

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
12 February 2009 (12.02.2009)

PCT

(10) International Publication Number
WO 2009/020657 A1

(51) **International Patent Classification:**
H04J 3/16 (2006.01) *H04J 3/22* (2006.01)

(21) **International Application Number:**
PCT/US2008/009557

(22) **International Filing Date:** 8 August 2008 (08.08.2008)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
60/954,660 8 August 2007 (08.08.2007) US

(71) **Applicant and**

(72) **Inventor:** KERNENE, Nicolas [US/US]; 38 W. 315 Heritage Oaks Drive, St. Charles, IL 60175 (US).

(74) **Agents:** BARKAUS, Keith, J. et al.; Ostrolenk, Faber, Gerb & Soffen LLP, 1180 Avenue of the Americas, New York, NY 10036 (US).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, 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, ST, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, 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:
— with international search report

(54) **Title:** SYSTEM AND METHOD FOR SECURELY TRANSMITTING DATA USING VIDEO VALIDATION

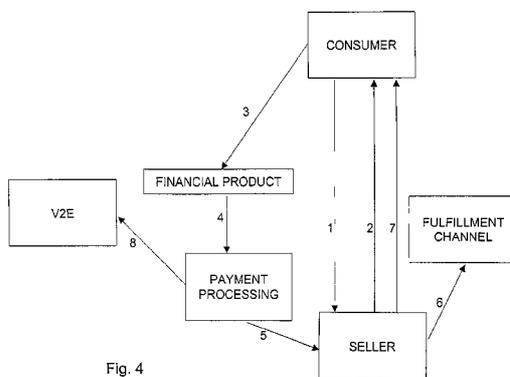


Fig. 4

(57) **Abstract:** A system and method is disclosed for secure transmission of electronic information between two parties. A first data communication session between a first computing device and a second computing device, wherein the first data communication session is via a first communication protocol. Further, the first computing device transmits first information via the first communication protocol that is received by the second computing device via the first communication protocol. During the first communication session, a second data communication session is provided between the first computing device and the second computing device. The second communication session is via a second communication protocol, which is more secure than the first communication protocol. The first computing device transmits second information via the second communication protocol that is received by the second computing device the second information via the second communication protocol. The second information relates at least partially to the first information. Moreover, the second communication session appears to a user of the first computing device to be the first communication session.



WO 2009/020657 A1

- 1 -

SYSTEM AND METHOD FOR SECURELY
TRANSMITTING DATA USING VIDEO VALIDATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is based on and claims priority to U.S. Provisional Patent Application Serial No. 60/954,660, filed on August 8, 2007, and entitled SYSTEM AND METHOD FOR SECURELY TRANSMITTING DATA USING VIDEO VALIDATION, which refers to and is partially based upon U.S. Patent Application Serial No. 11/757,953, filed on June 4, 2007, and entitled BROADBAND GAMING SYSTEM AND METHOD, the entire contents of which are incorporated herein by reference.

BACKGROUND

Field of the Invention

[0002] The present invention relates to middleware technology, and, more particularly, to security and validation with respect to remote user interactions.

Description of the Related Art

[0003] In the prior art, sensitive data, such as provided in a typical e-commerce application, are not securely isolated from the internet and from potential harm and/or abuse. Although prior art data security measures make a hacker's job difficult, access to sensitive data unfortunately remains possible in the prior art. Further, a repetitive cycle has emerged in the prior art as hackers overcome security measures, new security measures are installed, and hackers overcome the new measures, only for yet newer measures to be installed. Accordingly, continuous maintenance and updates are required,

and yet sensitive data such as related to e-commerce applications are not secure over time. It is believed that tens of billions of dollars are lost to data security-related issues.

[0004] Privacy and security remain important components of industry growth for e-retailers and their customers. Despite the significant market growth, consumers remain apprehensive about using a debit card or credit card to order goods on-line. A lack of consumer confidence combined with estimates of loss attributed to privacy and security fraud results in a setback for the industry. Furthermore, although the financial industry continues to benefit from robust online banking transactions, an impact is felt that is due to revenue loss and an erosion of consumer confidence from ineffective security measures that continue to allow fraud and piracy.

[0005] Further, fraud and security breach losses are not just a part of big business; they are big barriers to business. Businesses, manufacturers, trade and consumer associations and governments worldwide spend millions of dollars publicizing, packaging and advertising whenever they add new security measures or enact new safety, privacy and anti-fraud standards. Businesses must regularly invest in the reliability and the security of their e-commerce, data sharing, and payment methods, in part to persuade their customers that critical data are kept safe.

SUMMARY

[0006] The process described herein addresses these failures by employing improved security measures in connection with remote communications.

[0007] Accordingly, a system and method is disclosed for secure transmission of electronic information between two parties. A first data communication session between a first computing device and a second computing device, wherein the first data communication session is via a first communication protocol. Further, the first computing device transmits first information via the first communication protocol that is received by the second computing device via the first communication protocol. During the first communication session, a second data communication session is provided

between the first computing device and the second computing device. The second communication session is via a second communication protocol, which is more secure than the first communication protocol. The first computing device transmits second information via the second communication protocol that is received by the second computing device the second information via the second communication protocol. The second information relates at least partially to the first information. Moreover, the second communication session appears to a user of the first computing device to be the first communication session.

[0008] Other features and advantages of the present invention will become apparent from the following description of the invention that refers to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] For the purpose of illustration, there is shown in the drawings a form which is presently preferred, it being understood, however, that the invention is not limited to the precise arrangements and instrumentalities shown. The features and advantages of the descriptions herein will become apparent from the following description that refers to the accompanying drawing, in which:

[0010] Fig. 1 is a diagram of an example hardware arrangement that operates for control allocation of assets and rights, constructed in accordance with a preferred embodiment;

[0011] Fig. 2 is a block diagram illustrating functional elements of an information processor or user terminal in accordance with a preferred embodiment;

[0012] Fig. 3 illustrates an embodiment of an example arrangement including an example flow of information and order of operation in accordance with an embodiment; and

[0013] Fig. 4 illustrates an embodiment of an example arrangement and flow of information in accordance with an embodiment.

DESCRIPTION OF EMBODIMENTS

[0014] In accordance with the teachings herein, a new way to transmit data securely, such as to complete financial transactions, over the internet is provided without the transmission of any private data through the internet.

[0015] Information may be sent or received via an internet web sites comprising a related set of files which are maintained in one or more computer systems (e.g., web servers) and which, when transmitted to a user terminal, cause a user terminal to display and/or execute programmatic operations corresponding to the data contained in the files. Typically, the files comprising the web site are prepared using one or more of a combination of Hypertext Mark-Up Language (HTML), Extensible Mark-Up Language (XML), Java Applets, ActiveX programs, Standard Generalized Mark-Up Language (SGML) files and the like. Web site files are typically transmitted to a user terminal using one or more protocols, such as the Hypertext Transfer Protocol (HTTP) under the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of communication protocols.

[0016] Moreover, interactive video techniques are preferably implemented such that interactive data entry forms are provided via video in lieu of or in addition to data entry forms provided using HTTP and, for example, in HTML.

[0017] Also as used herein, the term, "browser" refers to an application program residing and executing on a user terminal which functions as an HTTP client, sending requests to web servers for web site files. A request is typically sent in the form of a Uniform Resource Locator (URL) or by selecting a hypertext link presented on the user terminal display. The browser functions to format the file and/or data received from the web server and format the received files and/or data in the manner described therein, displaying the same on the user terminal. Examples of browser programs include MICROSOFT INTERNET EXPLORER and NETSCAPE NAVIGATOR.

[0018] As used herein, the term, "module," refers, generally, to one or more discrete components that contribute to the effectiveness of the present invention. Modules can include software elements, including but not limited to functions, algorithms, classes and the like. Modules also include hardware elements, substantially as described below. Modules can operate independently or, alternatively, depend upon one or more other modules in order to function.

[0019] Referring now to the drawings figures in which like reference numerals refer to like elements, there is shown in Fig. 1 a diagram of an example hardware arrangement in accordance with the teachings herein, and designated generally as system 100. System 100 is preferably comprised of one or more information processors 102 coupled to one or more user terminals 104 across communication network 106. Further, printed output is provided, for example, via output printers 110.

[0020] Information processor 102 preferably includes all necessary databases for the present invention. However, it is contemplated that information processor 102 can access any required databases via communication network 106 or any other communication network to which information processor 102 has access. Information processor 102 can communicate devices comprising databases using any known communication method, including a direct serial, parallel, USB interface, or via a local or wide area network.

[0021] User terminals 104 communicate with information processors 102 using data connections 108, which are respectively coupled to communication network 106. Communication network 106 can be any communication network, but is typically the Internet or some other global computer network. Data connections 108 can be any known arrangement for accessing communication network 106, such as dial-up serial line interface protocol/point-to-point protocol (SLIPP/PPP), integrated services digital network (ISDN), dedicated leased-line service, broadband (cable) access, frame relay, digital subscriber line (DSL), asynchronous transfer mode (ATM) or other access techniques.

[0022] User terminals 104 are preferably coupled to or operate in conjunction with a set top box 105, such as a custom configured television set top box. Initially, the user connects to a web site via user terminal 104 and an HTTP connection. Thereafter, when the user desires to transmit sensitive or private data, such as to pay for a good in an e-commerce web site, the user communicates via interactive video in a session that preferably operates concurrently with the HTTP session. The interactive video session is preferably routed securely through a middleware platform, described in greater in co-pending and U.S. Patent Application No. 11/757,953 (incorporated herein by reference) and via set top box 105.

[0023] User terminals 104 preferably have the ability to send and receive data across communication network 106, and are equipped with web browsers to display the received data on display devices incorporated therewith. By way of example, user terminal 104 may be personal computers such as Intel Pentium-class computers or Apple Macintosh computers, but are not limited to such computers. Other terminals which can communicate over a global computer network such as palmtop computers, personal digital assistants (PDAs) and mass-marketed Internet access devices such as WebTV can be used. In addition, the hardware arrangement of the present invention is not limited to devices that are physically wired to communication network 106. Of course, one skilled in the art will recognize that wireless devices can communicate with information processors 102 using wireless data communication connections (e.g., WIFI).

[0024] Referring now to Fig. 2 the functional elements of each information processor 102 or user terminal 104 preferably include one or more central processing units (CPU) 202 used to execute software code in order to control the operation of information processor 102, read only memory (ROM) 204, random access memory (RAM) 206, one or more network interfaces 208 to transmit and receive data to and from other computing devices across a communication network, storage devices 210 such as a hard disk drive, floppy disk drive, tape drive, CD-ROM or DVD drive for storing program code, databases and application code, one or more input devices 212 such as a keyboard, mouse, track ball and the like, and a display 214.

[0025] The various components of information processor 102 need not be physically contained within the same chassis or even located in a single location. For example, as explained above with respect to databases which can reside on storage device 210, storage device 210 may be located at a site which is remote from the remaining elements of information processors 102, and may even be connected to CPU 202 across communication network 106 via network interface 208.

[0026] The functional elements shown in Fig. 2 (designated by reference numbers 202-214) are preferably the same categories of functional elements preferably present in user terminal 104. However, not all elements need be present, for example, storage devices in the case of PDAs, and the capacities of the various elements are arranged to accommodate expected user demand. For example, CPU 202 in user terminal 104 may be of a smaller capacity than CPU 202 as present in information processor 102. Similarly, it is likely that information processor 102 will include storage devices 210 of a much higher capacity than storage devices 210 present in work station 104. Of course, one of ordinary skill in the art will understand that the capacities of the functional elements can be adjusted as needed.

[0027] The nature of the present invention is such that one skilled in the art of writing computer executed code (software) can implement the described functions using one or more or a combination of a popular computer programming language including but not limited to C++, VISUAL BASIC, JAVA, ACTIVEX, HTML, XML, ASP, SOAP, DOCSIS (Data Over Cable Service Interface Specifications), OCAP (Open Cable Application Platform), and web application development environments.

[0028] As used herein, references to displaying data on user terminal 104 refer to the process of communicating data to the terminal across communication network 106 and processing the data such that the data can be viewed on the user terminal 104, via display 214 using a web browser or the like. The display screens on user terminal 104 present areas within system 100 such that a user can proceed from area to area within the system 100 by selecting a desired link. Therefore, each user's experience with system 100 will

be based on the order with which (s)he progresses through the display screens. In other words, because the system is not completely hierarchical in its arrangement of display screens, users can proceed from area to area without the need to "backtrack" through a series of display screens. For that reason and unless stated otherwise, the following discussion is not intended to represent any sequential operation steps, but rather the discussion of the components of system 100.

[0029] Although the teachings herein are described by way of example herein in terms of a web-based system using web browsers and a web site server (information processor 102), system 100 is not limited to that particular configuration. It is contemplated that system 100 can be arranged such that user terminal 104 can communicate with, and display data received from, information processor 102 using any known communication and display method, for example, using a non-Internet browser Windows viewer coupled with a local area network protocol such as the Internetwork Packet Exchange (IPX). It is further contemplated that any suitable operating system can be used on user terminal 104, for example, WINDOWS 3.X, WINDOWS 95, WINDOWS 98, WINDOWS 2000, WINDOWS CE, WINDOWS NT, WINDOWS XP, WINDOWS VISTA, LINUX and any suitable PDA or palm computer operating system.

[0030] Preferably, interactive video techniques are preferably implemented such that interactive data entry forms are provided via video instead of data entry forms provided using the hypertext transport protocol ("HTTP") and, for example, in the hypertext transport markup language ("HTML"). In a preferred embodiment, a user uses a computing device equipped with an internet web browser, and the computing device is preferably coupled to or operates in conjunction with a set top box, such as a custom configured television set top box. Initially, the user connects to a web site via an HTTP connection. Thereafter, when the user desires to transmit sensitive or private data, such as to pay for a good in an e-commerce web site, the user communicates via interactive video in a session that preferably operates concurrently with the HTTP session. The interactive video session is preferably routed securely through a middleware platform,

described in greater in co-pending and U.S. Patent Application No. 11/757,953 (incorporated herein by reference) and via the set top box.

[0031] The middleware platform preferably includes, *inter alia*, a media matching engine, a data matching engine, an internet security bridge and a video validation protocol. Moreover, non-recursive, non-pattern generating signatures are provided, thereby precluding any party that attempts to eavesdrop or otherwise intercept transmissions set forth herein gains no meaningful access to information. Accordingly, data are preferably filtered such that only reference information is transmitted and that identifying data, such as names, addresses, bank accounts or other personally identifying information, which may be used by unscrupulous parties, are not transmitted over the internet.

[0032] Private data transmissions occur via the secured interactive video session, and when the user (and the web site provider) has completed the private data transmissions, the less secured HTTP data communications resume. In this way, users are assured that sensitive and/or private data are not transmitted over the internet, but are instead routed via safe and secure "hard-wired" systems.

[0033] An example of the teachings herein is now provided with reference to an e-commerce application provided in conjunction with an internet web site.

[0034] A user operating a computing device that is coupled to a set top box connects to an internet web site operated by a vendor. The user connects to the vendor's web site using standard internet web browsing software. The web site offers goods for sale. Using the web site, the user selects items for purchase, and place the items in an e-commerce shopping cart. Once the user is done selecting items for purchase, the user continues the purchase operation, for example, by selecting a graphical screen control (e.g., a button) labeled "Check Out." Once the graphical screen control is selected, an interactive video session between the vendor and the user is established via the computing device and, accordingly, over the middleware platform provided by the teachings herein. The interactive video session is used to transmit private data, such as

the user's personally identifiable information, credit card information and other information the user desires to keep private.

[0035] Continuing with the above example, the checkout page that the user interacts with, such as by filling in data entry fields related to the purchase, looks and behaves as though it were a standard secured web page, such as encrypted via secured sockets layer ("SSL"). As noted above, however, the page is generated video broadcast that originates via the middleware platform and transmitted via the set top box. Thus, although the data entry display screen appears seamlessly integrated with the web site to the user, the data entry display screen is not an internet-based form. Moreover, as the user types, the user's respective keystrokes are not recognized as typical input, i.e. ASCII characters. Instead, the keystrokes generate new video, which is transmitted securely via the middleware platform back to the vendor.

[0036] Accordingly, the user has an experience that mimics typing and filling out a typical internet web-based checkout page. Instead, the user is typing, and not merely filling in blank fields in a form. As the user types, new video corresponding to the user's actions, selections and/or intentions is generated. The video feedback allows the user to validate the video the video observes (substantially in real time) against the data the user intended to enter. Collectively, the process referred to herein is referred to, generally, as a video validation engine.

[0037] Preferably, the middleware platform and corresponding data security protocol are provided that ensure secure, efficient and convenient operations for remote end-users. In one embodiment, a physical hardware architecture is provided that utilizes a cable television infrastructure that is supported by multiple system operators. Other embodiments include an implementation that utilizes satellite television and cellular telephone technology.

[0038] In another embodiment, a back-office technology is provided that includes a data storage element for storing digital video, video metadata, customer metadata and/or sequenced customer metadata with video metadata. The various data that are stored are

preferably consistently available for access for a customer service operation. In this way, customer service is provided with current and accurate data for problem resolution, responding to customer questions, and confirmation of transactions.

[0039] Further, disclosed is a financial transaction application that is operable to support a complete financial transaction, from start to finish. Sellers and purchasers alike preferably utilize the core middleware technology and back-office technology described herein for offering and/or selecting items and services for sale, and financial elements of the transaction are securely made without a threat of individual or corporate piracy. Further, the financial transaction application provided herein is operable for cable-television shopping. In another application, electronic and remote voting is provided in a secure fashion, and fees associated with voting, for example, during an interactive game are maintained under control by a proprietor of the systems and methods described herein.

[0040] In another embodiment, bridging internet transactions to secured cable systems is provided. Moreover, internet transactions are bridged over to secured satellite or mobile transmissions in accordance with the teachings herein. A bridging feature is provided wherein the topography of the internet is bridged to a cable multiple systems operator. Alternatively, bridging is provided for satellite television providers and cellular telephone providers.

[0041] Thus, the features and advantages of the systems and methods provided herein are supported at least in part by a media matching engine, a data matching engine, an internet security bridge and a video validation protocol. Moreover, non-recursive, non-pattern generating signatures are provided, thereby precluding any party that attempts to eavesdrop or otherwise intercept transmissions set forth herein gains no meaningful access to information. Accordingly, data are preferably filtered such that only reference information is transmitted and that identifying data, such as names, addresses, bank accounts or other personally identifying information, which may be used by unscrupulous parties, are not transmitted.

[0042] In yet another embodiment, time delay functionality is built into transmissions that guarantees the topology of least upper bound for the delay signatures. With regard to cellular telephone technology, cell switching delay methods, such as known in the art, are provided to guarantee that a transaction occurs in a single cell, at a single cell tower.

[0043] Preferably, systems and methods are provided herein for providing secure and efficient remote electronic interactions between suppliers of goods and services and consumers. Moreover, the systems and methods provided herein provide fulfillment of the goods and services. Preferably, a new arrangement of hardware and software elements and an arrangement of parties associated therewith operate to provide a new infrastructure that authenticates identities, locations and times associated with financial and data transactions, for example, in e-commerce transactions. As will become clear to one skilled in the art, the teachings herein reduce infrastructure and related costs, including for processing financial payments and product/service fulfillment, and ensure and improve data security and efficiency. For example, costs associated with hardware and software, such as in connection with initial purchases, leases and on-going maintenance fees, are eliminated by the teachings herein.

[0044] In particular and in accordance with an embodiment, a secure transfer of private and personal data is transmitted via an interactive cable medium and/or cellular telephone. Instead of merely placing a firewall, such as a router, proxy server or other known physical device, or, alternatively, security software that may operate as a firewall or other gateway, data are sent and validated through secure channels and used to confirm a person, location and time. Using the systems and methods described herein, transactions are protected and removed from hackers who would otherwise have access thereto, such via typical prior art internet and web site based transactions.

[0045] Preferably, the systems and methods herein are applicable to many services and define various business methods. For example, in a business-to-business ("B2B") retail environment as vendors are preferably charged a transactional fee to the proprietor hereof for use of the systems and methods disclosed herein. Further, in a B2B wholesale

environment, e-commerce vendors preferably pay distributors a transactional fee and the distributors, in turn, pay a license fee to the proprietor hereof. Moreover, in a business-business-to-consumer ("B2C") environment, e-commerce shoppers are preferably charged a fee by multiple system operators and preferably on their current billing system which would be secured by the means described herein. Multiple system operator, accordingly, pays at least a portion of that revenue to the proprietor hereof.

[0046] It is further believed that new markets are likely to spurn and/or expand as a direct result of the teachings herein. For example, large purchases can be remotely facilitated now as buyers and sellers achieve greater peace of mind in connection with the sales. Furthermore, the voting, taxation and other government related operations can be safely, securely and efficiently provided to end users. Moreover, cable television operators can realize increased profits in monthly billing. Furthermore, banks, financial service providers and insurance companies would further benefit from the security and improved data transmission layers.

[0047] In a preferred embodiment, payment-related information is securely transmitted via the data transmission source, described herein. Alternatively, e-commerce vendors initiate a session implementing the systems and methods herein during a checkout process. Multiple system operators and/or a proprietor hereof preferably are remunerated therefor.

[0048] Thus, in accordance with the foregoing, any company that has products or services which manage or assist in the securing of financial and data transactions for, for example, e-commerce vendors can partner with a proprietor hereof. For example, providers, such as CISCO, may benefit as the infrastructure according the teachings herein is reduced. Further, payment processors, such as PAYPAL, may benefit as costs associated with payment are reduced in accordance with the teachings herein. Further, security providers, such as CISCO and/or VERISIGN, may also benefit as data are secured while in transit, and safely off of the internet.

[0049] In one embodiment, live digital video feed is synchronized with real time auditing data that represents a person's actions, graphical screen control selections, indications, and/or financial purchases. A data audit trail is preferably instantly generated that corresponds to a person's activities to during a real-time event that is substantially simultaneously shown via digital video transmission. Preferably, small-sized data elements and/or small quantities of data elements are transmitted from a channel that consequently trigger applications and/or graphics for the user to select. In one embodiment, the term, "channel" refers generally to a full cable station, a sub-channel on a station, or and interactive add-in to an existing channel, as known in the art.

[0050] As will be clear to one skilled in the art, a new technology that greatly improves the speed of data transactions by enabling the transport of large amounts of information without a requirement for transmitting large quantities of data is provided herein. This preferably occurs as a function of metadata that represents and correlates with associated digital video data. By transmitting corresponding metadata and not the corresponding digital video, which requires significantly more bandwidth, performance is substantially faster than prior art transmissions.

[0051] In a preferred embodiment, and as described in greater detail below, media asset management is provided and replaces cost-prohibitive integration of, for example, customized or proprietary enterprise resource planning applications. In typical prior art installations of enterprise resource planning ("ERP") applications, as known in the art, often result in a customer incurring substantial fees. Expenses in the tens of millions of dollars of hidden costs for EAI (enterprise application integration) are not uncommon in multiple large-scale applications that require integration (to be able to share) and share information. The union of a media matching engine with a data matching engine, as described herein, provides a sort of universal card catalog system, in which multiple applications can draw from, store, and relate, data cataloged from multiple sources.

[0052] The data matching engine is operable to track user activity in relation to video feed, and tracking user response to video is provided without a need for a return feed of

the video. Moreover, software is provided for freeze-on-demand help screens during interaction with the interactive video. In this way, video transmission of data entry and or other content is paused while a help screen or other display is reviewed by user. The transmission preferably resumes from the point where the transmission or entry was paused.

[0053] The hardware and software architecture provided herein is designed to protect against and/or to address distributed denial of service ("DDoS") attacks, blackmail, identity fraud, age verification and money laundering. Moreover, responsible advertising, age verification standards and player protection measures are concerns that are addressed by the technological advancements provided herein.

[0054] Preferably, the application is provided that, in one or more embodiments, uses at least a non-proprietary set top box, data matching engine, and video matching engine which integrally plug into and comply with existing technology including, for example, OpenCable Applications Platform ("OCAP") programming and Data Over Cable Service Interface Specification ("DOCSIS") protocol.

[0055] Fig. 3 illustrates an embodiment of an example arrangement including an example flow of information and order of operation in accordance with an embodiment. As shown in Fig. 3, video feed 312 is transmitted to a user terminal 104, for example, at the user's home. Video feed 312 and video metadata 318 are preferably sent to media matching engine 317, and sequenced together. The sequenced video metadata 318 without video feed 312 is preferably transmitted data matching engine 321, and preferably located at a secure location close to user terminal 104. While user operating user terminal 104 watches video feed 312, the user decides to make a purchase. A request for purchase/transaction is sent to data matching engine 321. The transaction is preferably validated by matching the user's request with video metadata 318, thereby providing matched metadata 324. The matched metadata 324 is transmitted to the media matching engine 317, for example, to process a financial transaction and fulfillment. The completed transaction is preferably stored in information processor 102, such as a media asset management server, for example, for auditing and customer service.

[0056] Preferably, the application is provided that, in one or more embodiments, uses at least a non-proprietary set top box, data matching engine, and video matching engine which integrally plug into and comply with existing technology including, for example, OpenCable Applications Platform ("OCAP") programming and Data Over Cable Service Interface Specification ("DOCSIS") protocol.

[0057] One skilled in the art will appreciate that the broadcast channel or middleware applications, described above, provide an added value to user terminal 104 or other entertainment show that can be delivered as a full cable channel, a sub-channel on interactive Cable, or as an add-in to an existing channel, or even a single show.

[0058] Fig. 4 illustrates an embodiment of an example arrangement and flow of information in accordance with the teachings herein. At step 1, a consumer (user 204) decides to make a purchase. Thereafter, at step 2, a data transport begins, wherein the seller offers data transfer via the teachings herein or, alternatively, the user 204 selects data transfer via the teachings herein. Thereafter, at step 3, user 204 executes a payment method and a financial product is executed. A payment request is sent at step 4 to a payment processing center, and, at step 5, the financial transaction is validated, the user's 204 account is credited or debited, and a verification of the transaction is transmitted to the seller. The seller maintains an active communication session with, for example, information processor 102, which may be formatted as a media asset management server.

[0059] Continuing with reference to Fig. 4, at step 6, the seller begins a fulfillment process and, via a TCP/IP or other internet session, sends the user 204 a receipt of payment and acknowledgement of a completed transaction (step 7). Thereafter, at step 8, the payment processing center credits an account for the transaction.

[0060] Using the features shown in Fig. 4, consumers are protected against theft of information, or unauthorized use of their financial product, because the execution of the transaction is verified as genuine by the consumer's consent, the seller's consent, location verification, and by time stamping.

[0061] In accordance with an embodiment, security and personal identities for transactions are ensured as part of a new protocol for a cable environment. The new protocol preferably utilizes the physical characteristics of devices provided in the "last mile," as known in the art, to guarantee an audit of a location, time, and person. Preferably, one or more signatures are applied to transactions that are directly linked to properties regarding how a particular location is tied into a cable infrastructure. The signature encapsulates the identities of several physical objects or devices, each having a respective hardware signature. The combinatorics related to this type of security exceeds the value of two to the power of 32 (i.e., 2^{32}). This is many magnitudes better than the known PGP encryption or, alternatively, 64 bit md5-hash encryption, of PKI (Public Key Infrastructure) technologies.

[0062] Thus, a new technology integrator is provided for a unique and truly secure validation process that protects the electronic transfer of digital assets and financial data. As e-commerce is expanding exponentially, solutions are provided herein to the frailties of existing transactional security measures, which have become apparent and costly. Particularly, a proprietary data transport system that secures transactions within existing distributed communications systems, such as cable television, satellite television, and mobile telephone technologies, is provided. A significant impact is provided by utilizing bridging vital internet transactions over distributed systems that have been secured in accordance with the teachings herein. This feature, referred to herein, generally, as a "bridge-to-internet" solution, enhances known internet technology and provides the security of a "hard wired" system for those transactions that need to be protected beyond what the internet currently can ensure. Protection from theft of data and money by moving secured transactions to a system where those problems do not exist is provided. This is a first for the internet and it answers issues of security, fraud, and user confidence beyond any existing security solution.

[0063] Most thefts and hacks on the internet occur from malicious people and software attempting to impersonate an element of the communication path, such as the user, a router, a server, or a web site. Such impersonations are not possible in accordance

with the teachings herein. Instead, a consumer enjoys the freedom and expanse of choices previously expected from the internet. Once a consumer decides to make a purchase or exchange critical data, his/her private information is conveyed not via the internet, but via the systems and methods shown and described herein. Unlike prior art systems, private data are not transported exclusively over the internet.

[0064] Additionally, vendors and companies providing services on the internet can guarantee a new level of protection because the servers and systems that contain customer information will no longer be accessed through the public internet. The traditional CICS, or Customer Information Control Systems, would be "offline" and inaccessible from the internet. Costly breaches of security on the internet that typically originate from people accessing servers that contain financial information for thousands of users are now prevented.

[0065] The systems and methods herein do not replace existing known internet security measures, such as firewalls, key encryption, secured sockets layer, and PGP, but rather enhances and compliments these existing solutions at a more physical level. Users, vendors, and merchanting agents will all benefit from the systems and methods described herein. A technology enhancement is supported that is built on existing infrastructures, and hence, its speed of deployment, and growth are determined by the services already in use.

[0066] The systems and methods disclosed herein preclude penetrations from security, privacy, and financial threats is provided herein. In e-commerce applications, critical data are out of harm's way. For example, international piracy, identify fraud, malicious code, corporate espionage and hacking are thwarted.

[0067] In another embodiment, a consumer decides to make a purchase of a good. Data transport preferably begins when the seller of the good or consumer purchasing the good selects the middleware and data protocol for the sale mechanism. The consumer utilizes the middleware and secure data protocol to execute his/her payment method, and the financial product is executed. Thereafter, the seller's computer, e.g., server computer,

sends a handshake command (as known in the art) to determine that the user has interactive technology, such as interactive cable television, and, if so, ensures that the technology is compliant with the teachings herein. In case the connection is compliant, a checkout display screen is preferably sent to the user via the set top box. The checkout page is preferably generated video that corresponds to the user's responses, such as name, address, credit information or the like. When the checkout page is complete, a validation request is transmitted to the seller and, when validated, a receipt is preferably transmitted to the user and fulfillment of the purchase occurs. In this way, the consumer is protected against theft of information, or unauthorized use of his/her financial product, because the execution of the transaction is verified as genuine by the consumer's consent, the seller's consent, location verification, and by time stamping. Further, the consumer and seller are protected from internet fraud during the transaction because the transaction itself does not occur on the internet; it occurs on a more secure "hard wired" (e.g., cable system secured via the teachings herein) system. The consumer and seller are protected from corporate piracy at all points of data storage because those points can not be "seen" or accessed from the internet. In other words, servers at a vendor's site contain critical user data are off the internet, and on the cable system.

[0068] Moreover, existing security platforms benefit from the teachings herein. Rather than pose a competitive challenge to current and developing security and privacy platforms, known security measures are enhanced and enriched. The systems and methods herein work in conjunction with known platforms, such as DOCSIS[®], to maintain integrity and make them more potent. This is vital since DOCSIS was primarily developed to protect against theft of cable service from piracy and descramblers, and since current security measures require separate installations at the application program level. The systems and methods described herein "sit below" the DOCSIS transport, and guarantee security and privacy by seamlessly verifying the person and his action against what he is viewing at the time of his actions. Then, actions are verified and transactions are completed from a secure non-public location. In accordance with the teachings herein, data transfer activities occur off of the public internet, thereby fortifying existing security systems.

[0069] Thus and as described herein, a new security protocol is defined that provides protection beyond that previously available, for example, over the internet. The new protocol is preferably integrated into a new combination of hardware and software that makes the platform capable of being customized and licensed for various industries and uses, beyond gaming. Moreover, a use of a matrix switch, which is capable of connecting a plurality of input to a plurality of outputs, and operable with the data matching engine provides a convenient and cost-effective approach for distributing video across various platforms and over the "last mile."

[0070] The systems and methods for transmitting and validating data ensures that the platform is provided having an architecture that inherently prohibits known methods of online security fraud, hacking, and identity theft. Further, there is tremendous potential to generate revenue from the licensing of the systems and methods described herein. Low break even points, low start up costs, low scalability cost of growth, low subscriber requirements for success, low requirements in staffing and fixed assets and no technological/hardware infrastructure obstacles to growth are all factored together that results in a profitable and lucrative business model.

[0071] Although the present invention has been described in relation to particular embodiments thereof, many other variations and modifications and other uses will become apparent to those skilled in the art. For example, using the secured protocol and middleware described herein, health insurance providers can offer in-home access to confidential and previously unavailable medical records. In a preferred embodiment, a health channel is provided that includes a patient and doctor side. Patients retrieve information, shop for doctors, even pay medical bills or contact insurance companies. Doctors post medical results, schedule meetings and collect revenues. Both patients and doctors preferably store, retrieve, and view critical record and film, and comply with various requirements, such as defined by the Health Insurance Portability and Accountability Act ("HIPAA") . Such compliance is provided because a person, the person's location , and permission to view an object securely are validated and ensured.

[0072] The systems and methods described herein provide an effective risk management tool to reduce costs, for example, due to lawsuit stemming from lost records. In one business method, the middleware and secure protocol can be provided for a low fee, such as one dollar a month added value for health insurance carriers to offer to their subscribers, potentially netting tens of millions of dollars in previously unrealized capital.

[0073] In another embodiment, the middleware and secure protocol described herein can function to securely transport files between imaging centers and physicians' offices. A typical physicians' office with four to six physicians may spend an average of \$150k per year on courier and transportation services. It is believed that those physicians would gladly pay more for a faster and safer delivery method. Moreover, many (if not most) physicians' offices would save an FTE (Full Time Equivalent person of 30k year) when they employ electronic records handling in accordance with the teachings herein. A proprietor of the systems and methods herein that provides a secure transport of files between hospitals and physicians' offices may result in earnings of hundreds of millions of dollars.

[0074] Moreover, similar to insurance companies, physicians who use the systems and methods described herein can offer records access to all their patients. The middle and secure protocol that offers such record access service at, for example, \$5,000 per year, per practice, may net hundreds of millions of dollars.

[0075] In yet another application, the middleware and secure data protocol can be implemented for electronic bill payments. For example, the systems and methods described herein can be offered as a single source for all home maintenance bills such as oil, gas, electric, water, cable television, and/or telephone phone. This is believed to be an attractive alternative for many internet users who do not trust the internet for secure financial information. Such users would be more amenable to the secure platform provided herein, as well as the ease of use and overall convenience.

[0076] Accordingly, the middleware platform and corresponding data protocol that ensure secure, efficient and convenient operations for end-users, even for users who are not technically proficient, is provided. Moreover, a core technology is preferably provided that includes at least a matching engine that receives metadata representing a video feed, and metadata that represents a customer and the customer's actions, and matches the two sources of metadata. The two sources of data are preferably sequenced together for cross-referencing purposes. A physical topology or architecture is further disclosed that utilizes, in one embodiment, a cable television infrastructure that is supported by multiple system operators. Other embodiments include satellite television and cellular telephone technologies.

[0077] Further, a back-office technology is provided that includes a data storage element for storing digital video, video metadata, customer metadata and/or sequenced customer metadata with video metadata. The various data that are stored are preferably available 24-hours per day, seven days per week for access by a live help-desk or customer service operation. In this way, customer service is provided for customers that includes current and accurate data.

[0078] The features and advantages of the systems and methods provided herein are supported at least in part by a media matching engine, a data matching engine, an internet security bridge and a video validation protocol. Moreover, non-recursive, non-pattern generating signatures are provided, thereby precluding any party that attempts to eavesdrop or otherwise intercept transmissions set forth herein gains no meaningful access to information. Instead, data are preferably filtered such that only reference information is transmitted and that identifying data, such as names, addresses, bank accounts or other personally identifying information, which may be used by unscrupulous parties, are not transmitted.

[0079] Accordingly, the teachings herein effectively secure the transfer of private and personal data, for example, via interactive cable platforms and cell telephones. Such security is preferably provided and utilized over the internet, but without transmitting

private data via HTTP connections on the internet. The teachings herein effectively and economically solve many data security issues -starting with ecommerce and personal financial data.

[0080] Although the present invention has been described in relation to particular embodiments thereof, many other variations and modifications and other uses will become apparent to those skilled in the art. It is envisioned and preferred, therefore, that the present invention not be limited by the specific disclosure, herein.

WHAT IS CLAIMED IS:

1. A method for secure transmission of electronic information between two parties, the method comprising:

establishing a first data communication session between a first computing device and a second computing device, wherein the first data communication session is via a first communication protocol;

transmitting by the first computing device first information via the first communication protocol and receiving by the second computing device the first information via the first communication protocol;

establishing during the first communication session a second data communication session between the first computing device and the second computing device, wherein the second communication session is via a second communication protocol, and further wherein the second communication session and the second communication protocol is more secure than the first communication session and the second communication protocol, respectively; and

transmitting by the first computing device second information via the second communication protocol and receiving by the second computing device the second information via the second communication protocol, wherein the second information relates at least partially to the first information,

wherein the second communication session appears to a user of the first computing device to be the first communication session.

2. The method of claim 1, wherein the first communication session occurs over the internet and the first communication protocol is HTTP, and the second communication session occurs over a cable television infrastructure and the second communication protocol provides interactive video.

3. The method of claim 2, wherein the second information is transmitted via data entry display forms provided via the interactive video.

4. The method of claim 3, wherein the interactive video is provided via a set top box.

5. The method of claim 2, further comprising fee sharing arrangements among at least one of a cable television provider and a multiple system operator.

6. The method of claim 1, wherein the first communication session occurs over the internet and the first communication protocol is HTTP, and the second communication session occurs over a satellite television infrastructure and the second communication protocol provides interactive video.

7. The method of claim 1, wherein the first communication session occurs over the internet and the first communication protocol is HTTP, and the second communication session occurs over a cellular telephone infrastructure and the second communication protocol provides interactive video.

8. The method of claim 1, wherein the transmission relates to shopping for goods and services.

9. The method of claim 1, wherein the transmission relates to voting.

10. The method of claim 1, further comprising providing an audit trail relating to the transmission of the first information and the second information.

11. A system for secure transmission of electronic information between two parties, the method comprising:

a first data communication session between a first computing device and a second computing device, wherein the first data communication session is via a first communication protocol;

a first transmission sent by the first computing device first information via the first communication protocol and received by the second computing device via the first communication protocol;

a second data communication session established during the first communication session between the first computing device and the second computing device, wherein the second communication session is via a second communication protocol, and further wherein the second communication session and the second communication protocol is more secure than the first communication session and the second communication protocol, respectively; and

a second transmission by the first computing device second information via the second communication protocol and receiving by the second computing device the second information via the second communication protocol, wherein the second information relates at least partially to the first information,

wherein the second communication session appears to a user of the first computing device to be the first communication session.

12. The system of claim 11, wherein the first communication session occurs over the internet and the first communication protocol is HTTP, and the second communication session occurs over a cable television infrastructure and the second communication protocol provides interactive video.

13. The system of claim 12, wherein the second information is transmitted via data entry display forms provided via the interactive video.

14. The system of claim 13, further comprising a set top box for providing the interactive video.

15. The system of claim 12, further comprising a fee sharing arrangement among at least one of a cable television provider and a multiple system operator.

16. The system of claim 11, wherein the first communication session occurs over the internet and the first communication protocol is HTTP, and the second communication session occurs over a satellite television infrastructure and the second communication protocol provides interactive video.

17. The system of claim 11, wherein the first communication session occurs over the internet and the first communication protocol is HTTP, and the second communication session occurs over a cellular telephone infrastructure and the second communication protocol provides interactive video.

18. The system of claim 11, wherein the transmission relates to shopping for goods and services.

19. The system of claim 11, wherein the transmission relates to voting.

20. The system of claim 11, further comprising an audit trail relating to the transmission of the first information and the second information.

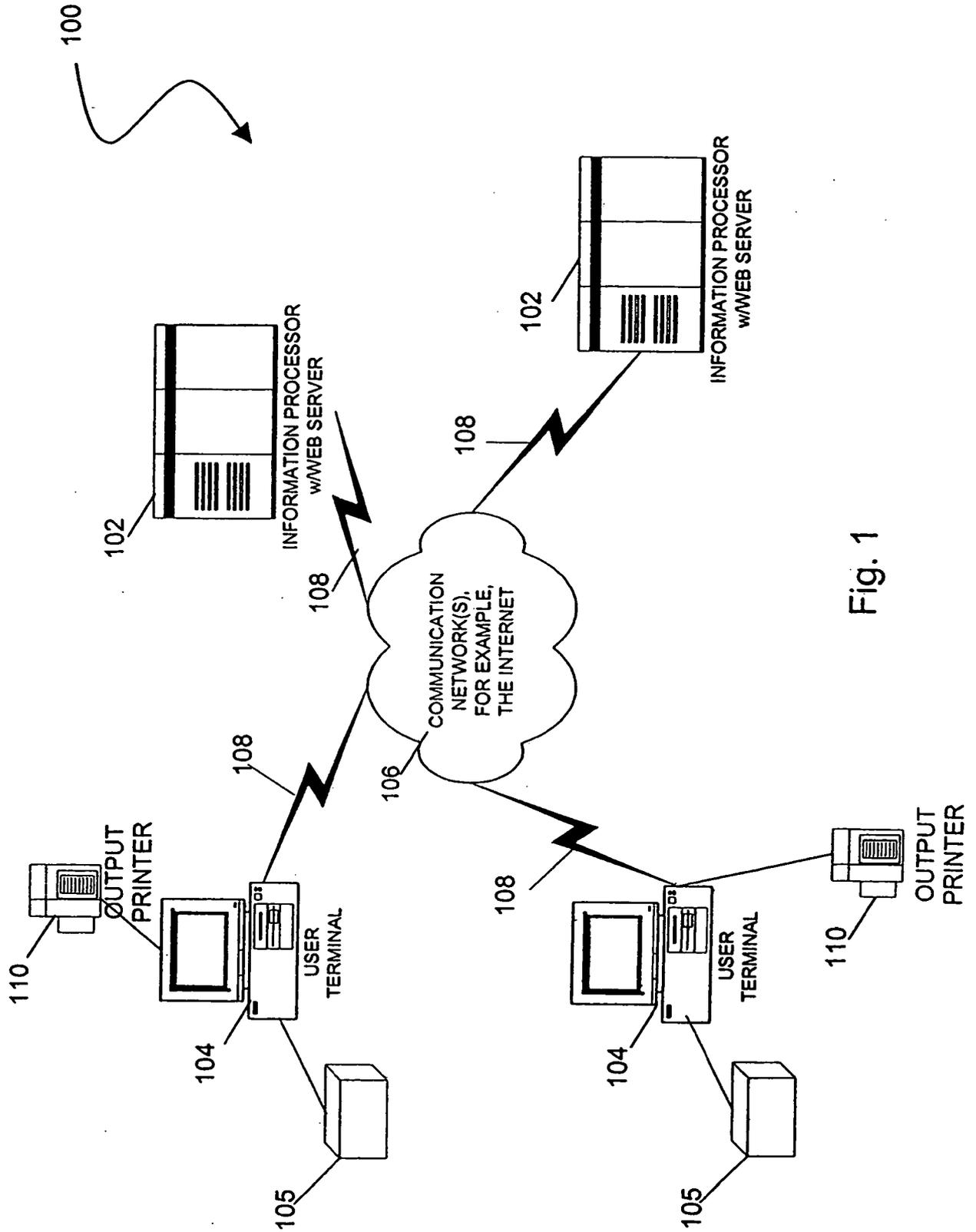


Fig. 1

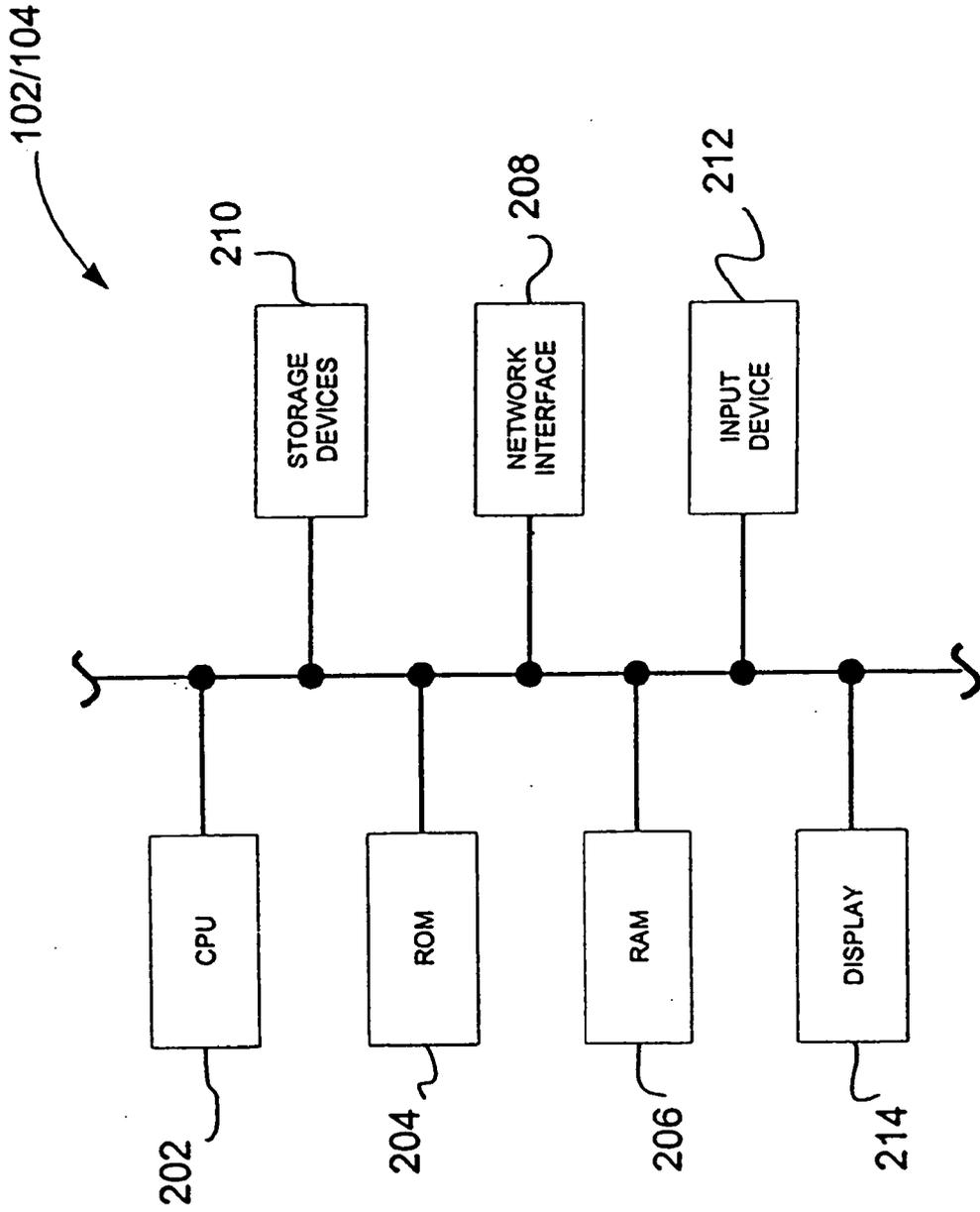


Fig. 2

3/4

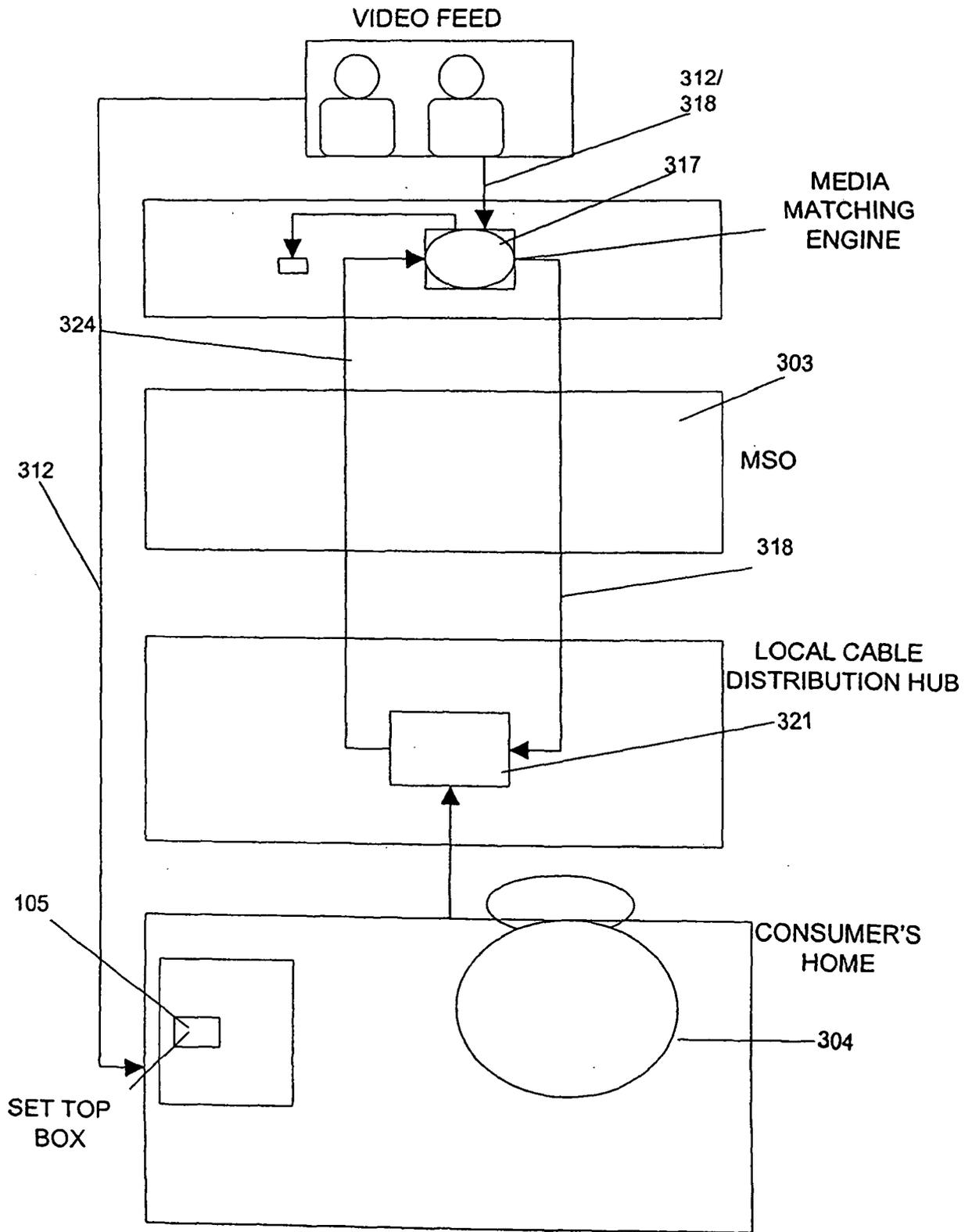


Fig. 3

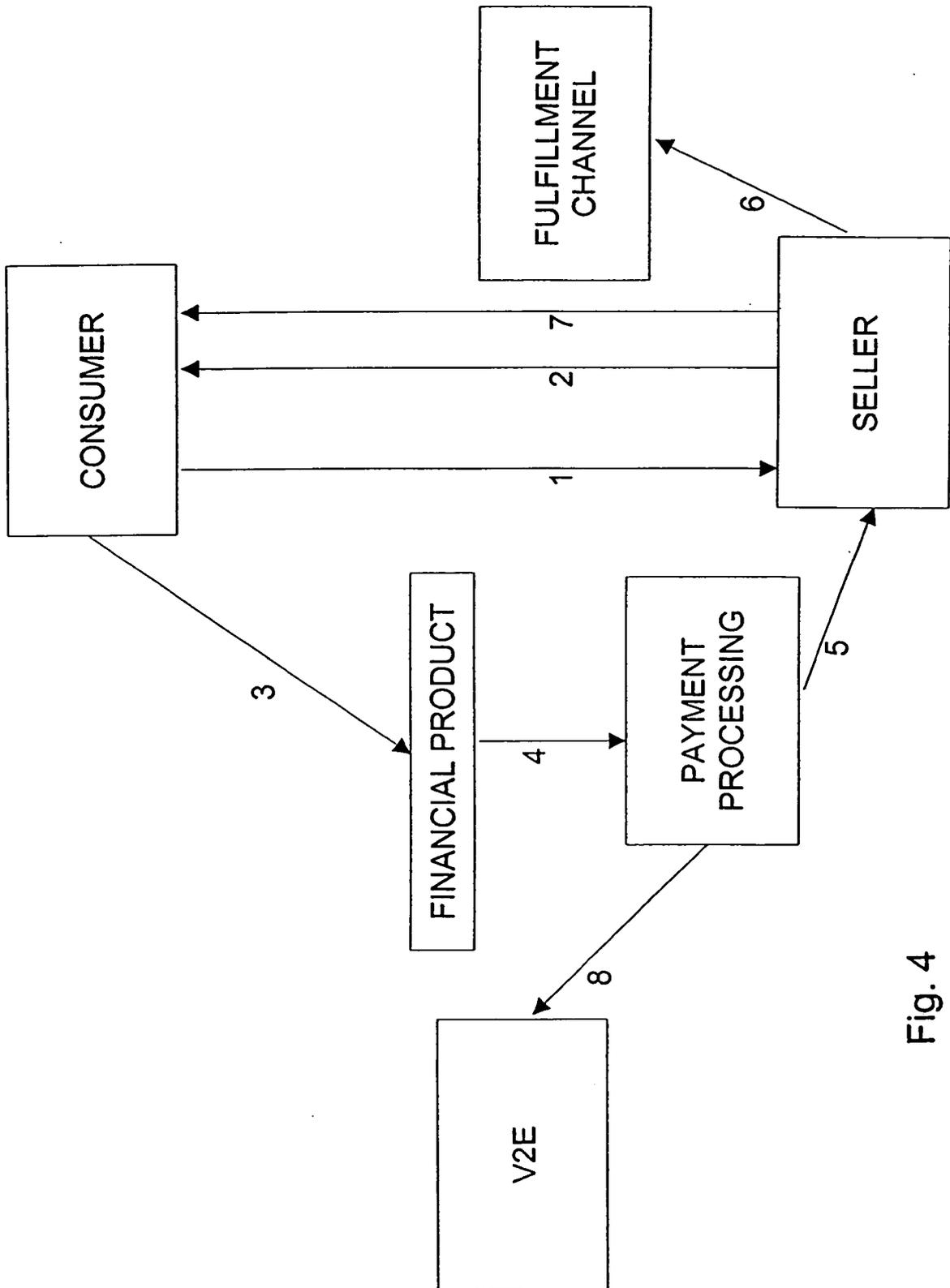


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US 08/09557

A CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04J 3/16, H04J 3/22 (2008.04)
USPC - 370/466
According to International Patent Classification (IPC) or to both national classification and IPC

B FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - H04J 3/16, H04J 3/22 (2008 04)
USPC - 370/466

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 725/112, 113, 705/1 (text search)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
OialogClassic, Google, freepatentsonline com, search terms used internet, web, purchase, buy, secure, securely, securing, fee sharing, audit, transmit

C DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
X ---	US 2004/0031057 A 1 (WAITES) 12 February 2004 (12 02 2004), entire document, especially Fig 1, para [0006], [0008], [0010]	1, 2, 8, 11, 12, 18
Y		3-5, 6, 7, 9, 10, 13-17, 19, 20
Y	US 2004/0003412 A 1 (HALBERT) 01 January 2004 (01 01 2004), entire document, especially Fig 1, para [0012], [0014], [0023], [0035], [0063], [0064]	3, 4, 6, 7, 9, 13, 14, 16, 17, 19
Y	US 2006/0015904 A 1 (MARCUS) 19 January 2006 (19 01 2006), entire document, especially para [0331], [0364], [0447], [0578], [0579]	5, 10, 15, 20

Further documents are listed in the continuation of Box C

* Special categories of cited documents
 "A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier application or patent but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed
 "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "Z" document member of the same patent family

Date of the actual completion of the international search
13 October 2008 (13 10 2008)

Date of mailing of the international search report
05 NOV 2008

Name and mailing address of the ISA/US
Mail Stop PCT, Attn ISA/US, Commissioner for Patents
P O Box 1450, Alexandria, Virginia 22313-1450
Facsimile No 571-273-3201

Authorized officer
Lee W Young
PCT Helpdesk 571 272-4300
PCT OSP 571 272 7774