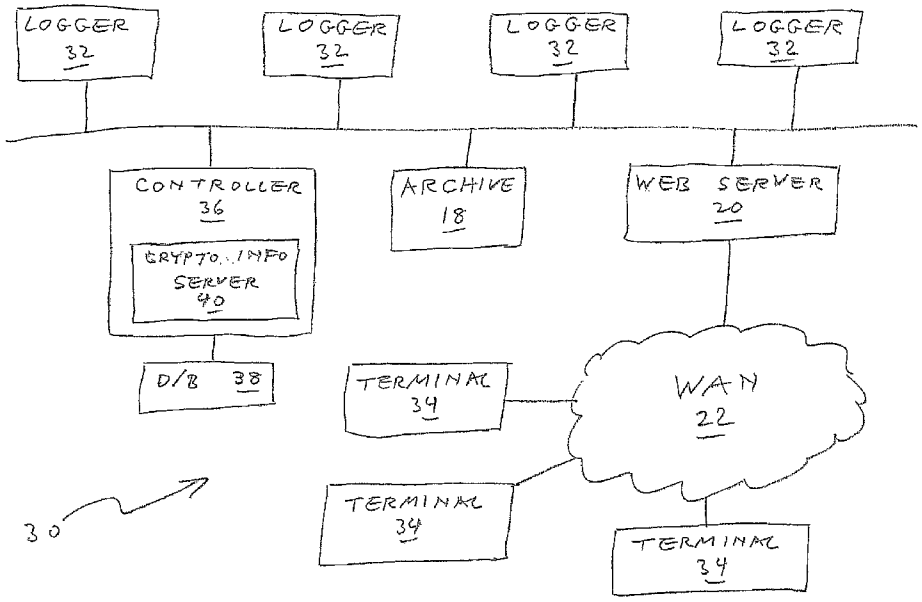
(74) Agent: **FRIEDMAN, Mark**; 7 Jabotinsky St., 52520 Ramat Gan (IL).

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

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

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

(54) **Title:** METHOD AND SYSTEM FOR SECURE DATA COLLECTION AND DISTRIBUTION



(57) **Abstract:** A data provider generates a data encryption key and an identifier, uses the data encryption key to encrypt data, sends the encrypted data and the identifier to a data requestor, and sends the data encryption key and the identifier to a crypto information server. The data requestor sends the identifier to the crypto information server to request the encryption key. The crypto information server authenticates the data requestor and, contingent on that authentication, sends the data encryption key to the data requestor. If a plurality of data instances are captured, then for each instance, a respective data encryption key and identifier are generated.

WO 2008/032304 A2

METHOD AND SYSTEM FOR SECURE DATA COLLECTION AND DISTRIBUTION

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a method and system for collecting data at a source and distributing the data to one or more destinations and, more particularly, to such a method and system in which the data are protected from eavesdropping and from unauthorized changes from when the data leave the source until the data arrive at their ultimate destination(s).

The efficient storage and retrieval of multi-channel data communications, and especially of voice data, are critically important in many modem business and government applications. For example, financial institutions record instructions from clients as a protection against fraud and as evidence in legal proceedings about the content of telephone conversations; public safety agencies record emergency calls for event reconstruction and future investigations; commercial entities monitor transactions over the phone to evaluate salespersons' efficiency, to ensure customer satisfaction and to develop training programs.

Data logging and retrieval systems for capturing, recording and retrieving data transmitted over multiple communication lines are known in the art. See for example Henits, US Patent No. 6,775,372, which patent is incorporated by reference for all purposes as if fully set forth herein, and the references cited therein. Figure 1 is a high-level schematic block diagram of an exemplary prior art system **10** for capturing, storing and retrieving telephone conversations. System **10** is based on a Local Area Network (LAN) **12** that uses the IP protocol to transfer digital data, borne by IP packets, among the other components of system **10**. System **10** includes several loggers **14**, as described for example in the Henits patent, for capturing digital data that represent telephone conversations. Digital records of the telephone conversations are stored in an archive **18**. A controller **16** manages LAN **12**.

LAN **12** is connected to the outside world, specifically to a Wide Area Network (WAN) **22** such as the worldwide Internet, by a Web server **20**. User terminals **24**, represented as personal computers, also are connected to WAN **22**. A user of a terminal **24** uses a standard Web browser to access data stored in archive **18** via Web server **20**.

System **10** is vulnerable to eavesdropping. Even if, as is usually the case, data captured by loggers **14** is encrypted and is stored in an encrypted form in archive **14**, Web server **20** typically decrypts data requested by a user of a terminal **24** before exporting the

data to WAN **22**. There are many ways in which eavesdroppers can intercept the data on WAN **22**, especially if WAN **22** is the worldwide Internet.

System **10** also is vulnerable to unauthorized modification of the data. This is true even if access to data in archive **18** were to be limited to terminals connected to LAN **12**. For example, if archive **14** is responsible for encryption, data can be tampered with in transit from loggers **14** to archive **18**.

There is thus a widely recognized need for, and it would be highly advantageous to have, a data collection and distribution system in which the data are continuously protected from eavesdropping and unauthorized modification, from when the data leave their original source until the data arrive at their ultimate destination.

SUMMARY OF THE INVENTION

The present invention defends data against eavesdropping by encrypting the data as soon as the data are collected or generated and then keeping the data encrypted at all times until the data actually are displayed to an authorized user.

According to the present invention there is provided a method of distributing data, including the steps of: (a) encrypting the data, using a data encryption key, thereby providing encrypted data; (b) requesting the data, by a data requestor; (c) in response to the request, sending the encrypted data to the data requestor; (d) authenticating the data requestor, by a crypto information server; and (e) contingent on the authenticating, sending the data encryption key to the data requestor, by the crypto information server.

According to the present invention there is provided a system for secure distribution of data, including: (a) a data requestor; (b) a data provider operative: (i) to encrypt the data using a data encryption key, thereby providing encrypted data, and (ii) to send the encrypted data to the data requestor; and (c) a crypto information server operative: (i) to authenticate the data requestor, and (ii) contingent on the authentication, to send the data encryption key to the data requestor.

According to the present invention there is provided a method of collecting and distributing a plurality of instances of data, including the steps of: (a) for each instance: (i) generating a respective data encryption key, and (ii) encrypting the each instance, using the respective data encryption key, thereby providing respective encrypted data; (b) requesting at least a portion of one of the instances, by a data requestor; and (c) in response to the request,

sending a corresponding portion of the respective encrypted data of the one instance to the data requestor.

According to the present invention there is provided a system for secure collection and distribution of a plurality of instances of data, including: (a) a set, of at least one data provider, operative: (i) to capture the instances, and (ii) for each instance: (A) to generate a respective data encryption key, and (B) to encrypt the each instance, using the respective data encryption key, thereby providing respective encrypted data; (b) a data requestor operative: (i) to request at least a portion of one of the instances; and (c) an archive operative: (i) to store the encrypted data; and (ii) in response to the request of the at least portion of the one instance by the data requestor: to send a corresponding portion of the respective encrypted data of the one instance to the data requestor.

The first method of the present invention is a method of distributing data such as voice data, voice over IP (VoIP) data, video data and screen data, among others. According to the basic embodiment of the first method, the data are encrypted, using a data encryption key, to provide encrypted data. When a data requestor requests the data, the encrypted data are sent to the data requestor. A crypto information server authenticates the data requestor. Contingent on the authenticating, *i.e.*, if the crypto information server determines that the data requestor is authorized to receive the data, the crypto information server sends the data encryption key to the data requestor. Preferably, the data encryption key is a symmetric key, to enable the data requestor to decrypt the encrypted data. In the preferred embodiments below, user terminals **34** and **112** are the data requestors.

Preferably, the data encryption key is sent to the data requestor in encrypted form.

Preferably, the data requestor requests the data encryption key, and the authentication of the data requestor is in response to that request.

Preferably, the method includes generating the data encryption key and associating the data encryption key with a respective identifier. Most preferably, the data encryption keys are generated according to a predefined key granularity.

More preferably, the identifier is sent to the data requestor along with the encrypted data; and the data requestor sends the identifier to the crypto information server to request the data encryption key. The authentication of the data requestor is in response to receipt of the identifier from the data requestor by the crypto information server.

Also more preferably, the crypto information server stores the data encryption key and the identifier in a database. Most preferably, the data encryption key is stored in the database in encrypted form, to prevent unauthorized access of the data encryption key.

Preferably, the data are encrypted by a data provider, and the encrypted data also are stored in an archive that is separate from the data provider. When the data requestor requests the data, the encrypted data are sent to the data requestor from the archive. In the preferred embodiments below, loggers **32** are the data providers.

Preferably, a message authentication code is attached to the data prior to encrypting the data, so that the message authentication code becomes part of the data and is encrypted along with the data. The attaching of the message authentication code to the data may be, for example, by appending the message authentication code to the data, by prepending the message authentication code to the data or by inserting the message authentication code in the data. Contingent on the authenticating, the crypto information server sends a message authentication code key of the message authentication code to the data requestor.

More preferably, the method includes the steps of generating the data encryption key and the message authentication code key and associating the data encryption key and the message authentication code key with a common respective identifier. The identifier is sent to the data requestor along with the encrypted data; and the data requestor sends the identifier to the crypto information server to request the data encryption key and the message authentication code key. The authentication of the data requestor is in response to receipt of the identifier from the data requestor by the crypto information server. Most preferably, the data encryption key and the message authentication code key are generated according to a predefined key granularity.

Also more preferably, the crypto information server stores the data encryption key, the message authentication code key and the identifier in a database. Most preferably, the data encryption key and the message authentication code key are stored in the database in encrypted form, to prevent unauthorized access of the data encryption key and the message authentication code key.

A first basic system of the present invention, for secure distribution of data, includes a data requestor, a data provider and a crypto information server. The data provider encrypts the data using a data encryption key, thereby providing encrypted data, and sends the encrypted data to the data requestor. The crypto information server authenticates the data requestor. Contingent on that authentication, *i.e.*, if the crypto information server determines

that the data requestor is authorized to receive the data, the crypto information server sends the data encryption key to the data requestor. Preferably, the crypto information server sends the data encryption key to the data requestor in encrypted form.

Preferably, the data provider also generates the data encryption key and associates the data encryption key with a respective identifier. Most preferably, the data provider generates the data encryption key according to a predefined key granularity. More preferably, the data provider also sends the identifier to the data requestor along with the encrypted data and also sends the data encryption key to the crypto information server along with the identifier. The data requestor requests the data encryption key from the crypto information server by sending the identifier to the crypto information server. The authentication of the data requestor by the crypto information server then is in response to receipt of the identifier from the data requestor by the crypto information server.

Most preferably, both the data provider and the data requestor include respective instances of a crypto information client that is operative to generate the data encryption key and its respective identifier, to send the data encryption key and its identifier to the crypto information server, and to request the data encryption key from the crypto information server by sending the identifier to the crypto information server.

Even more preferably, the system also includes a database wherein the crypto information server stores the data encryption key and the identifier. Most preferably, the data encryption key is stored in the database in encrypted form.

Preferably, the system also includes an archive, separate from the data provider, for storing the encrypted data. The sending of the encrypted data from the data provider to the data requestor may be either direct or via the archive: most preferably, the archive is operative to send the encrypted data to the data requestor.

Preferably, the data provider also attaches a message authentication code to the data prior to encrypting the data, and, contingent on the authenticating, the crypto information server sends a message authentication code key to the data requestor.

More preferably, the data provider also generates the data encryption key and the message authentication code key, and associates the data encryption key and the message authentication code key with a common respective identifier. Even more preferably, the data provider also sends the identifier to the data requestor along with the encrypted data and also sends the data encryption key and the message authentication code key to the crypto information server along with the identifier. The data requestor requests the data encryption

key and the message authentication code key from the crypto information server by sending the identifier to the crypto information server. The authentication of the data requestor by the crypto information server then is in response to receipt of the identifier from the data requestor by the crypto information server. Most preferably, the data provider generates the data encryption key and the message authentication code key according to a predefined key granularity.

Most preferably, both the data provider and the data requestor include respective instances of a crypto information client that is operative to generate the data encryption key, the message authentication code key and their respective common identifier, to send the data encryption key, the message authentication code key and their identifier to the crypto information server, and to request the data encryption key and the message authentication code key from the crypto information server by sending the identifier to the crypto information server.

Even more preferably, the system also includes a database wherein the crypto information server stores the data encryption key, the message authentication code key and the identifier. Most preferably, the data encryption key and the message authentication code key are stored in the database in encrypted form.

A second method of the present invention is a method of collecting and distributing a plurality of instances of data. What constitutes an "instance" of data is implementation dependent. For example, in the first preferred embodiment discussed below, the data instances are files of audio data, and in the second preferred embodiment discussed below, the data instances are all the data captured in different external channels and all the data captured as a result of different initializations of screen agents **118**. According to the basic embodiment of the second method, for each data instance, a corresponding respective data encryption key is generated and the data instance is encrypted using that data encryption key, thereby providing respective encrypted data. When a data requestor requests at least a portion of one of the data instances, a corresponding portion of the requested data instance's respective encrypted data is sent to the data requestor.

Preferably, the requested data instance includes voice data, VoIP data, video data and/or screen capture data.

Preferably, the data encryption keys are symmetric keys, to enable the data requestor to decrypt the encrypted data.

Preferably, the data encryption keys are generated according to a predefined key granularity.

Preferably, each data instance is captured by a respective data provider that then generates the respective data encryption key and uses that data encryption key to encrypt the data instance.

Most preferably, the respective encrypted data of each data instance are stored in an archive separate from the data provider that captured the data instance. Encrypted data are sent to the data requestor from the archive rather than from the data provider that captured the corresponding data instance.

Preferably, the data requestor is authenticated by a crypto information server. Contingent on the authenticating, *i.e.*, if the crypto information server determines that the data requestor is authorized to receive the data, the crypto information server sends the respective data encryption key of the requested data instance portion to the data requestor, most preferably in encrypted form. More preferably, the authenticating is in response to the data requestor requesting the respective data encryption key of the requested data instance portion. Most preferably, each data encryption key is associated with a respective identifier that is sent to the data requestor along with the requested data instance portion, and the data requestor requests the respective data encryption key of the requested data instance portion by sending the associated identifier to the crypto information server. Also even more preferably, the crypto information server stores the data encryption keys and the identifiers in a database, most preferably in encrypted form.

Preferably, a respective message authentication code is attached to each data instance prior to encrypting the data instance, so that the message authentication code becomes part of the data instance and is encrypted along with the data instance. More preferably, a respective message authentication code key is generated and is used to generate the respective message authentication code. Most preferably, the message authentication code keys are generated according to a predefined key granularity. The attaching of the message authentication code to the data instance may be, for example, by appending the message authentication code to the data instance, by prepending the message authentication code to the data instance or by inserting the message authentication code in the data instance. The data requestor is authenticated by a crypto information server. Contingent on the authenticating, *i.e.*, if the crypto information server determines that the data requestor is authorized to receive the data, the crypto information server sends the respective data encryption key of the requested data

instance portion, along with a message authentication code key of the requested data instance portion, to the data requestor, most preferably in encrypted form. More preferably, the authenticating is in response to the data requestor requesting the respective data encryption key and the respective message authentication code key of the requested data instance portion. Most preferably, each data-encryption-key-message-authentication-code-key pair is associated with a respective identifier that is sent to the data requestor along with the requested data instance portion, and the data requestor requests the respective data encryption key and the respective message authentication code key of the requested data instance portion by sending the associated identifier to the crypto information server. Also even more preferably, the crypto information server stores the data encryption keys, the message authentication code keys and the identifiers in a database, most preferably in encrypted form.

A second basic system of the present invention, for secure collection and distribution of a plurality of instances of data, includes a set of one or more data providers, a data requestor and an archive. The set of data providers capturers the data instances and, for each captured data instance, generates a respective data encryption key and uses that data encryption key to encrypt the data instance, thereby providing respective encrypted data. The data requestor requests at least a portion of one of the data instances. The encrypted data are stored in the archive. In response to the request for the data instance portion, the archive sends the data requestor a corresponding portion of the respective encrypted data of the requested data instance portion.

Although the set of data providers could serve to archive their own encrypted data, especially in an embodiment with only one data provider, it is preferable that the archive be separate from the set of data providers.

Preferably, the set of data providers generates the data encryption keys according to a predefined key granularity.

Preferably, the system also includes a crypto information server that authenticates the data requestor and that, contingent on the authentication (*i.e.*, if the crypto information server determines that the data requestor is authorized to receive the data), sends the respective data encryption key of the requested data instance portion to the data requestor, most preferably in encrypted form.

More preferably, the data requestor also requests the respective data encryption key of the requested data instance portion from the crypto information server, and the authenticating is in response to that request. Even more preferably, the set of data providers

associates each data encryption key with a respective identifier, and the archive, in response to the request of the data instance portion by the data requestor, sends the respective identifier of the requested data instance portion to the data requestor along with the requested data instance portion. The data requestor then requests the respective data encryption key of the requested data instance portion from the crypto information server by sending the identifier of the requested data instance portion to the crypto information server.

Most preferably, each data provider, as well as the data requestor, includes a respective instance of a crypto information client that is operative to generate the data encryption keys and the identifiers, to send the data encryption keys and the identifiers to the crypto information server, and to request the data encryption keys from the crypto information server by steps including, for each requested data encryption key, sending the identifier of the requested data encryption key to the crypto information server.

More preferably still, the system also includes a database wherein the crypto information server stores the data encryption keys and the identifiers, most preferably in encrypted form.

Preferably, the set of data providers also generates a respective message authentication code key for each data instance, uses that message authentication code key to generate a respective message authentication code, and attaches the respective message authentication code key thus generated to the data instance prior to encrypting the data instance. Most preferably, the set of data providers generates the message authentication code keys according to a predefined key granularity. The system also includes a crypto information server that authenticates the data requestor and that, contingent on that authentication, sends the respective data encryption key and the respective message authentication code key of the requested data instance portion to the data requestor, most preferably in encrypted form.

Even more preferably, the set of data providers associates each data-encryption-key-message-authentication-code-key pair with a respective identifier, and the archive, in response to the request of the data instance portion by the data requestor, sends the respective identifier of the requested data instance portion to the data requestor along with the requested data instance portion. The data requestor then requests the respective data encryption key and the respective message authentication code key of the requested data instance portion from the crypto information server by sending the identifier of the requested data instance portion to the crypto information server.

Most preferably, each data provider, as well as the data requestor, includes a respective instance of a crypto information client that is operative to generate the data encryption keys, the message authentication code keys and the identifiers, to send the data encryption keys, the message authentication code keys and the identifiers to the crypto information server, and to request the data encryption keys and the message authentication code keys from the crypto information server by steps including, for each requested data-encryption-key-message-authentication-code-key pair, sending the identifier of the requested data-encryption-key-message-authentication-code-key pair to the crypto information server.

More preferably still, the system also includes a database wherein the crypto information server stores the data encryption keys, the message authentication code keys and the identifiers, most preferably in encrypted form.

Blair et al., in US Patent Application Publication No. 2006/0123106, teach a wiretapping device that is intended to be used by law enforcement officials to secretly record conversations legally even before such recording has been authorized by a judge. The device encrypts the conversations immediately upon intercept, using a password that is available to the law enforcement officials only from the judge, and stores the encrypted conversations. Without receiving the password from the judge, the recorded conversations are unintelligible to the law enforcement officials. Unlike the present invention, the device of Blair et al. lacks mandatory end-to-end encryption: having obtained the password, the law enforcement officials are free to decrypt the conversations in-place.

Coordinated Systems, Inc. of East Hartford CT, USA, offers a data logging and retrieval system called Virtual Observer that is similar to the logging system of the present system, insofar as Virtual Observer encrypts the data immediately on capture and conditions playback of archived data on authentication of the party requesting the playback. However, as far as the present inventors are aware, Virtual Observer sends unencrypted data to authenticated requesting parties and so lacks the end-to-end authentication of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is herein described, by way of example only, with reference to the accompanying drawings, wherein:

FIG. 1 is a high-level schematic block diagram of a prior art system for capturing, storing and retrieving telephone conversations;

FIG. 2 is a high-level schematic block diagram of the system of FIG. 1 as modified according to the present invention;

FIG. 3 is a high-level schematic block diagram of a logger of the system of FIG. 2;

FIG. 4 is a high-level schematic block diagram of a user terminal of the system of FIG. 2;

FIG. 5 illustrates the data flow in the system of FIG. 2;

FIG. 6 is a high-level schematic block diagram of a second system of the present invention;

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The principles and operation of a data collection and distribution system according to the present invention may be better understood with reference to the drawings and the accompanying description.

Referring again to the drawings, Figure 2 is a high-level schematic block diagram of a first system **30** of the present invention. Specifically, system **30** is system **10** of Figure 1 modified according to the principles of the present invention. System **30** inherits LAN **12**, archive **18**, Web server **20** and WAN **22** from system **10** substantially unchanged. The new components of system **30** include modified loggers **32**, modified user terminals **34**, a modified controller **36** and a key database **38**.

Figure 3 is a high-level schematic block diagram of a logger **32** of the system **30**, for logging multichannel audio input. Logger **32** includes an input interface **44** to the audio input, a digital signal processor (DSP) **48**, a controller **50**, a non-volatile memory **52** and an output interface **54** to LAN **12**. Depending on how interface **44** is configured, the audio input could be, for example, analog input, digital extension input, E1/T1 trunk input or VoIP input. Controller **50** is responsible for overall operation of logger **32**. One of the features of controller **50** that is relevant to the present invention is that controller **50**, with the help of an instance **56** of a crypto information client, as described below, attaches a message authentication code (MAC) to the compressed data that controller **50** receives from DSP **48** and then encrypts the compressed data together with the MAC. Controller **50** stores the

encrypted data in non-volatile memory **52** and retrieves the stored encrypted data from non-volatile memory **52**. Controller **50** also exchanges data with LAN **12** via interface **54**.

Figure 4 is a high-level schematic block diagram of a user terminal **34** of the present invention. Terminal **34** includes an interface **58** to LAN **12**, a controller **60**, a set of user output devices represented by a display block **62** and a set of user input devices represented by an input block **64**. The user input devices represented by input block **64** include standard input devices such as a keyboard and a mouse. The user output devices represented by display block **62** include standard output devices such as a video display screen, a speaker and a printer. Controller **60** is responsible for overall operation of terminal **34**. A user of terminal **34** uses input devices **64** to request data for display from web server **20**. The data are received via interface **58** and are displayed at one or more of output devices **62**. The data are exported in encrypted form, as described below; and one of the features of controller **60** that is relevant to the present invention is that controller **60**, with the help of an instance **66** of a crypto information client, as described below, decrypts the data for display and verifies that the data have not been altered subsequent to their encryption by their source logger **32**. Note that in the present context, "displaying" data means presenting the data to a user in a perceptible form: visually at a display screen, audibly via a speaker, etc.

The crypto information client of the present invention has several functions. One of these functions is the generation of the MAC keys that are used by controller **50** to generate MACs and of the data encryption keys that are used by controller **50** to encrypt data. Any conventional real-time symmetric encryption algorithm may be used, but the preferred algorithm is the AES algorithm. Preferably, each MAC key is 128 bits long and each data encryption key is 256 bits long. The data encryption keys and the MAC keys are generated according to a predefined key granularity, for example, per telephone conversation or periodically (*e.g.* daily or monthly), rather than according to a master key. For each file that controller **50** needs to encrypt, instance **56** of the crypto information client generates an associated MAC key, an associated symmetric data encryption key and a corresponding Global Unique Identifier (GUID). Periodically, for example at the end of a telephone conversation, controller **50** sends the accumulated files and the corresponding GUIDs from non-volatile memory **52** to archive **18** via LAN **12**. At the same time, controller **50** sends the associated MAC keys, the associated data encryption keys and the corresponding GUIDs to controller **36** via LAN **12**. Crypto information server **40** of controller **36** encrypts the MAC

keys and the data encryption keys for storage, along with the corresponding GUIDs, in database **38**.

The data that terminal **34** receives from Web server **20** are encrypted and so are useless unless terminal **34** can decrypt the data. Terminal **34** also needs to verify the authenticity of the data, to make sure that the data have not been modified subsequent to their encryption by logger **32**. Therefore, another function of the crypto information client of the present invention is fetching MAC keys and data encryption keys from database **38**. Terminal **34** receives data files from Web server **20** along with the corresponding GUIDs. For each data file that terminal **34** receives from Web server **20**, instance **56** of the crypto information client sends the corresponding GUID to controller **36** with a request for the associated MAC key and the associated data encryption key. Crypto information server **40** negotiates with instance **56** of the crypto information client to authorize the sending of the MAC key and the data encryption key to terminal **34**. If terminal **34** is authorized to receive the MAC key and the data encryption key, crypto information server **40** fetches the MAC key and the data encryption key from database **38** according to the GUID received from terminal **34**, decrypts the MAC key and the data encryption key and sends the MAC key and the data encryption key to the requesting terminal **34**.

Authentication methods suitable for use by crypto information server **40** and instance **56** of the crypto information client are well-known in the art and need not be elaborated herein. For example, in an Active Directory® environment, a protocol such as Kerberos or Integrated Windows Authentication (IWA) is used. In a non-Active-Directory environment, crypto information server **40** and instance **56** of the crypto information client authenticate each other by exchanging public key certificates. In either case, if the authentication is successful, crypto information server **40** sends the requested keys to terminal **34** in encrypted form, albeit encrypted differently than how the keys are stored in database **38**. For example, in a non-Active-Directory environment, crypto information server **40** uses a public key algorithm to encrypt the requested keys. After all, if a data encryption key were to be sent to terminal **34** in unencrypted form, an eavesdropper could use the data encryption key to decrypt the associated data file, thereby circumventing the present invention.

Note that the functionality of the crypto information client is different in terminal **34** than in logger **32**. In logger **32**, the crypto information client generates the keys and the GUIDs. In terminal **34**, the crypto information client uses the GUIDs to fetch the keys. It follows that loggers **32** and terminals **34** could be equipped with different clients. Preferably,

however, loggers **32** and terminals **34** use instances of the same crypto information client. This simplifies the design of the present system.

Figure 5 illustrates the data flow among crypto information server **40** and instances **56** and **66** of the crypto information client according to the present invention. Given a data file to encrypt, instance **56** generates a data encryption key **70** and a corresponding GUID **72**. Instance **56** also generates a MAC key **78** that is used to generate a MAC **76** that is embedded in the data file. Data encryption key **70** is used to encrypt the data, including embedded MAC **76**, thereby producing an encrypted data file **74**. File **74** and GUID **72** are stored in archive **18**. Data encryption key **70**, MAC key **78** and GUID **72** are sent to crypto information server **40** that stores data encryption key **70**, MAC key **78** and GUID **72** in database **38**. Upon receipt of encrypted data file **74** and GUID **72** from archive **18**, instance **66** sends GUID **72** to crypto information server **40** as part of a request for data encryption key **70**. If the request receives authorization, crypto information server **40** fetches data encryption key **70** and MAC key **78** from database **38** according to GUID **72** and sends data encryption key **66** and MAC **78** to instance **66**.

The description above of the operation of system **30** is in terms of a single logger **32** and a single user terminal **34**. As illustrated in Figure 2, system **30** almost always includes many loggers **32** and many user terminals **34**; but these loggers **32** and user terminals **34** typically operate independently of each other. Crypto information server **40** stores all the encryption keys **70** and all the associated GUIDs **72** in database **38** and sends encryption keys **70** to all terminals **34** contingent on those terminals **34** being authorized to receive encryption keys **70**.

Figure 6 is a high-level schematic block diagram of a second system **100** of the present invention. System **100** is based on the NICE Perform® system available from NICE Systems Ltd. of Raanana, Israel. Specifically, system **100** is a NICE Perform® system modified according to the principles of the present invention. Like a NICE perform® system, system **100** includes several multimedia loggers **104**, several user terminals **112**, a controller **106**, a storage center **108** and external storage **110**, all communicating with each other via a LAN **102**.

Loggers **104** capture whatever kind of multichannel data they are configured to capture: voice, VoIP, video and/or screen capture data. The captured data are stored in storage center **108** that functions in a manner similar to archive **18** of systems **10** and **30**. Each user terminal includes a screen agent **118** that sends screen capture data to an associated

logger **104** and a player application **120** for playing (*i.e.*, displaying) data fetched from storage center **108**. Overall control of system **100** is provided by controller **106** that includes a playback media server **114** that mediates between terminals **112** and their potential data sources (loggers **104** and storage center **108**) and an audio analysis server **116** that provides audio analysis capabilities such as speech recognition, excitement detection and talk analysis. Optionally, for efficient operation of storage center **108**, captured data also are archived in external storage **110**. The functionality listed in this paragraph is standard in NICE Perform® systems. More details may be found in the following three documents that are accessible to authorized distributors and customers of NICE Systems Ltd. at http://www.extranice.com:

NICE Perform™ Architecture Overview

NICE Perform™ Solution Overview

NICE Perform™ Solution Brief

To ensure that these three documents remain available for the full life of the patent that is expected to issue from the present patent application, all three documents are reproduced herein in their entirety, as Appendix.

In addition, loggers **104** include respective instances **124** of a crypto information client of the present invention, user terminals **112** include respective instances **126** of a crypto information client of the present invention and controller **106** includes a crypto information server **122** of the present invention. Crypto information client instances **124** generate data encryption keys and MAC keys for their respective loggers **104**. The data encryption keys are generated according to a predefined key granularity. A separate data encryption key and a separate MAC key, with the associated GUID, is generated for each external channel from which data are captured, as well as for each initialization of a screen agent **118**. Loggers **104** packetize the captured data, insert respective MACs in the media headers and encrypt the packets to provide encrypted data that are stored in storage center **108** along with associated GUIDs. Controller **106** stores the data encryption keys, the MAC keys and the associated GUIDs in a key database **128**. When a user of a user terminal **112** wants to play back stored data, the user fetches the data and its GUID from storage center **108**. The user then sends the GUID to controller **106** to request the associated keys. Crypto information client instance **126** of that user terminal **112** negotiates with crypto information server **122** as described above to authorize the sending of the keys to user terminal **112**.

While the invention has been described with respect to a limited number of embodiments, it will be appreciated that many variations, modifications and other applications of the invention may be made. For example, the data logging and data storing functionality of logger **32** can be partitioned between a telcom stage and a recorder stage, as taught in the Henits patent.

WHAT IS CLAIMED IS

1. A method of distributing data, comprising the steps of:

(a) encrypting the data, using a data encryption key, thereby providing encrypted data;

(b) requesting the data, by a data requestor;

(c) in response to said request, sending said encrypted data to said data requestor;

(d) authenticating said data requestor, by a crypto information server ; and

(e) contingent on said authenticating, sending said data encryption key to said data requestor, by said crypto information server .

2. The method of claim 1, wherein said data encryption key is a symmetric key.

3. The method of claim 1, wherein said data encryption key is sent to said data requestor in encrypted form.

4. The method of claim 1, further comprising the step of:

(f) requesting said data encryption key, by said data requestor, said authenticating being in response to said requesting of said data encryption key.

5. The method of claim 1, further comprising the steps of:

(f) generating said data encryption key; and

(g) associating said data encryption key with a respective identifier.

6. The method of claim 5, wherein said data encryption key is generated according to a predefined key granularity.

7. The method of claim 5, wherein said identifier is sent to said data requestor along with said encrypted data, the method further comprising the step of:

(h) sending said identifier to said crypto information server, by said data requestor, to request said data encryption key, said authenticating being in response to receipt of said identifier from said data requestor by said crypto information server .

8. The method of claim 5, further comprising the step of:

(h) storing said data encryption key and said identifier in a database, by said crypto information server .

9. The method of claim 8, wherein said data encryption key is stored in said database in encrypted form.

10. The method of claim 1, wherein the data are encrypted by a data provider, the method further comprising the step of:

(f) storing said encrypted data in an archive separate from said data provider, said encrypted data being sent to said data requestor from said archive.

11. The method of claim 1, further comprising the steps of:

(f) attaching a message authentication code to the data prior to said encrypting; and

(g) contingent on said authenticating, sending a message authentication code key of said message authentication code to said data requestor, by said crypto information server.

12. The method of claim 11, further comprising the steps of:

(h) generating said data encryption key and said message authentication code key; and

(i) associating said data encryption key and said message authentication code key with a common respective identifier.

13. The method of claim 12, wherein said data encryption key and said message authentication code key are generated according to a predefined key granularity.

14. The method of claim 12, wherein said identifier is sent to said data requestor along with said encrypted data, the method further comprising the step of:

(j) sending said identifier to said crypto information server, by said data requestor, to request said data encryption key and said message authentication code key, said authenticating being in response to receipt of said identifier from said data requestor by said crypto information server.

15. The method of claim 12, further comprising the step of:

(j) storing said data encryption key and said message authentication code key in a database, by said crypto information server.

16. The method of claim 15, wherein said data encryption key and said message authentication code key are stored in said database in encrypted form.

17. A system for secure distribution of data, comprising:

(a) a data requestor;

(b) a data provider operative:

(i) to encrypt the data using a data encryption key, thereby providing encrypted data, and

(ii) to send said encrypted data to said data requestor; and

(c) a crypto information server operative:

(i) to authenticate said data requestor, and

(ii) contingent on said authentication, to send said data encryption key to said data requestor.

18. The system of claim 17, wherein said crypto information server is operative to send said data encryption key to said data requestor in encrypted form.

19. The system of claim 17, wherein said data provider also is operative:

(iii) to generate said data encryption key; and

(iv) to associate said data encryption key with a respective identifier.

20. The system of claim 19, wherein said data provider is operative to generate said data encryption key according to a predefined key granularity.

21. The system of claim 19, wherein said data provider also is operative:

(v) to send said identifier to said data requestor along with said encrypted data; and

(vi) to send said data encryption key and said identifier to said crypto information server ;

wherein said data requestor is operative to request said data encryption key from said crypto information server by steps including sending said identifier to said crypto information server, said authenticating being in response to receipt of said identifier from said data requestor by said crypto information server .

22. The system of claim 21, wherein each of said data provider and said data requestor includes a respective instance of a crypto information client that is operative:

(i) to generate said data encryption key;

(ii) to generate said respective identifier;

(iii) to send said data encryption key and said identifier to said crypto information server; and

(iv) to request said data encryption key from said crypto information server by steps including sending said identifier to said crypto information server.

23. The system of claim 21, further comprising:

(d) a database wherein said crypto information server stores said data encryption key and said identifier.

24. The system of claim 23, wherein said crypto information server stores said data encryption key in said database in encrypted form.

25. The system of claim 17, further comprising:

(d) an archive, separate from said data provider, for storing said encrypted data.

26. The system of claim 25, wherein said archive is operative to send said encrypted data to said data requestor.

27. The system of claim 17, wherein said data provider also is operative:

(iii) to attach a message authentication code to the data prior to encrypting the data;

and wherein said crypto information server also is operative:

(iii) contingent on said authenticating, to send a message authentication code key of said message authentication code to said data requestor.

28. The system of claim 27, wherein said data provider also is operative:

(iv) to generate said data encryption key and said message authentication code key; and

(v) to associate said data encryption key and said message authentication code key with a common respective identifier.

29. The system of claim 28, wherein said data provider is operative to generate said data encryption key and said message authentication key according to a predefined key granularity.

30. The system of claim 28, wherein said data provider also is operative:

(vi) to send said identifier to said data requestor along with said encrypted data; and

(vii) to send said data encryption key, said message authentication code key and said identifier to said crypto information server;

wherein said data requestor is operative to request said data encryption key and said message authentication code key from said crypto information server by steps including sending said identifier to said crypto information server, said authenticating being in response to receipt of said identifier from said data requestor by said crypto information server.

31. The system of claim 30, wherein each of said data provider and said data requestor includes a respective instance of a crypto information client that is operative:

(i) to generate said data encryption key;

(ii) to generate said message authentication code key;

(iii) to generate said respective common identifier;

(iv) to send said data encryption key, said message authentication code key and said identifier to said crypto information server; and

(v) to request said data encryption key and said message authentication code key from said crypto information server by steps including sending said identifier to said crypto information server.

32. The system of claim 30, further comprising:

(d) a database wherein said crypto information server stores said data encryption key, said message authentication code key and said identifier.

33. The system of claim 32, wherein said crypto information server stores said data encryption key and said message authentication code key in said database in encrypted form.

34. A method of collecting and distributing a plurality of instances of data, comprising the steps of:

(a) for each instance:

(i) generating a respective data encryption key, and

(ii) encrypting said each instance, using said respective data encryption key, thereby providing respective encrypted data;

(b) requesting at least a portion of one of the instances, by a data requestor; and

(c) in response to said request, sending a corresponding portion of said respective encrypted data of said one instance to said data requestor.

35. The method of claim 34, wherein said one instance includes voice data.

36. The method of claim 34, wherein said one instance includes VoIP data.

37. The method of claim 34, wherein said one instance includes video data.

38. The method of claim 34, wherein said one instance includes screen capture data.

39. The method of claim 34, wherein said data encryption keys are symmetric keys.

40. The method of claim 34, wherein said data encryption keys are generated according to a predefined key granularity.

41. The method of claim 34, further comprising the step of:

(d) for each instance: capturing said instance, by a respective data provider, said generating of said respective data encryption key and said encrypting of said each instance being effected by said respective data provider.

42. The method of claim 41, further comprising the step of:

(e) for each instance, storing said encrypted data in an archive separate from said respective data provider, said respective encrypted data being sent to said data requestor from said archive.

43. The method of claim 34, further comprising the step of:

(d) for said one instance:

(i) authenticating said data requestor, by a crypto information server; and

(ii) contingent on said authenticating, sending said respective data encryption key of said one instance to said data requestor, by said crypto information server.

44. The method of claim 43, wherein said respective data encryption key of said one instance is sent to said data requestor in encrypted form.

45. The method of claim 43, further comprising the step of:

(e) for said one instance: requesting said respective data encryption key, by said data requestor, said authenticating being in response to said requesting of said respective data encryption key.

46. The method of claim 45, further comprising the step of:

(f) for each instance, associating said respective data encryption key with a respective identifier.

47. The method of claim 46, further comprising the step of:

(g) for said one instance: sending said respective identifier of said one instance to said data requestor along with said respective encrypted data of said one instance, said requesting of said respective data encryption key by said data requestor then including sending said respective identifier of said one instance to said crypto information server.

48. The method of claim 46, further comprising the step of:

(g) for each instance, storing said respective data encryption key and said respective identifier in a database, by said crypto information server.

49. The method of claim 48, wherein said data encryption keys are stored in said database in encrypted form.

50. The method of claim 43, further comprising the steps of:

(d) for each instance, attaching a respective message authentication code to said each instance prior to said encrypting; and

(e) for said one instance:

(i) authenticating said data requestor by a crypto information server; and

(ii) contingent on said authenticating, sending said respective data encryption key of said one instance and a message authentication code key of said respective message authentication code of said one instance to said data requestor, by said crypto information server.

51. The method of claim 50, further comprising the step of:

(f) for each instance:

(i) generating a respective message authentication code key; and

(ii) generating said respective message authentication code, using said respective message authentication code key.

52. The method of claim 51, wherein said message authentication code keys are generated according to a predefined key granularity.

53. The method of claim 50, wherein said respective data encryption key and said respective message authentication code key of said one instance are sent to said data requestor in encrypted form.

54. The method of claim 50, further comprising the step of:

(f) for said one instance: requesting said respective data encryption key and said respective message authentication code key, by said data requestor, said authenticating being in response to said requesting of said respective data encryption key and said respective message authentication code key.

55. The method of claim 54, further comprising the step of:

(g) for each instance, associating said respective data encryption key and said respective message authentication code key with a common respective identifier.

56. The method of claim 55, further comprising the step of:

(h) for said one instance: sending said respective identifier of said one instance to said data requestor along with said respective encrypted data of said one instance, said requesting of said respective data encryption key and said respective message authentication code key by said data requestor then including sending said respective identifier of said one instance to said crypto information server.

57. The method of claim 55, further comprising the step of:

(h) for each instance, storing said respective data encryption key, said respective message authentication code key and said respective identifier in a database, by said crypto information server.

58. The method of claim 57, wherein said data encryption keys and said message authentication code keys are stored in said database in encrypted form.

59. A system for secure collection and distribution of a plurality of instances of data, comprising:

(a) a set, of at least one data provider, operative:

(i) to capture said instances, and

(ii) for each instance:

(A) to generate a respective data encryption key, and

(B) to encrypt said each instance, using said respective data encryption key, thereby providing respective encrypted data;

(b) a data requestor operative:

(i) to request at least a portion of one of the instances; and

(c) an archive operative:

(i) to store said encrypted data; and

(ii) in response to said request of said at least portion of said one instance by said data requestor: to send a corresponding portion of said respective encrypted data of said one instance to said data requestor.

60. The system of claim 59, wherein said archive is separate from said set of at least one data provider.

61. The system of claim 59, wherein said set of said at least one data provider is operative to generate said data encryption keys according to a predefined key granularity.

62. The system of claim 59, further comprising:

(d) a crypto information server, operative:

(i) to authenticate said data requestor; and

(ii) contingent on said authentication, to send said respective data encryption key of said one instance to said data requestor.

63. The system of claim 62, wherein said crypto information server is operative to send said data encryption key to said data requestor in encrypted form.

64. The system of claim 62, wherein said data requestor also is operative:

(ii) to request said respective data encryption key of said one instance from said crypto information server, said authenticating being in response to said requesting of said respective data encryption key.

65. The system of claim 64, wherein said set of said at least one data provider also is operative, for each instance:

(C) to associate said respective data encryption key with a respective identifier;

wherein said archive also is operative:

(iii) in response to said request of said at least portion of said one instance by said data requestor: to send said respective identifier of said one instance to said data requestor;

and wherein said data requestor requests said respective data encryption key of said one instance from said crypto information server by steps including sending said respective identifier of said one instance to said crypto information server.

66. The system of claim 65, wherein each of said at least one data provider and said data requestor includes a respective instance of a crypto information client that is operative:

(i) to generate said data encryption keys and said identifiers;

(ii) to send said data encryption keys and said identifiers to said crypto information server; and

(iii) to request said data encryption keys from said crypto information server by steps including, for each requested said data encryption key, sending said identifier thereof to said crypto information server.

67. The system of claim 65, further comprising:

(e) a database, wherein said crypto information server stores said data encryption keys and said identifiers.

68. The system of claim 67, wherein said crypto information server stores said data encryption keys and said identifiers in said database in encrypted form.

69. The system of claim 59, wherein said set of said at least one data provider also is operative, for each instance:

(C) to generate a respective message authentication code key;

(D) to generate a respective message authentication code, using said respective message authentication code key; and

(E) to attach said respective message authentication code to said each instance prior to encrypting said each instance;

and wherein the system further comprises:

(d) a crypto information server, operative:

(i) to authenticate said data requestor; and

(ii) contingent on said authentication, to send said respective data encryption key and said respective message authentication code key of said one instance to said data requestor.

70. The system of claim 69, wherein said set of said at least one data provider is operative to generate said message authentication code keys according to a predefined key granularity.

71. The system of claim 69, wherein said crypto information server is operative to send said respective data encryption key and said respective message authentication code key of said one instance to said data requestor in encrypted form.

72. The system of claim 69, wherein said set of said at least one data provider also is operative, for each instance:

(F) to associate said respective data encryption key and said respective message authentication code key with a common respective identifier;

wherein said archive also is operative:

(iii) in response to said request of said at least portion of said one instance by said data requestor: to send said respective identifier of said one instance to said data requestor;

and wherein said data requestor requests said respective data encryption key and said respective message authentication code key of said one instance from said crypto information server by steps including sending said respective identifier of said one instance to said crypto information server.

73. The system of claim 72, wherein each of said at least one data provider and said data requestor includes a respective instance of a crypto information client that is operative:

(i) to generate said data encryption keys, said message authentication code keys and said identifiers;

(ii) to send said data encryption keys, said message authentication code keys and said identifiers to said crypto information server; and

(iii) to request said data encryption keys and said message authentication code keys from said crypto information server by steps including, for each requested said data encryption key and for each requested said message authentication code key, sending said identifier thereof to said crypto information server.

74. The system of claim 72, further comprising:

(e) a database, wherein said crypto information server stores said data encryption keys, said message authentication code keys and said identifiers.

75. The system of claim 74, wherein said crypto information server stores said data encryption keys, said message authentication code keys and said identifiers in said database in encrypted form.

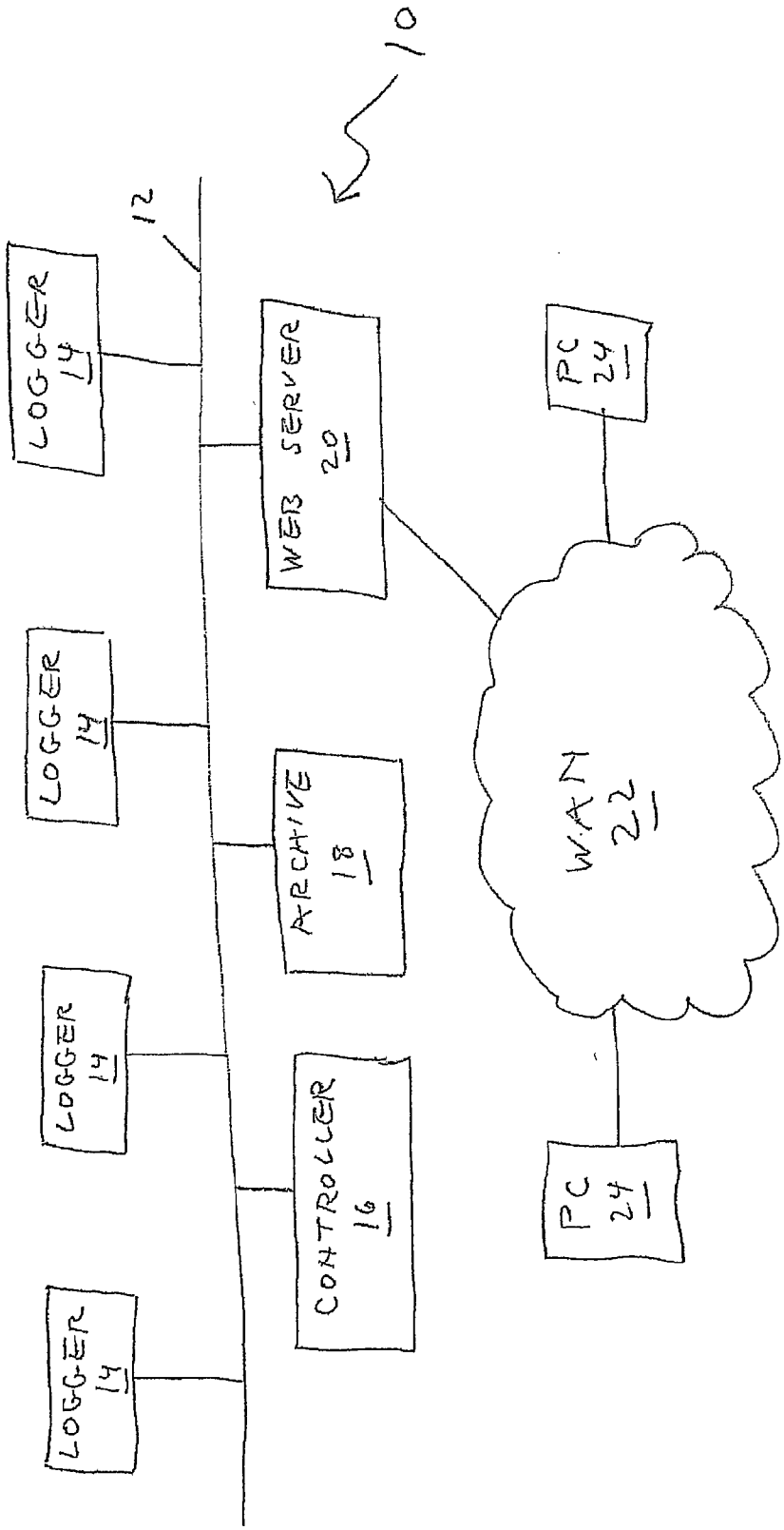


FIGURE 1 (PRIOR ART)

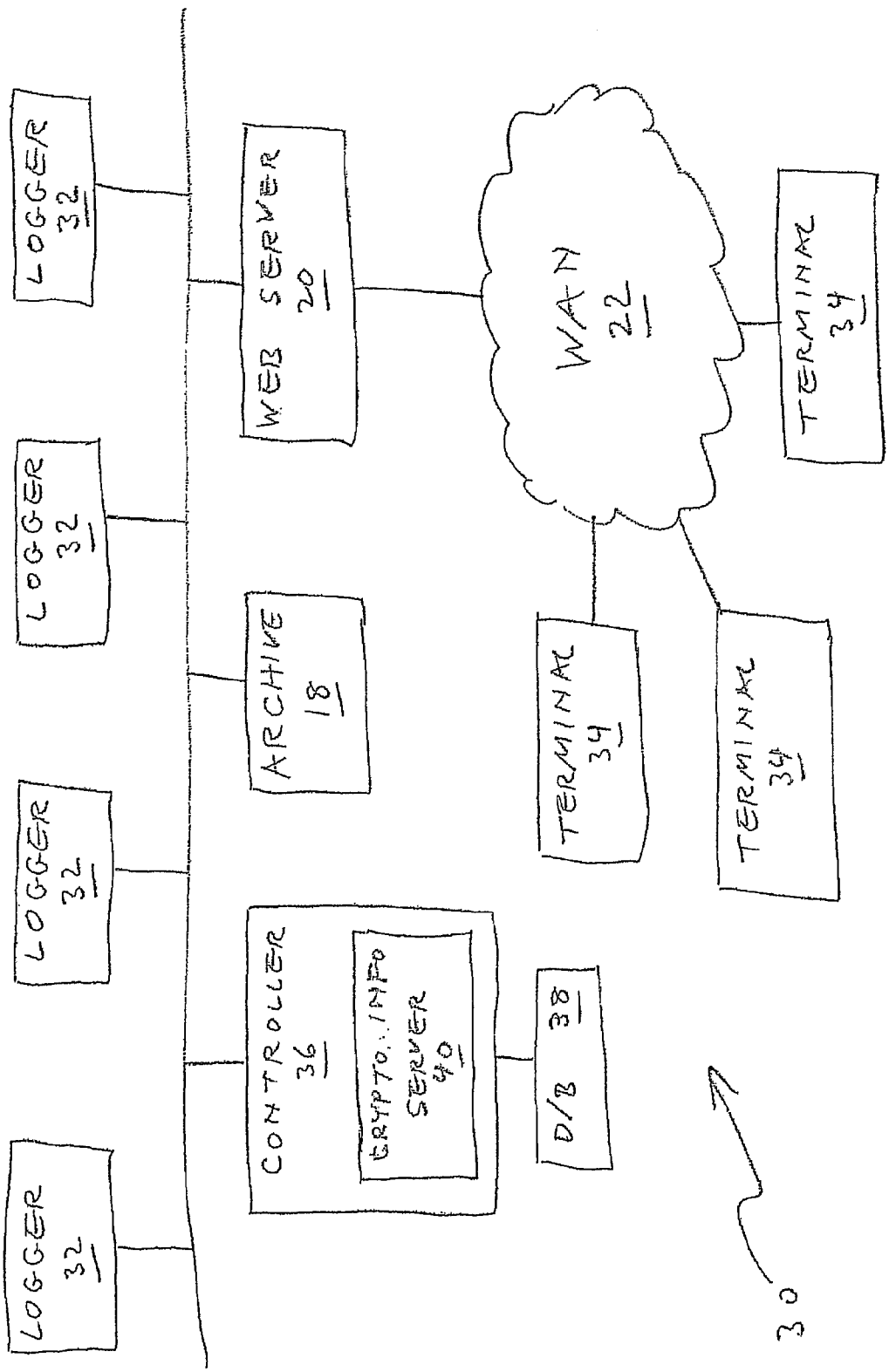

LOGGER
32
LOGGER
32
LOGGER
32
LOGGER
32
WEB SERVER
20
ARCHIVE
18
CONTROLLER
36
CRYPTO. INFO
SERVER
40
D/B 38
WAN
22
TERMINAL
34
TERMINAL
34
TERMINAL
34
30

FIGURE 2

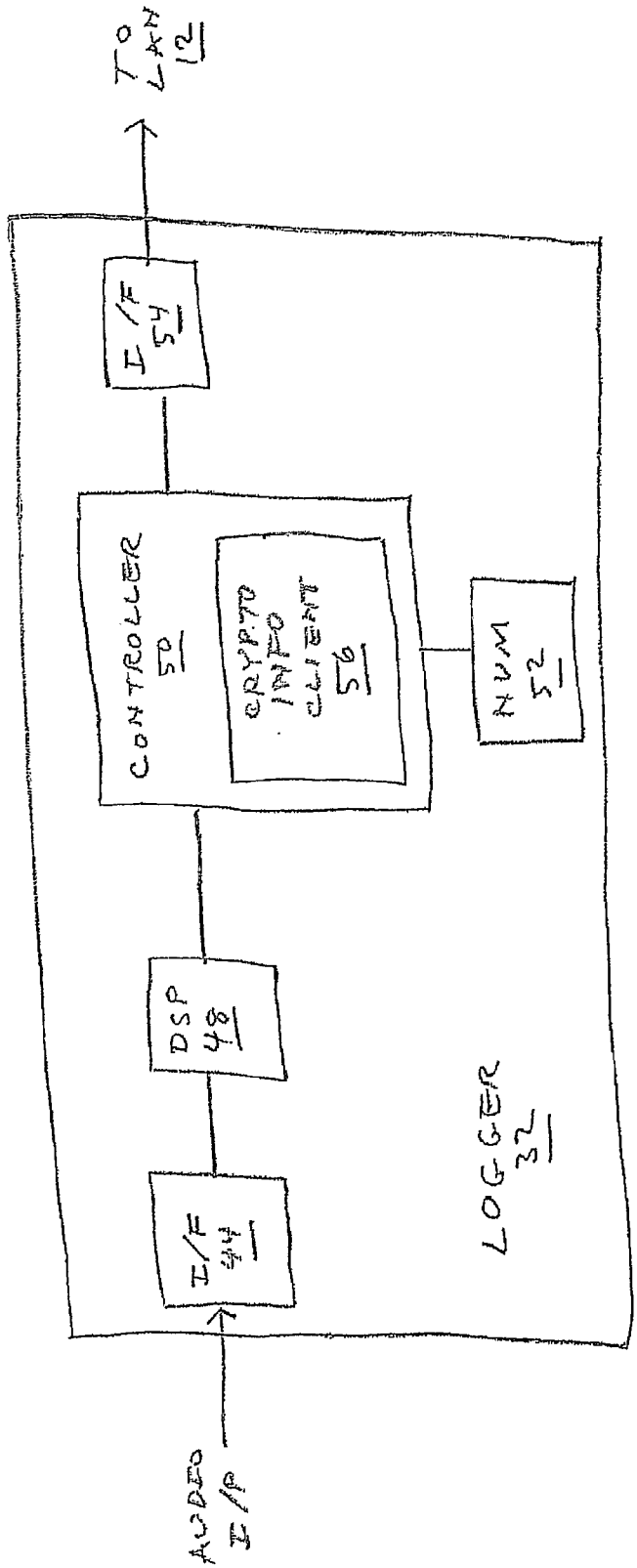

TO LAN 12
I/F 54
CONTROLLER 50
CRYPTO INFO CONTENT 56
NVM 52
DSP 48
I/F 44
LOGGER 32
AUDIO I/P

FIGURE 3

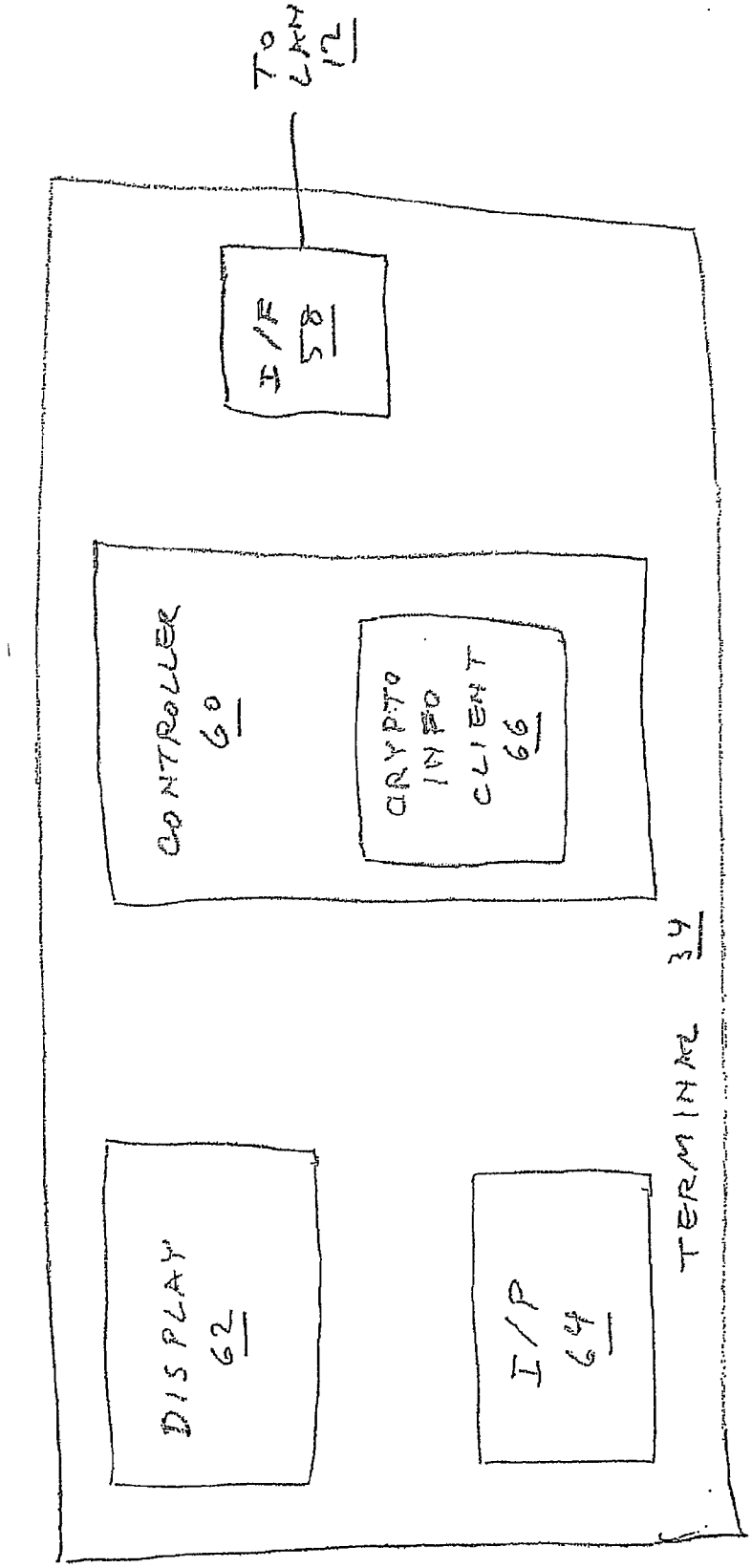

TO LAN 12
I/F 58
CONTROLLER 60
CRYPTO INFO CLIENT 66
DISPLAY 62
I/P 64
TERMINAL 34

FIGURE 4

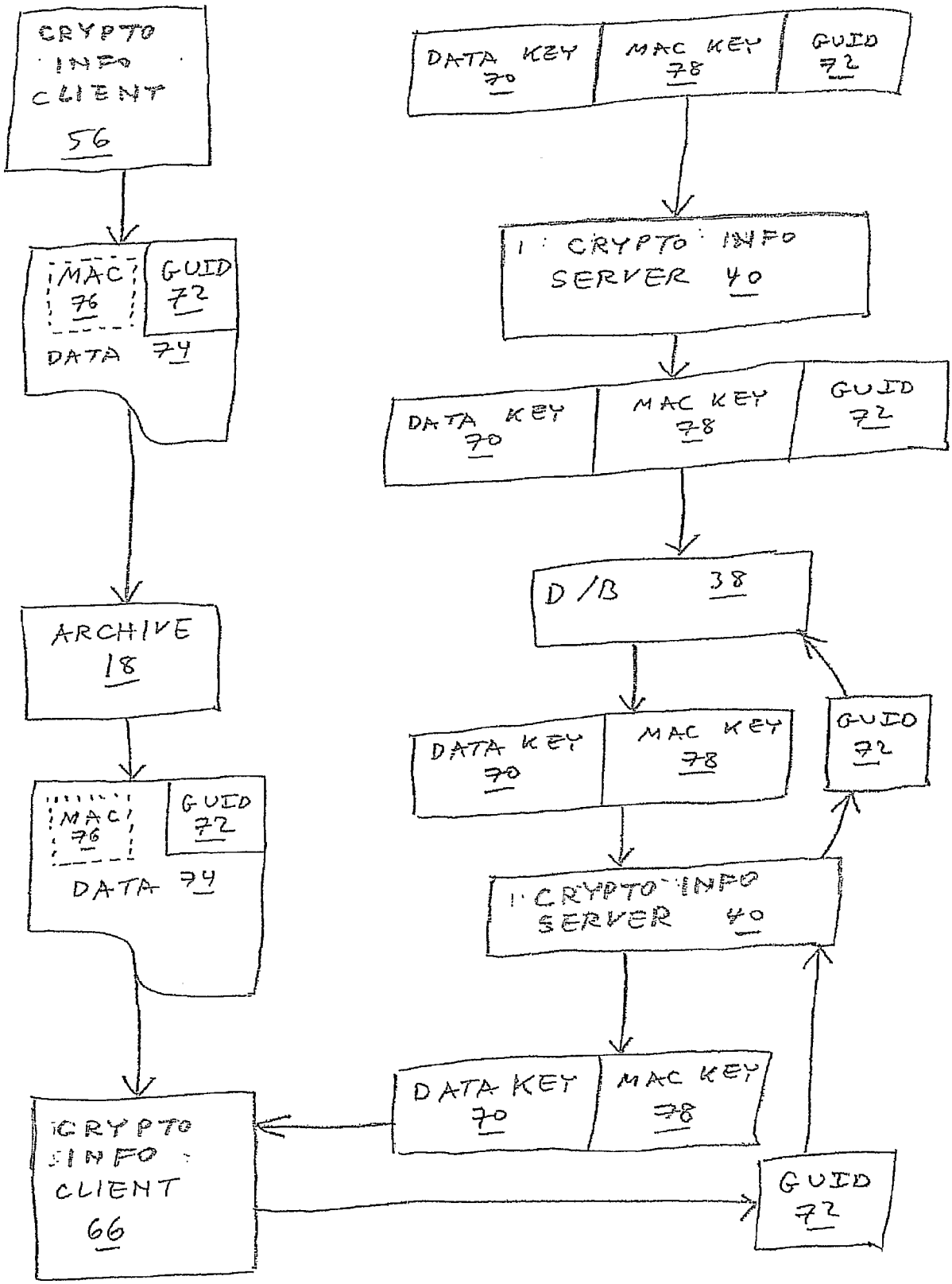

CRYPTO INFO CLIENT 56
MAC 76
GUID 72
DATA 74
ARCHIVE 18
MAC 76
GUID 72
DATA 74
CRYPTO INFO CLIENT 66
DATA KEY 70
MAC KEY 78
GUID 72
CRYPTO INFO SERVER 40
DATA KEY 70
MAC KEY 78
GUID 72
D/B 38
DATA KEY 70
MAC KEY 78
GUID 72
CRYPTO INFO SERVER 40
DATA KEY 70
MAC KEY 78
GUID 72

FIGURE 5

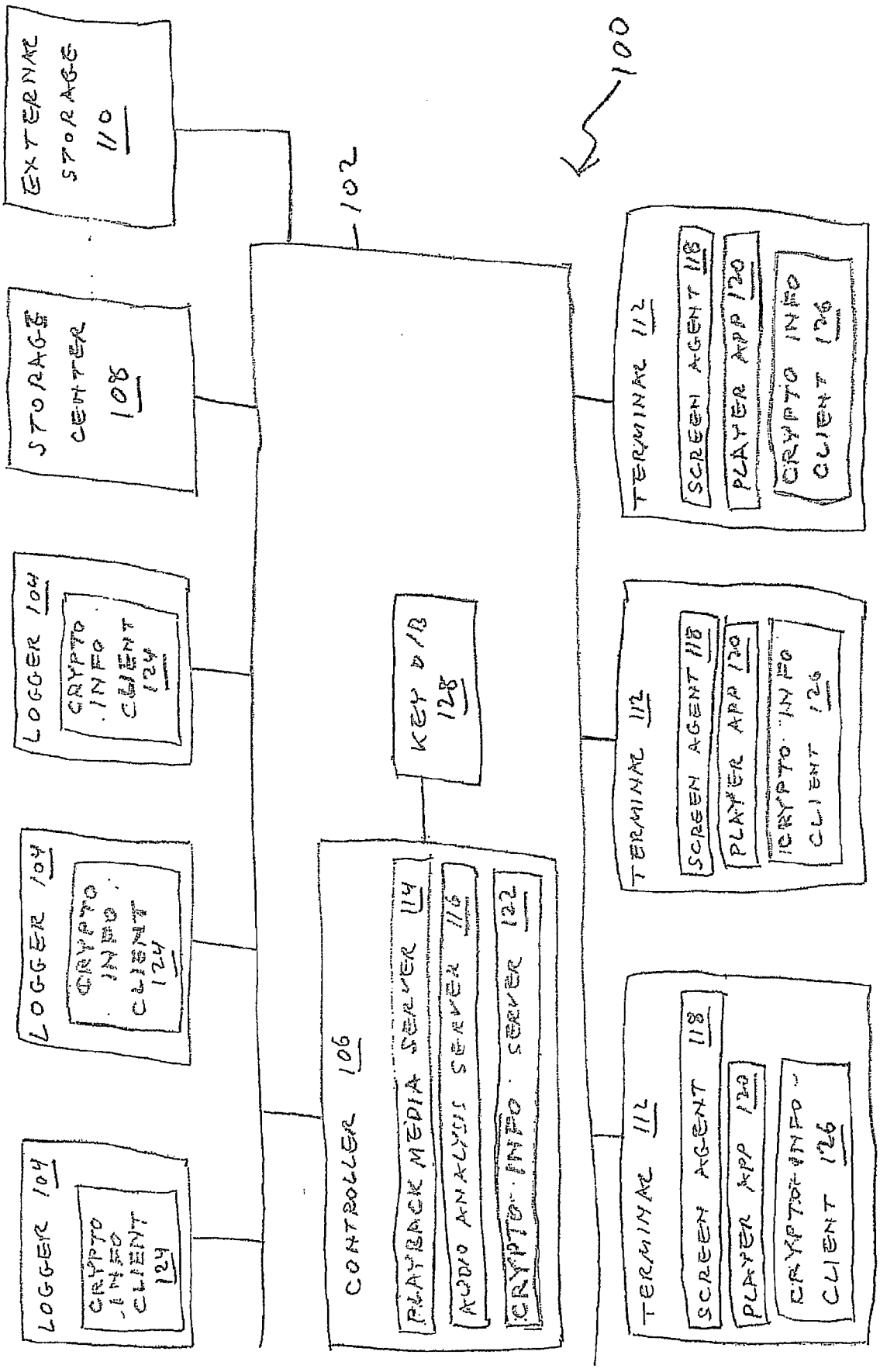

EXTERNAL STORAGE 110
100
102
STORAGE CENTER 108
LOGGER 104
CRYPTO INFO CLIENT 124
LOGGER 104
CRYPTO INFO CLIENT 124
LOGGER 104
CRYPTO INFO CLIENT 124
KEY DB 128
CONTROLLER 106
PLAYBACK MEDIA SERVER 114
AUDIO ANALYSIS SERVER 116
CRYPTO INFO SERVER 122
TERMINAL 112
SCREEN AGENT 118
PLAYER APP 120
CRYPTO INFO CLIENT 126
TERMINAL 112
SCREEN AGENT 118
PLAYER APP 120
CRYPTO INFO CLIENT 126
TERMINAL 112
SCREEN AGENT 118
PLAYER APP 120
CRYPTO INFO CLIENT 126

FIGURE 6