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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 July 2023 (20.07.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/135462 A1

(51) International Patent Classification:
H04N 21/25 (2011.01) *H04N 21/80* (2011.01)
H04N 21/43 (2011.01)

(21) International Application Number:
PCT/IB2022/061245

(22) International Filing Date:
22 November 2022 (22.11.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202211002677 17 January 2022 (17.01.2022) IN

(72) Inventor; and
(71) Applicant: **AGRAWAL, Sanjay** [IN/IN]; 143, Munirka Enclave, New Delhi 110067 (IN).

(74) Agent: **KHURANA & KHURANA, ADVOCATES & IP ATTORNEYS**; E-13, UPSIDC, Site-IV, Behind-Grand Venice, Kasna Road, Greater Noida, National Capital Region, Uttar Pradesh 201310 (IN).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV,

(54) Title: SYSTEM AND METHOD FOR CONTROLLING DIGITAL CONTENT VIEWERSHIP

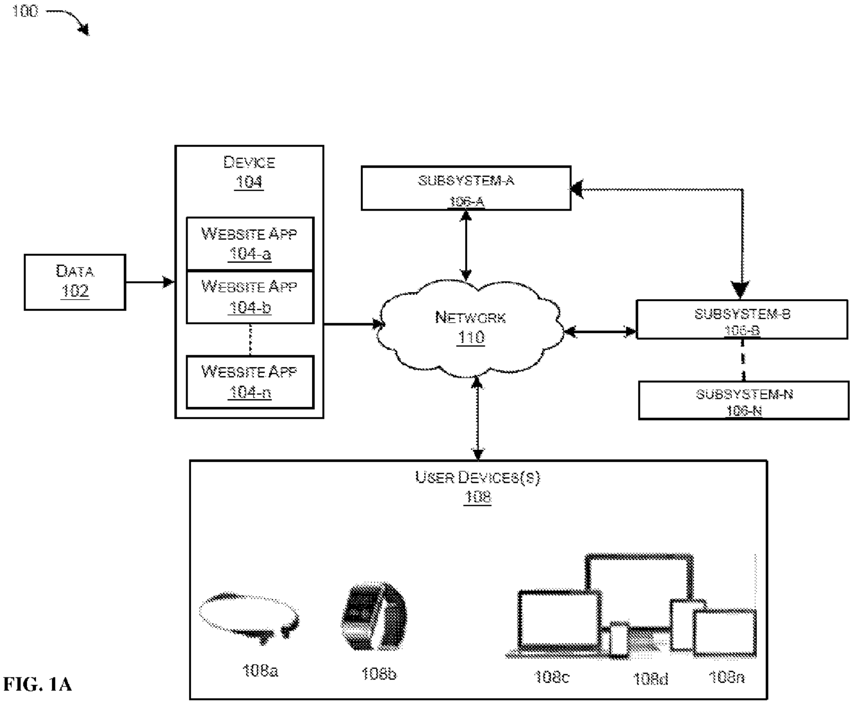

FIG. 1A

(57) **Abstract:** The present disclosure relates to a system and method for controlling digital content viewership. The system (100) comprises one or more user devices (108), a subsystem-A (106- A), the subsystem- B (106-B). The one or more user devices (108) comprise unique device identifier, wherein each of the one or more user devices (108) are authenticated and registered by the subsystem-B (106-B) using the unique device identifier. The subsystem-A encodes data, stores data, enables transmission security check, transmission quality check, to transmit the encoded data to the subsystem-B (106-B). Subsystem-B (106-B) is configured to receive and encode the received data from the subsytem-A, where the subsytem-B is configured to encode and transmit each stream specific to each registered device, where the encoded data restricts unauthorized access to the transmitted data.

WO 2023/135462 A1

[Continued on next page]

GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

SYSTEM AND METHOD FOR CONTROLLING DIGITAL CONTENT VIEWERSHIP

TECHNICAL FIELD

[0001] The present disclosure relates to the field of data streaming, and more particularly the present disclosure relates to a system and method for controlling digital content viewership.

BACKGROUND

[0002] Background description comprises information that may be useful in understanding the present invention. It is not an admission that any of the information provided herein is prior art or relevant to the presently claimed invention, or that any publication specifically or implicitly referenced is prior art.

[0003] Consumers are becoming accustomed to near ubiquitous access to Internet-based and web-based services and applications. In the past, data intensive applications, such as steaming video, on-demand video, video conferencing, etc., were limited to devices, such as personal computers, set-top boxes, stand-alone video conferencing systems, etc., having dedicated, high-speed (e.g., broadband) data connections provided by an Internet service provider (ISP). Today, consumers have access to a plethora of electronic devices, including smartphones, tablet computers, personal data devices, personal digital assistants, etc., that support Internet connectivity, and may have sufficient processing power to support at least some media-rich applications.

[0004] Currently, the scenario of regular streaming of data on any device is not able to restrict, check or control the number of users of said data. When the number of users that have access to the data are restricted, checked or controlled it becomes inconvenient to the user(s).

[0005] There is, therefore, a need to overcome the above drawback and providean efficient, secure and reliable system and method for controlling digital content viewership, during data streaming.Further, there is also a need to reduce the complexity and cost involved in managing device-specific keys

OBJECTS OF THE PRESENT DISCLOSURE

[0006] Some of the objects of the present disclosure, which at least one embodiment herein satisfies are as listed herein below.

[0007] It is an object of the present disclosure to provide a simple, secure, and efficient system and method for controlling digital content viewership.

[0008] It is an object of the present disclosure to provide a simple, secure, and efficientsystem and method for streaming data seamlessly to user devices such as IoT devices, infotainment devices, gaming devices, and the likes.

[0009] It is an object of the present disclosure to efficiently, economically, and securely manage the authentication of the user devices, and multi layered encoding of the data.

[0010] It is an object of the present disclosure to restrict unauthorized access to the transmitted data.

SUMMARY

[0011] The present disclosure relates to the field of data streaming, and more particularly the present disclosure relates to a system and method for controlling digital content viewership.

[0012] An aspect of the present disclosure pertains to system for controlling digital content viewership comprising one or more user devices, a subsystem-A, a subsystem-B, and other subsystem-N. The one or more user devices comprising unique device identifier, where the each of the one or more user devices are authenticated and registered by using the unique device identifier, where the each one or more user devices are registered user device. The subsystem-A can be communicatively coupled to a subsystem-B, other subsystem-N, and the one or more user devices. The subsystem-A can be configured to authenticate and register the one or more user devices using the unique device identifier to encode data, store data, enable transmission security check, transmission quality check, and to transmit the encoded data to the subsystem-B. The subsystem-B can be communicatively coupled to the one or more user devices, where the subsytem-B can be configured to receive and encode the received data from the subsytem-A. The subsytem-B can be configured to encoding and transmitting each stream specific to each registered device, where the encoded data restricts unauthorized access to the transmitted data.

[0013] An aspect of the present disclosure pertains to method for controlling digital content viewership can comprises authenticating and registering one or more user devices by a subsystem-A using unique device identifier, where the each one or more user devices are registered device. Further, the subsystem-A can receive and encode data by enabling transmission security check, transmission quality check, such that the encoded data is transmitted to the subsytem-B. The subsystem-B can perform streaming and transmitting of the encoded data, to each registered device, where the encoded data restricts unauthorized access to the transmitted data.

[0014] In an aspect of the present disclosure pertains to a system and method,the registered device can comprises unique device identifier selected from a group comprising device id, device type, device location, IP address, IMEI number and a combination thereof. The registered device can comprise includes unique electronic signature/fingerprint configuration.

[0015] In an aspect of the present disclosure pertains to a system and method,the one or more user devices can include non-wearable device(s) and wearable device(s), where the non-wearable device(s) and the wearable device(s) can be configured to ensure authorized usage check and transmission security check performed by the subsystem-A.

[0016] In an aspect of the present disclosure pertains to a system and method, the encoded data can be seamlessly decoded and streamed to the non-wearable device(s) and the user wearable device(s) based on occurrence of a data synchronization and passing of the transmission security check with permitted usage of data.

[0017] In an aspect of the present disclosure pertains to a system and method, the subsystem-A can be configured to perform a multi layered encoding to detect unauthorized usage of data, where separate and specific encoding can be performed on the one or more user devices and one or more transmissions by allocating an unique encoding identifier, where the one or more user devices and one or more transmissions can be traced along with location through which data is unauthorized used.

[0018] In an aspect of the present disclosure pertains to a system and method, the subsystem-A can be configured to interrupt the transmission of encoded data based on faults detected in the security of transmission of encoded data.

[0019] Various objects, features, aspects and advantages of the inventive subject matter will become more apparent from the following detailed description of preferred embodiments, along with the accompanying drawing figures in which like numerals represent like components.

BRIEF DESCRIPTION OF DRAWINGS

[0020] The accompanying drawings are comprised to provide a further understanding of the present disclosure, and are incorporated in and constitute a part of this specification. The drawings illustrate exemplary embodiments of the present disclosure and, together with the description, serve to explain the principles of the present disclosure. The diagrams are for illustration only, which thus is not a limitation of the present disclosure.

[0021] In the figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[0022] FIGs. 1A and 1B illustrate exemplary network architecture of the proposed systemfor controlling digital content viewership, in accordance with an embodiment of the present disclosure.

[0023] FIG. 2 illustrates an exemplary architecture of the proposed system for controlling digital content viewership, in accordance with an embodiment of the present disclosure.

[0024] FIG. 3 illustrates an exemplary block diagram 300 implementing the mechanism for controlling digital content viewership, in accordance with an embodiment of the present disclosure.

[0025] FIG. 4 illustrates an exemplary flow diagram of steps involved in the proposed method for controlling digital content viewership, in accordance with an embodiment of the present disclosure.

[0026] FIG. 5 illustrates an exemplary computer system in which or with which embodiments of the present invention can be utilized in accordance with embodiments of the present disclosure.

DETAILED DESCRIPTION

[0027] The following is a detailed description of embodiments of the disclosure depicted in the accompanying drawings. The embodiments are in such detail as to clearly communicate the disclosure. However, the amount of detail offered is not intended to limit the anticipated variations of embodiments; on the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the present disclosure as defined by the appended claims.

[0028] In the following description, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the present invention. It will be apparent to one skilled in the art that embodiments of the present invention may be practiced without some of these specific details.

[0029] The present disclosure relates to the field of data streaming, and more particularly the present disclosure relates to a system and method for controlling digital content viewership.

[0030] An embodiment of the present disclosure pertains to system for controlling digital content viewership comprising one or more user devices, a subsystem-A, a subsystem-B, and other subsystem-N. The one or more user devices comprising unique device identifier, where the each of the one or more user devices are authenticated and registered by using the unique device identifier, where the each one or more user devices are registered user device. The subsystem-A can be communicatively coupled to a subsystem-B, other subsystem-N, and the one or more user devices. The subsystem-A can be configured to authenticate and register the one or more user devices using the unique device identifier to encode data, store data, enable transmission security check, transmission quality check, and to transmit the encoded data to the subsystem-B. The subsystem-B can be communicatively coupled to the one or more user devices, where the subsytem-B can be configured to receive and encode the received data from the subsytem-A. The subsytem-B can be configured to encoding and transmitting each stream specific to each registered device, where the encoded data restricts unauthorized access to the transmitted data.

[0031] An embodiment of the present disclosure pertains to method for controlling digital content viewership can comprises authenticating and registering one or more user devices by a subsystem-A using unique device identifier, where the each one or more user devices are registered device. Further, the subsystem-A can receive and encode data by enabling transmission security check, transmission quality check, such that the encoded data is transmitted to the subsytem-B. The subsystem-B can perform streaming and transmitting of the encoded data, to each registered device, where the encoded data restricts unauthorized access to the transmitted data.

[0032] In an embodiment, the registered device can comprises unique device identifier selected from a group comprising device id, device type, device location, IP address, IMEI number and a combination thereof. The registered device can comprise includes unique electronic signature/fingerprint configuration.

[0033] In an embodiment,the one or more user devices can include non-wearable device(s) and wearable device(s), where the non-wearable device(s) and the wearable device(s) can be configured to ensure authorized usage check and transmission security check performed by the subsystem-A.

[0034] In an embodiment, the encoded data can be seamlessly decoded and streamed to the non-wearable device(s) and the user wearable device(s) based on occurrence of a data synchronization and passing of the transmission security check with permitted usage of data.

[0035] In an embodiment, the subsystem-A can be configured to perform a multi layered encoding to detect unauthorized usage of data, where separate and specific encoding can be performed on the one or more user devices and one or more transmissions by allocating an unique encoding identifier, where the one or more user devices and one or more transmissions can be traced along with location through which data is unauthorized used.

[0036] In an embodiment,the subsystem-A can be configured to interrupt the transmission of encoded data based on faults detected in the security of transmission of encoded data.

[0037] Referring to FIGs. 1and 2, the proposed system 100 for controlling digital content viewership comprises one or more user devices 108-1 to 108-N (collectively referred to as devices 108, herein), data102, a device 104 includes multiple website applications104-a to 104-n, a subsystem-A 106-A, a subsystem-B 106-B, a subsystem-N, a network 110. The one or more user devices 108-1 to 108-N includes non-wearable device(s) and wearable device(s), where the non-wearable device(s) can be selected from a group comprising smart phones, laptops, Amazon echo show, palmtop and the like. Further, the wearable device(s) can be selected from a group comprising Bluetooth earphones, air pods, smart watches, head-mounted displays, smart home devices, and the like (also designated as 108, herein). The system 100 includes the network 110 which is configured to establish communication between the device 104, the subsystem-A 106-A, the subsystem-B 106-B, and the one or more user devices.

[0038] The one or more user devices 108 comprising unique device identifiers, where each of the one or more user devices are authenticated and registered by using the unique device identifier. The registered device comprises unique device identifier selected from a group comprising device id, device type, device location, IP address, IMEI number and the like. Thus, the each one or more user devices are known as registered user device. The one or more user devices 108 can comprise includes unique electronic signature/fingerprint configuration.

[0039] In another exemplary embodiment, the system can include either the device 104 or a satellite 112 (Figure 1B). Thedevices104 are selected from IoT devices, infotainment devices, gaming devices, and the likes.The devices 104 includes multiple website applications 104-a to 104-ncomprising but not limited to, YouTube, Netflix, Amazon prime, Discovery Plus. The satellite 202 is also known as communications satellite, which is an artificial satellite that relays and amplifies radio telecommunication signals. The satellite 202 creates a communication channel between a source transmitter and a receiver at different locations on Earth. The satellite 202 comprising but not limited to television, telephone, radio, internet, military applications.

[0040] In an embodiment, the proposed system 100 is implemented using any or a combination of hardware components and software components such as a cloud, a server, a computing system, a computing device, a network device, and the like. Further, devices 104 interact with the subsystem-A, through an application or software 104-a...104-n that resides in the devices 104. In an implementation, the system 100 is accessed by an application that is configured with any operating system, comprising but not limited to, Android^{TM}, iOS^{TM}, Windows, and the like. It will be understood that the system is implemented as any suitable computing system known in the art, such as a desktop, a laptop, a server, web server, and the like.

[0041] Further, network 110 is a wireless network, a wired network or a combination thereof that is implemented as one of the different types of networks, such as Intranet, Local Area Network (LAN), Wide Area Network (WAN), Internet, and the like. Further, the network is either a dedicated network or a shared network. The shared network represents an association of the different types of networks that uses a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), and the like.

[0042] In an embodiment, the non-wearable device(s) and the wearable device(s) 108 of the system 100 are configured to ensure authorized usage check and transmission security check performed by the subsystem-A 106-A, where the subsystem-A is configured to authenticate and register the one or more user devices 108 using the unique device identifier to encode data, store data, enable transmission security check, transmission quality check, and to transmit the encoded data to the subsystem-B.

[0043] In another embodiment, the subsystem-B is configured to receive and encode the received data from the subsytem-A106-A, where the subsytem-B 106-B is configured to encode and transmit each stream specific to each registered device 108, wherein the encoded data restricts unauthorized access to the transmitted data. The encoded data can include audio data, video data, and the likes.

[0044] In an embodiment, the one or more user devices 108 are configured to ensure authorized usage check and transmission security check performed by the subsystem-A, where the encoded data is seamlessly decoded and streamed to the non-wearable device(s) and the user wearable device(s) 108 based on occurrence of a data synchronization and passing of the transmission security check with permitted usage of data.

[0045] In an embodiment, the subsystem-A 106-A is configured to perform a multi layered encoding to detect unauthorized usage of data. The subsystem-A is configured to encode separate and specific the one or more user devices 108 and one or more transmissions by allocating an unique encoding identifier. The one or more user devices 108 and one or more transmissions can be traced along with location through which data is unauthorized used. Further, the subsystem-A is configured to interrupt the transmission of encoded data based on faults detected in the security of transmission of encoded data.

[0046] In another embodiment, the subsystem-A 106-A includes a feedback loop (not shown in figure). The feedback loop is incorporated in the subsystem-A 106-A in order to monitor the changes occurring in the system 100. For instance, when the subsystem-A 106-A provides encoded data to a user(s) via the one or more user devices, then the feedback loop is configured to monitor and receive the activities performed by the user(s) by using the one or more user devices of the subsystem-A 106-A. Finally, the feedback loop updates the subsystem-A 106-A regarding the status of the particular encoded data which has been accessed by the one or more user devices. The feedback loop of the subsystem-A 106-A plays a prominent role in the system 100 by updating the status of every transmission to the subsystem-A 106-A which has been conducted.

[0047] FIG. 2 illustrates an exemplary architecture 200 of the proposed system 100 for controlling digital content viewership, in accordance with an embodiment of the present disclosure.

[0048] As illustrated in FIG.2, an exemplary architecture 200 of the proposed system 100. The system architecture 200 comprises one or more processor(s) 202. The one or more processor(s) 202 are implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, logic circuitries, and/or any devices that manipulate data based on operational instructions. Among other capabilities, one or more processor(s) 202 are configured to fetch and execute computer-readable instructions stored in a memory of the computing unit. The memory 204 stores one or more computer-readable instructions or routines, which are fetched and executed to create or share the data units over a network service. Memory 204 comprises any non-transitory storage device comprising, for example, volatile memory such as RAM, or non-volatile memory such as EPROM, flash memory, and the like.

[0049] In an embodiment, the system 100 also comprises an interface(s) 206. The interface(s) 206 comprises a variety of interfaces, for example, interfaces for data input and output devices referred to as I/O devices, storage devices, and the like. The interface(s) 206 facilitates communication of the second computing unit 106 with various devices coupled to the second computing unit 106. The interface(s) 206 also provides a communication pathway for one or more components of the second computing unit. Examples of such components comprise, but are not limited to, processing engine(s) 208 and database 216. The Interface 206 comprises a platform for communication with the devices to read real-time data /write data or certificates in the second computing unit, and to communicate with the OEM backend. The interfaces 206 comprise Graphical interface that allows user to feed inputs, to type/write/ upload the data and certificates, and other software and hardware interfaces, for example, interfaces 206 for peripheral device(s), such as a keyboard, a mouse, an external memory, and a printer.

[0050] In an embodiment, the processing engine(s) 208 are implemented as a combination of hardware and programming (for example, programmable instructions) to implement one or more functionalities of the processing engine(s) 208. In the examples described herein, such combinations of hardware and programming may be implemented in several different ways. For example, the programming for the processing engine(s) 208 are processor-executable instructions stored on a non-transitory machine-readable storage medium, and the hardware for the processing engine(s) 208 comprises a processing resource (for example, one or more processors), to execute such instructions. In the present examples, the machine-readable storage medium stores instructions that, when executed by the processing resource, implement the processing engine(s) 208. In such examples, the second computing unit 106 comprises the machine-readable storage medium storing the instructions and the processing resource to execute the instructions, or the machine-readable storage medium may be separate but accessible to the computing unit and the processing resource. In other examples, the processing engine(s) 208 is implemented by electronic circuitry.

Database 222 comprises data that is either stored or generated as a result of functionalities implemented by any of the components of the processing engine(s).

[0051] In an embodiment, the processing engine(s) 208 comprises a device identifier unit 210, a transmission security check unit 212, an encoding identifier unit 214, a transmission quality check unit 216, a data unit 218, and other units (s) 220, but not limited to the likes. The other unit(s) 220 implements functionalities that supplement applications or functions performed by the system 100or the processing engine(s) 208. The data (or database 222) serves, amongst other things, as a repository for storing data processed, received, and generated by one or more of the units.

[0052] FIG. 3 illustrates an exemplary block diagram 300 implementing the mechanism for controlling digital content viewership, in accordance with an embodiment of the present disclosure.

[0053] In an embodiment, the block diagram 300 includes various essential components of the present invention such as a subsystem-A 106-A, one or more user devices 108. When the subsystem-A 106-A receives data either from websites or entities or satellite, the subsystem-A 106-A performs encoding on the received data and stores the data. Further, the subsystem-A 106-A is configured to authenticate the encoded data and perform the multilayered encoding data, where each and every transmission is encoded. Furthermore, the data is decoded and transmitted to the one or more user device 108.

[0054] FIG. 4 illustrates an exemplary flow diagram of steps involved in the proposed method 400 for controlling digital content viewership, in accordance with an embodiment of the present disclosure.

[0055] In an embodiment, at block 402, one or more user devices 108 are authenticated and registered by the subsystem-A 106-A using unique device identifier, where the each one or more user devices 108 are registered device. At block 404, the subsystem-A 106-A can be configured to receive and encode data, by enabling transmission security check, transmission quality check. The subsystem-A 106-A transmits the encoded data to the subsytem-B. At block 406, the subsystem-B streams and transmits the encoded data to each registered device, where the encoded data restricts unauthorized access to the transmitted data.

[0056] FIG.5 illustrates an exemplary computer system in which or with which embodiments of the present invention can be utilized in accordance with embodiments of the present disclosure.

[0057] Referring to FIG. 5, computer system includes an external storage device 510, a bus 520, a main memory 530, a read only memory 540, a mass storage device 550, communication port 560, and a processor 570. A person skilled in the art will appreciate that computer system may include more than one processor and communication ports. Examples of processor 570 include, but are not limited to, an Intel® Itanium® or Itanium 2 processor(s), or AMD® Opteron® or Athlon MP® processor(s), Motorola® lines of processors, FortiSOC™ system on a chip processors or other future processors. Processor 570 may include various modules associated with embodiments of the present invention. Communication port 560 can be any of an RS-232 port for use with a modem based dialup connection, a 10/100 Ethernet port, a Gigabit or 10 Gigabit port using copper or fiber, a serial port, a parallel port, or other existing or future ports. Communication port 660 may be chosen depending on a network, such a Local Area Network (LAN), Wide Area Network (WAN), or any network to which computer system connects.

[0058] In an embodiment, the memory 530 can be Random Access Memory (RAM), or any other dynamic storage device commonly known in the art. Read only memory 640 can be any static storage device(s) e.g., but not limited to, a Programmable Read Only Memory (PROM) chips for storing static information e.g., start-up or BIOS instructions for processor 670. Mass storage 560 may be any current or future mass storage solution, which can be used to store information and/or instructions. Exemplary mass storage solutions include, but are not limited to, Parallel Advanced Technology Attachment (PATA) or Serial Advanced Technology Attachment (SATA) hard disk drives or solid-state drives (internal or external, e.g., having Universal Serial Bus (USB) and/or Firewire interfaces), e.g. those available from Seagate (e.g., the Seagate Barracuda 7102 family) or Hitachi (e.g., the Hitachi Deskstar 7K1000), one or more optical discs, Redundant Array of Independent Disks (RAID) storage, e.g. an array of disks (e.g., SATA arrays), available from various vendors including Dot Hill Systems Corp., LaCie, Nexsan Technologies, Inc. and Enhance Technology, Inc.

[0059] In an embodiment, the bus 520 communicatively couples processor(s) 570 with the other memory, storage and communication blocks. Bus 520 can be, e.g. a Peripheral Component Interconnect (PCI) / PCI Extended (PCI-X) bus, Small Computer System Interface (SCSI), USB or the like, for connecting expansion cards, drives and other subsystems as well as other buses, such a front side bus (FSB), which connects processor 570 to software system.

[0060] In another embodiment, operator and administrative interfaces, e.g. a display, keyboard, and a cursor control device, may also be coupled to bus 520 to support direct operator interaction with computer system. Other operator and administrative interfaces can be provided through network connections connected through communication port 660. External storage device 510 can be any kind of external hard-drives, floppy drives, IOMEGA® Zip Drives, Compact Disc - Read Only Memory (CD-ROM), Compact Disc - Re-Writable (CD-RW), Digital Video Disk - Read Only Memory (DVD-ROM). Components described above are meant only to exemplify various possibilities. In no way should the aforementioned exemplary computer system limit the scope of the present disclosure.

[0061] If the specification states a component or feature "may", "can", "could", or "might" be included or have a characteristic, that particular component or feature is not required to be included or have the characteristic.

[0062] As used in the description herein and throughout the claims that follow, the meaning of "a," "an," and "the" includes plural reference unless the context clearly dictates otherwise. Also, as used in the description herein, the meaning of "in" includes "in" and "on" unless the context clearly dictates otherwise.

[0063] Moreover, in interpreting the specification, all terms should be interpreted in the broadest possible manner consistent with the context. In particular, the terms "comprises" and "comprising" should be interpreted as referring to elements, components, or steps in a non-exclusive manner, indicating that the referenced elements, components, or steps may be present, or utilized, or combined with other elements, components, or steps that are not expressly referenced. Where the specification claims refer to at least one of something selected from the group consisting of A, B, C….and N, the text should be interpreted as requiring only one element from the group, not A plus N, or B plus N, etc.

[0064] While the foregoing describes various embodiments of the invention, other and further embodiments of the invention may be devised without departing from the basic scope thereof. The scope of the invention is determined by the claims that follow. The invention is not limited to the described embodiments, versions or examples, which are comprised to enable a person having ordinary skill in the art to make and use the invention when combined with information and knowledge available to the person having ordinary skill in the art.

ADVANTAGES OF THE INVENTION

[0065] The proposed invention provides a simple, secure, and efficient system and method for controlling digital content viewership.

[0066] The proposed invention provides a simple, secure, and efficient system and method for streaming data seamlessly to user devices such as IoT devices, infotainment devices, gaming devices, and the likes.

[0067] The proposed invention efficiently, economically, and securely manages the authentication of the user devices, and multi layered encoding of the data.

[0068] The proposed invention restricts unauthorized access to the transmitted data.

I Claim:

1. A system (100) for controlling digital content viewership comprises:

one or more user devices (108) comprising unique device identifier, wherein each of the one or more user devices (108) are authenticated and registered by using the unique device identifier, wherein the each one or more user devices (108) are registered user device;

a subsystem-A(106-A) communicatively coupled to a subsystem-B (106-B), other subsystem-N(106-N), and the one or more user devices (108), wherein the subsystem-A (106-A) is configured to authenticate and register the one or more user devices (108) using the unique device identifier to encode data, store data, enable transmission security check, transmission quality check, and to transmit the encoded data to the subsystem-B (106-B); and

the subsystem-B (106-B) is communicatively coupled to the one or more user devices (108), wherein the subsytem-B is configured to receive and encode the received data from the subsytem-A, wherein the subsytem-B is configured to encoding and transmitting each stream specific to each registered device, wherein the encoded data restricts unauthorized access to the transmitted data.

2. The system (100) as claimed in claim 1, wherein the registered device comprises unique device identifier selected from a group comprising device id, device type, device location, IP address, IMEI number and a combination thereof.

3. The system (100) as claimed in claim 1, wherein the one or more user devices (108) includes non-wearable device(s) and wearable device(s), wherein the non-wearable device(s) and the wearable device(s) are configured to ensure authorized usage check and transmission security check performed by the subsystem-A (106-A).

4. The system (100) as claimed in claim 1, wherein the encoded data is seamlessly decoded and streamed to the non-wearable device(s) and the user wearable device(s) based on occurrence of a data synchronization and passing of the transmission security check with permitted usage of data.

5. The system (100) as claimed in claim 1, wherein the subsystem-A (106-A) is configured to perform a multi layered encoding to detect unauthorized usage of data, wherein separate and specific encoding is performed on the one or more user devices (108) and one or more transmissions by allocating an unique encoding identifier, wherein the one or more user devices (108) and one or more transmissions can be traced along with location through which data is unauthorized used.

6. The system (100) as claimed in claim 1, wherein the subsystem-A (106-A) is configured to interrupt the transmission of encoded data based on faults detected in the security of transmission of encoded data.

7. A method for controlling digital content viewership comprises:

authenticating and registering one or more user devices (108), by a subsystem-A (106-A), using unique device identifier, wherein the each one or more user devices (108) are registered device;

receiving and encoding data, by the subsystem-A (106-A), enable transmission security check, transmission quality check, and to transmit the encoded data to the subsytem-B; and

streaming and transmitting the encoded data, by the subsystem-B (106-B), to each registered device, wherein the encoded data restricts unauthorized access to the transmitted data.

8. The method as claimed in claim 7, wherein the registered device comprises unique device identifier selected from a group comprising device id, device type, device location, IP address, IMEI number and a combination thereof.

9. The method as claimed in claim 7, wherein the one or more user devices (108) includes non-wearable device(s) and wearable device(s), wherein the non-wearable device(s) and the wearable device(s) are configured to ensure authorized usage check and transmission security check performed by the subsystem-A (106-A).

10. The method as claimed in claim 7, wherein the encoded data is seamlessly decoded and streamed to the non-wearable device(s) and the user wearable device(s) based on occurrence of a data synchronization and passing of the transmission security check with permitted usage of data.

11. The method as claimed in claim 7, wherein a multi layered encoding is performed to detect unauthorized usage of data, wherein separate and specific encoding is performed on the one or more user devices (108) and one or more transmissions by allocating an unique encoding identifier, wherein the one or more user devices (108) and one or more transmissions can be traced along with location through which data is unauthorized used.

12. The method as claimed in claim 8, wherein the subsystem-A (106-A) is configured to interrupt the transmission of encoded data based on faults detected in the security of transmission of encoded data.

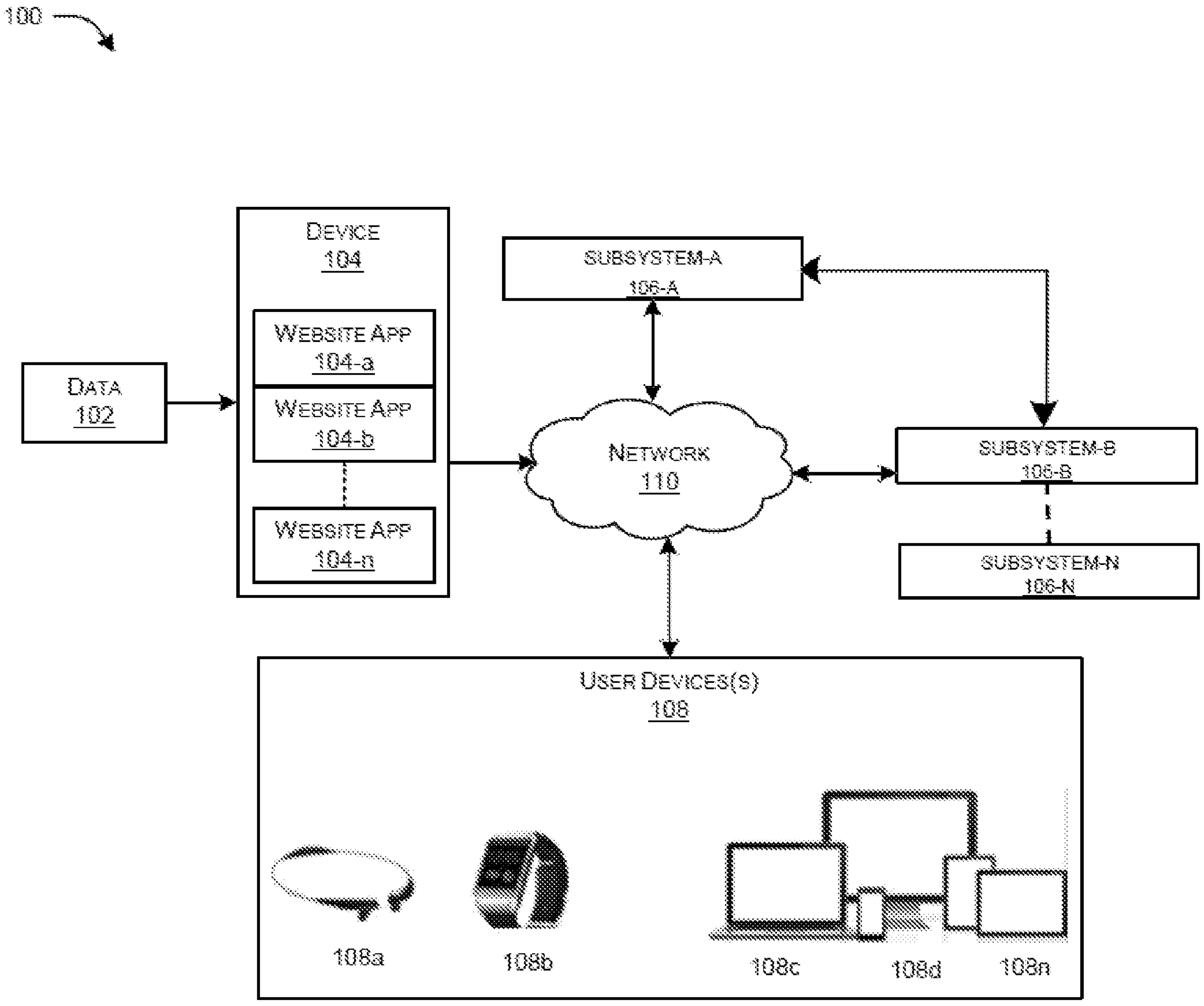
100
DEVICE
104
WEBSITE APP
104-a
WEBSITE APP
104-b
WEBSITE APP
104-n
DATA
102
SUBSYSTEM-A
106-A
NETWORK
110
SUBSYSTEM-B
106-B
SUBSYSTEM-N
106-N
USER DEVICES(S)
108
108a
108b
108c
108d
108n

FIG. 1A

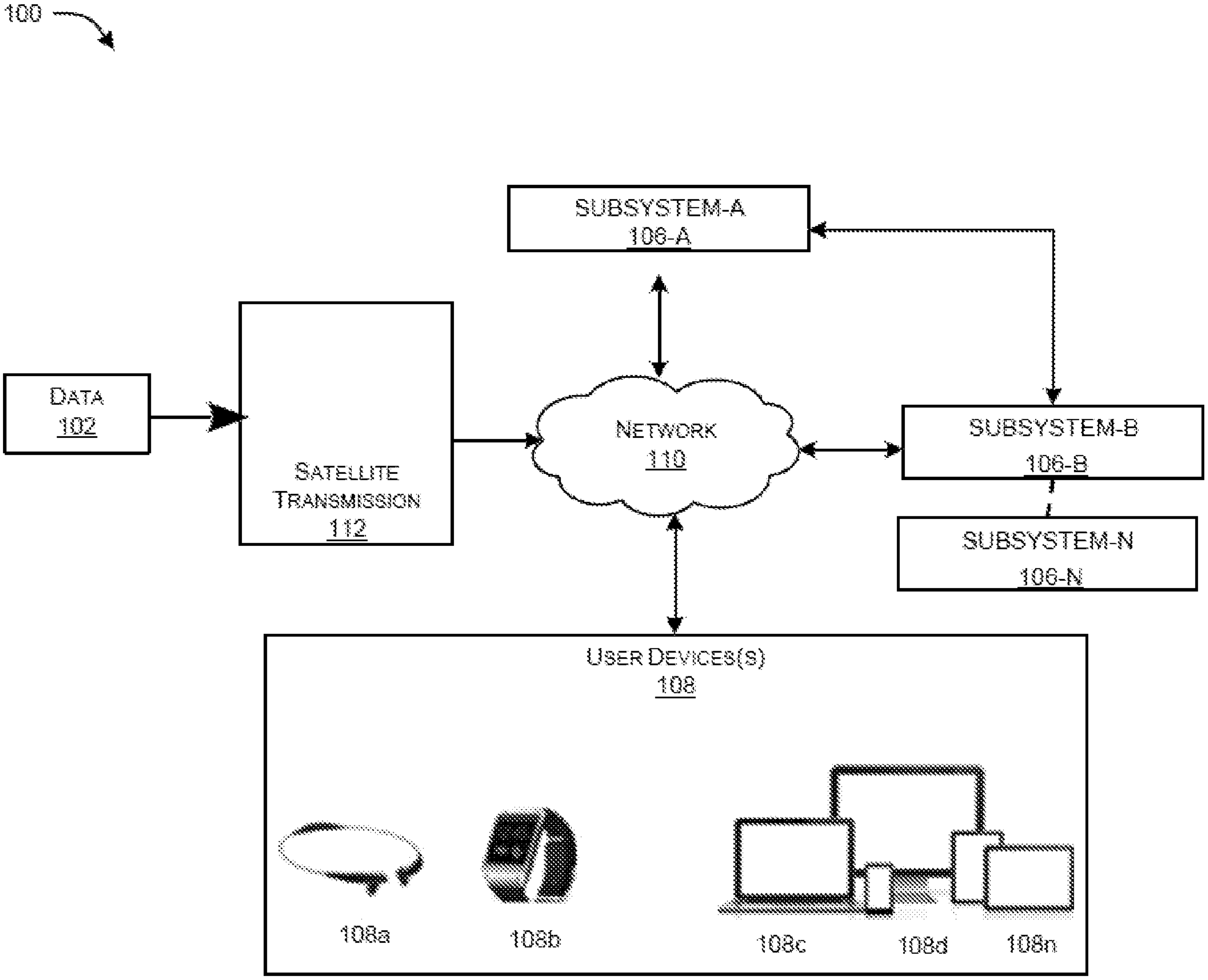
100
SUBSYSTEM-A
106-A
DATA
102
SATELLITE
TRANSMISSION
112
NETWORK
110
SUBSYSTEM-B
106-B
SUBSYSTEM-N
106-N
USER DEVICES(S)
108
108a
108b
108c
108d
108n

FIG. 1B

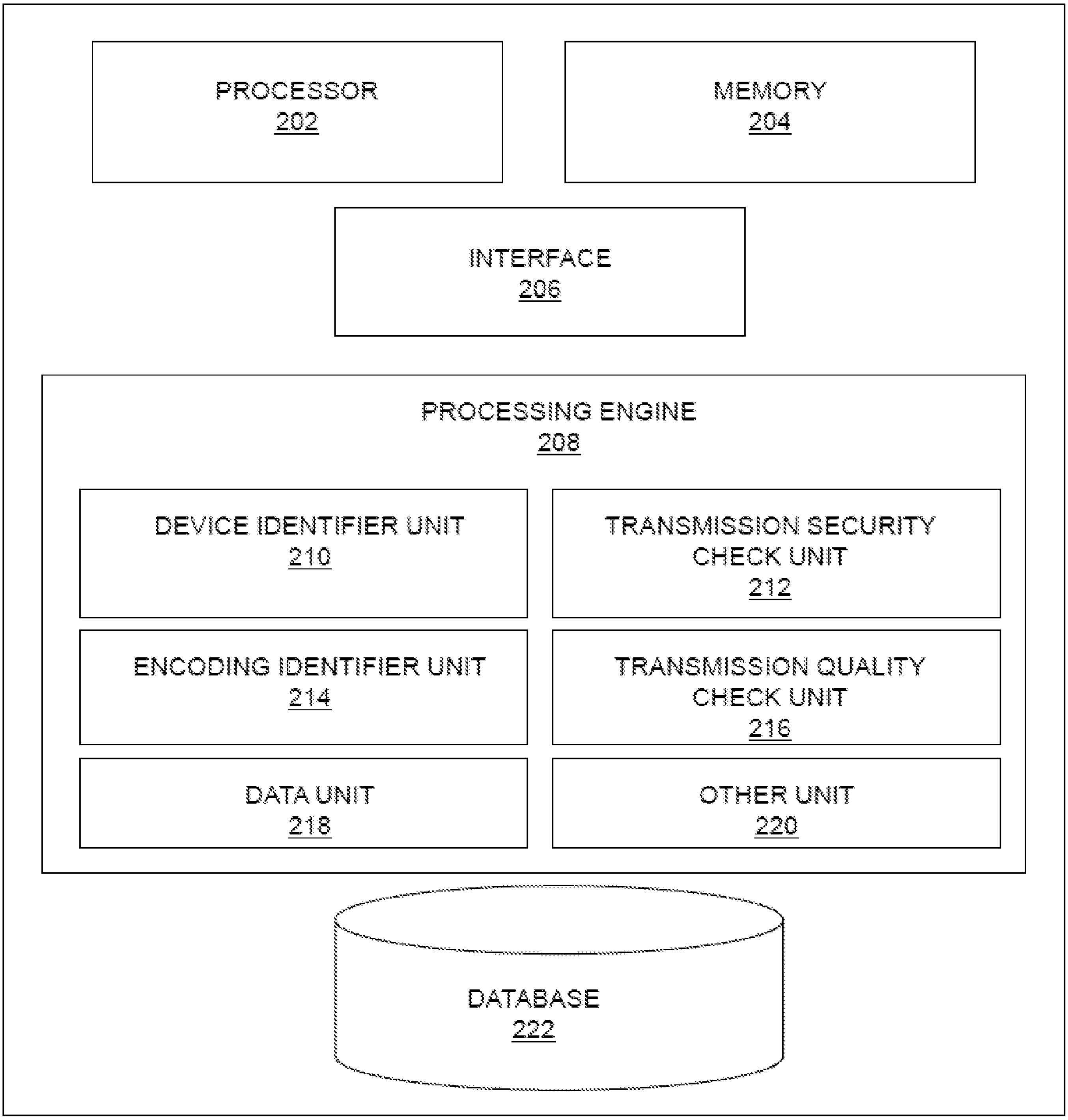
PROCESSOR
202
MEMORY
204
INTERFACE
206
PROCESSING ENGINE
208
DEVICE IDENTIFIER UNIT
210
TRANSMISSION SECURITY CHECK UNIT
212
ENCODING IDENTIFIER UNIT
214
TRANSMISSION QUALITY CHECK UNIT
216
DATA UNIT
218
OTHER UNIT
220
DATABASE
222

FIG. 2

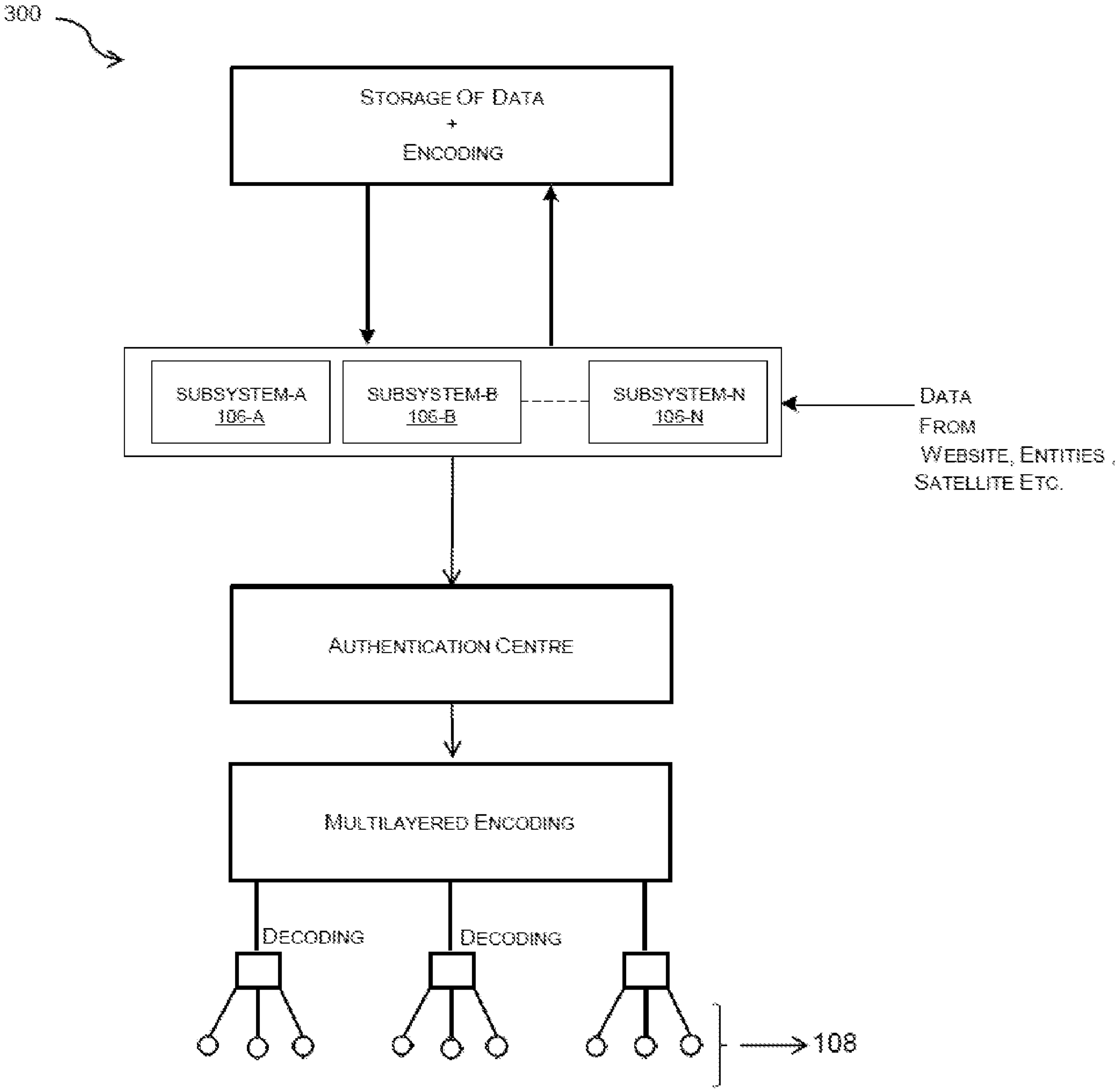
300
Storage Of Data
+
Encoding
Subsystem-A
106-A
Subsystem-B
106-B
Subsystem-N
106-N
Data
From
Website, Entities ,
Satellite Etc.
Authentication Centre
Multilayered Encoding
Decoding
Decoding
108

FIG. 3

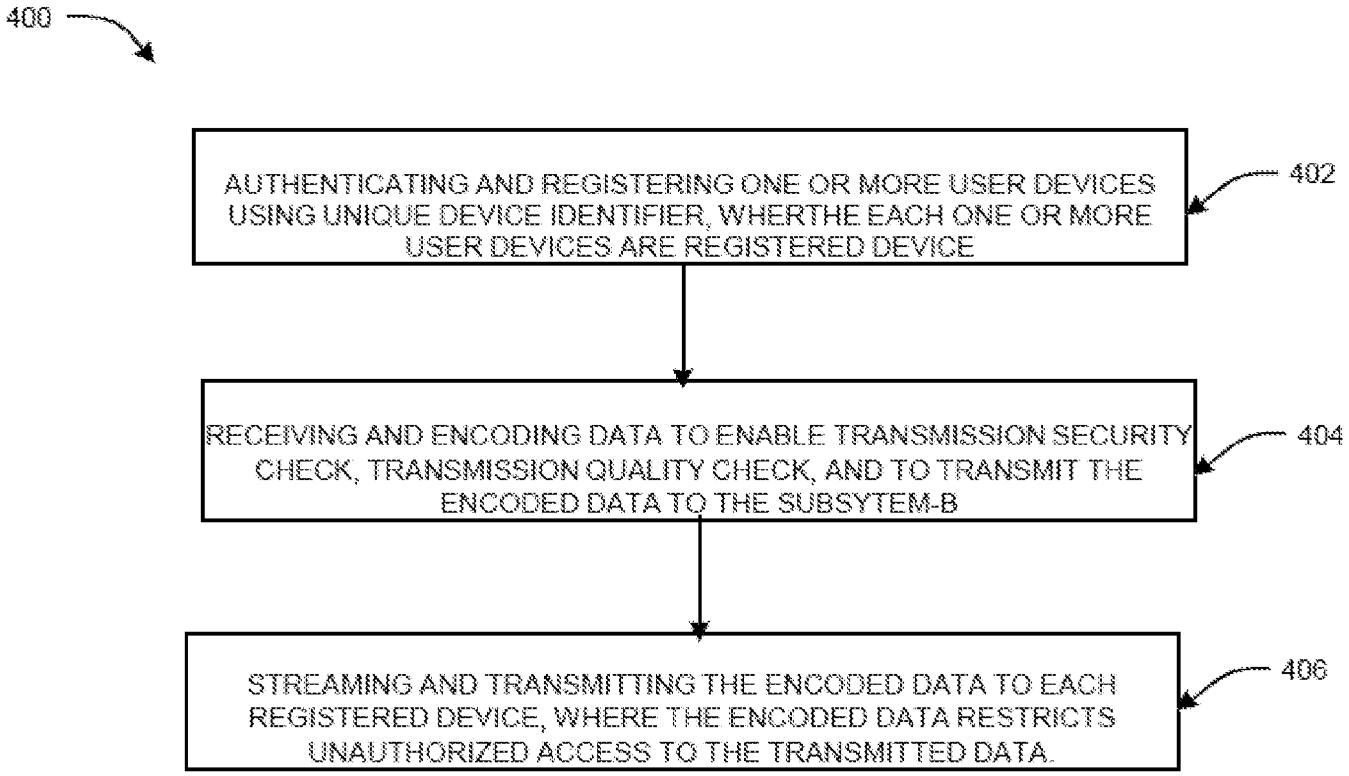
400
AUTHENTICATING AND REGISTERING ONE OR MORE USER DEVICES USING UNIQUE DEVICE IDENTIFIER, WHERTHE EACH ONE OR MORE USER DEVICES ARE REGISTERED DEVICE
402
RECEIVING AND ENCODING DATA TO ENABLE TRANSMISSION SECURITY CHECK, TRANSMISSION QUALITY CHECK, AND TO TRANSMIT THE ENCODED DATA TO THE SUBSYTEM-B
404
STREAMING AND TRANSMITTING THE ENCODED DATA TO EACH REGISTERED DEVICE, WHERE THE ENCODED DATA RESTRICTS UNAUTHORIZED ACCESS TO THE TRANSMITTED DATA.
406

FIG. 4

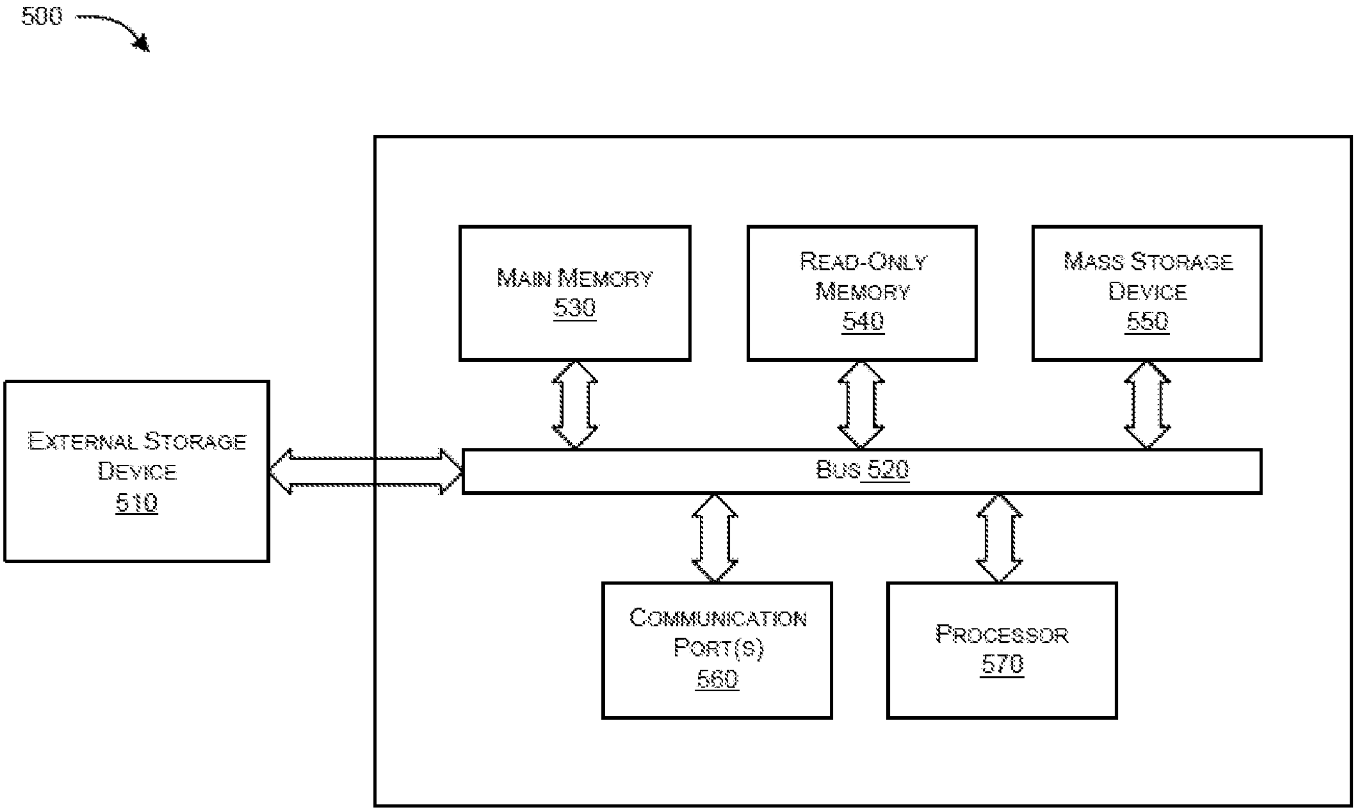
500
External Storage Device 510
Main Memory 530
Read-Only Memory 540
Mass Storage Device 550
Bus 520
Communication Port(s) 560
Processor 570

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB2022/061245

A. CLASSIFICATION OF SUBJECT MATTER

H04N21/25,H04N21/43,H04N21/80 Version=2023.01

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)

H04N, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database consulted during the international search (name of database and, where practicable, search terms used)

Databases:- Patseer, IPO Internal Database
Keywords:-control, digital, stream , wearable

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US11222298B2 (Daniel H. Abelow [US])(11 Jan 2022) (11/01/2022) Claims 1-37, figures 31,66,87,172, column 265, lines 4-21	1-12
T	US2022272091A1(AGRAWAL SAGAR[IN])(25 Aug 2022) (25/08/2022) the whole document	1-12

□ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"D" document cited by the applicant in the international application

"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

"&" document member of the same patent family

Date of the actual completion of the international search 23-02-2023	Date of mailing of the international search report 23-02-2023
Name and mailing address of the ISA/ Indian Patent Office Plot No.32, Sector 14,Dwarka,New Delhi-110075 Facsimile No.	Authorized officer Shubhanshu Gautam Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2022/061245

Citation	Pub.Date	Family	Pub.Date
US 11222298 B2	11-01-2022	US 9183560 B2	10-11-2015
		WO 2011149558 A2	01-12-2011