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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 April 2022 (28.04.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/087206 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/14* (2006.01)

(21) International Application Number:
PCT/US2021/055956

(22) International Filing Date:
21 October 2021 (21.10.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/104,795 23 October 2020 (23.10.2020) US

(71) Applicant: **SECTURION SYSTEMS, INC.** [US/US]; 520 North Marketplace Dr., Suite 203, Centerville, Utah 84014 (US).

(72) Inventors: **TAKAHASHI, Richard J.**; 1510 N 2075 E, LAYTON, Utah 84040 (US). **ABEL, Timothy Paul**; 170 EDGEHILL CIRCLE, FRUIT HEIGHTS, Utah 84037 (US). **NIELSON, Benjamin Kirk**; 2372 S CAMERON DR., WEST HAVEN, Utah 84401 (US).

(74) Agent: **NEEL, Bruce T.** et al.; Greenberg Traurig (PHX) c/o: Greenberg Traurig, 77 West Wacker Drive, Suite 3100, Chicago, Illinois 60601 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, 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, 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, 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).

Declarations under Rule 4.17:
- *as to the identity of the inventor (Rule 4.17(i))*
- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

(54) **Title:** MULTI-INDEPENDENT LEVEL SECURITY FOR HIGH PERFORMANCE COMPUTING AND DATA STORAGE SYSTEMS

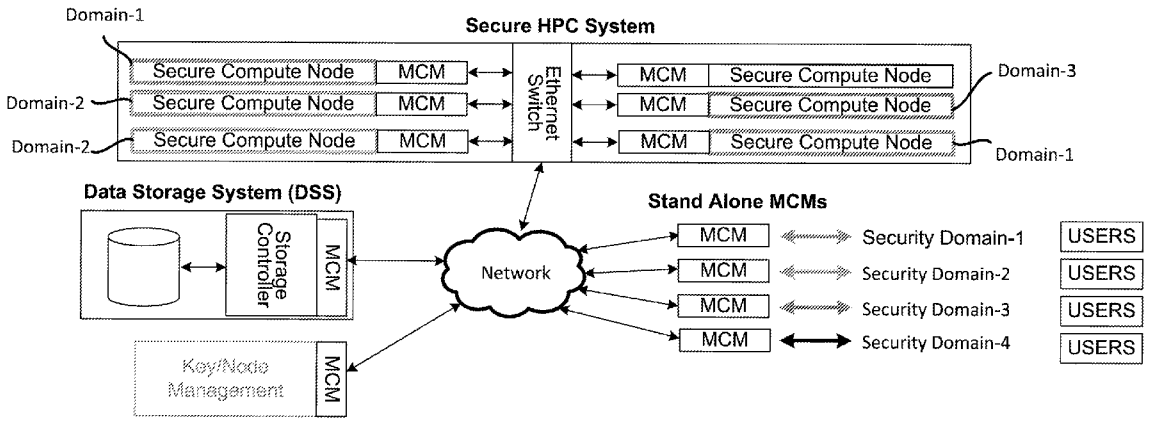


FIG. 1

(57) **Abstract:** Systems, methods, and apparatus for a MILS HPC, data storage system (DSS) system architecture that incorporates a multi-crypto module (MCM) to provide end- to-end multi-independent level security (MILS) protection. Configuration of each MCM enables a high performance computing (HPC) resource to compute different security domains with the associated security level keys from a key/node manager. The HPC resource can be dynamically re-allocated to different security level domain(s) by the key/node manager. In one embodiment, the DSS stores encrypted data regardless of the domains.

[Continued on next page]

WO 2022/087206 A1

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

MULTI-INDEPENDENT LEVEL SECURITY FOR HIGH PERFORMANCE COMPUTING AND DATA STORAGE SYSTEMS

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Application Serial No. 63/104,795, filed October 23, 2020, entitled "MULTI-INDEPENDENT LEVEL SECURITY FOR HPC AND DATA STORAGE SYSTEM ARCHITECTURE OVER ETHERNET NETWORK," by Takahashi et al., the entire contents of which application is incorporated by reference as if fully set forth herein.

FIELD OF THE TECHNOLOGY

[0002] At least some embodiments disclosed herein relate to computing systems and data storage systems in general, and more particularly, but not limited to multi-level security for such systems (e.g., systems having devices that communicate over Ethernet networks).

BACKGROUND

[0003] Existing military-intelligence and other secure computing systems require physically isolated, protected data storage sites for each level of classified data. This requires separated storage systems for each level of classified data. This is a costly method to store data and access data. In addition, sharing cross-domain information (e.g., sharing data between classified systems) is slow and cumbersome in a world where minutes can make a significant difference in the results achieved.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The embodiments are illustrated by way of example and not limitation in the figures of the accompanying drawings in which like references indicate similar elements.

[0005] **FIG. 1** shows a system architecture for an HPC and DSS system that uses multiple-cryptographic modules (MCMs) (sometimes simply referred to as "multi-crypto modules"), in accordance with some embodiments.

[0006] **FIG. 2** shows a secure compute node with a multiple cryptographic module (MCM), in accordance with some embodiments.

[0007] **FIG. 3** shows a stand-alone MCM, in accordance with some embodiments.

[0008] **FIGs. 4-9** show various embodiments that implement the above system architecture.

DETAILED DESCRIPTION

[0009] The following disclosure describes various embodiments for multi-level independent security as implemented in computing systems (e.g., high performance computing (HPC) systems and/or data storage systems (DSS)). At least some embodiments herein relate to configuring secure (e.g., multiple secured levels) communications over networks between hardware devices in such systems (e.g., Ethernet networks).

[0010] Procuring and maintaining compute, storage, and networking resources for each isolated security domain in a computing or data storage system is costly and redundant. This can cause technical problems including the need for excessive hardware, complicated procedures, and/or inefficiency or unreliability in operation. This can reduce system performance and/or lead to a failure of systems in some cases.

[0011] Various embodiments described herein provide a technological solution to the above and other problems. In one embodiment, a multi-level security architecture allows dynamic security provisioning of HPC compute resources, as well as a method to securely share the same physical data storage and network hardware. This architecture uses one or more multi-crypto modules (MCMs). This is accomplished by providing a coupling of a compute resource, which has the ability to be completely sanitized, with a trusted MCM. The MCM only decrypts and passes on data/information that the MCM is keyed for, and only if the data/information passes an integrity check. In one embodiment, the compute resource obtains all data from an encrypted trusted source. This data includes, but is not limited to, boot code, operating systems, applications, and/or communications with other nodes.

[0012] In various embodiments, an MCM is a device that encrypts all data types that are input to the MCM according to the detected application metadata. In one embodiment, each application requires corresponding cipher, keys, and sensitivity to protocol metadata. In one embodiment, any undetermined data type can be handled

through rejection, or a default encryption cipher, key, and metadata handling scheme.

[0013] **FIG. 1** shows a block diagram for a MILS HPC data storage system (DSS) system architecture that incorporates the MCM to provide an end-to-end multi-independent level security (MILS) protection. Configuration of each MCM enables nodes within the single HPC resource to compute different security domains with the associated security level keys from a key/node manager. The HPC resource can be dynamically re-allocated to one or more different security level domain(s) by the key/node manager. In one embodiment, the DSS only stores encrypted data regardless of the domains.

[0014] Re-allocation is accomplished by command from the node manager through a secure connection to the node. When reallocation is commanded, a clearing procedure occurs (sanitization), followed by an identity assignment. Based on the identity assignment, keys can be distributed to the MCM in the node allowing the node to communicate with other components of like identity assignment.

[0015] In one embodiment, a system uses a MACsec appliance and a file and block-level data at rest encryptor (DARE), each supporting data rates of, for example, 100 Gbps or greater. In one example, this network and encryption technology can be scaled up to 400 Gbps, or to terabit speeds. These components can be consolidated into the multi-crypto module to provide both data-at-rest and data-in-transit encryption.

[0016] The multi-crypto module (MCM) is a component used as a cryptographic processing element in the system. It can be built as a network interface card in a PCIe form factor as shown in **FIG. 2**. The MCM provides high-speed I/O over PCIe to the server, high-speed Ethernet to the black network, and additional ports for keying and remote management. In one embodiment, the MCM provides a hardware-enforced, EMSEC-enclosed information assurance and cryptographic boundary consisting of MACsec and the data at rest encryptor (DARE) to create a secure, provisioned enclave. The MACsec functionality provides confidentiality and integrity as it establishes a secure Ethernet tunnel with other nodes provisioned into a specific domain. Other transport encryption protocols such as IPSec, or TLS can also be supported. The MCM has access to the server through IPMI to sanitize the system when deprovisioning or changing security levels (e.g. clear volatile RAM contents, reboot the system, verify sanitization, load a new operating system, etc.).

[0017] SFP as illustrated in **FIG. 2** represents a small form-factor pluggable transceiver. In one example, this is an industry standard modular slot for a media specific transceiver. The SFP is one of various other interfaces that can be used.

[0018] In one embodiment, the MCM DARE is a file and block-level encryptor that encrypts individual files over network filesystems such as NFS or CIFS, or blocks over iSCSI. Block-level encryption allows any filesystem to be used on the server and still provide confidentiality. Any file or data transfer through the MCM is encrypted before it reaches the black network. The multi-crypto module can be instantiated as a network card interfacing with a computer's native I/O interface (e.g., PCI-Express) as shown in **FIG. 2**, or instantiated as a standalone unit that provides an Ethernet interface on the red side, as shown in **FIG. 3**. The key/node management can be done through either the black network or a separate management interface as shown in **FIG. 2** and **FIG. 3**.

[0019] In one embodiment, the key/node manager contains the primary MCM and has connectivity to all other MCMs in the MILS system. This node is responsible for provisioning each MCM to the configured security level, providing or activating appropriate device credentials, and managing keys for MACsec and DARE. Once an MCM has credentials matching the provisioned security level, it can request keys over the network. In one example, KMIP will be used to get keying material from an HSM (e.g., hardware security module). In one example, the KMIP is a Key Management Interoperability Protocol, which is a communication protocol for manipulating keys on a key management server. In other examples, other key management protocols can be used. In one example, the key manager uses a key communication protocol other than KMIP.

[0020] In one embodiment, the data storage system (DSS) consists of a COTS storage controller with an MCM to provide MACsec connectivity to each of the security levels in the system. Before data is received at the DSS, the DARE functionality of the originating MCM will have encrypted the data with a key unique to the provisioned security level. This provides the cryptographic separation of the MILS data that can then be written to the shared storage media. The MCM allows for multiple MACsec connectivity associations for each security level, which in turn provides a redundant check to ensure data separation.

[0021] In one embodiment, the secure HPC system consists of multiple servers installed with the MCM designated as the "Secure Compute Node" in **FIG. 2**. These

servers contain no non-volatile memory, and for example, PXE boot from the DSS. Each node in the secure HPC system can be allocated and provisioned as needed for computational load at each security domain. The MCM will perform the DARE and MACsec functions. The MACsec functionality provides a secure link to other nodes at the same security level and to the DSS. The DARE functionality encrypts data on the way to the DSS and decrypts it on the way back. Each HPC secure compute node in the cluster is sanitized directly after use through the IPMI function by removing the power to clear all of the volatile memory components contained in the node and verify the compute node is in a sanitized state.

[0022] Various examples of tracing data through the MILS HPC DSS System are now described below.

[0023] 1. User Terminal through MCM to the DSS: A user's file is transmitted from a security domain to the MCM. The MCM recognizes the file as one of the storage file types and encrypts it using the DARE function. The encrypted file is then transferred through the secure MACsec tunnel to the DSS. The encrypted file is then written to the storage media.

[0024] 2. User Terminal through MCM to the HPC System: A user's data is transmitted to the MCM, and then to the HPC node through the MACsec tunnel.

[0025] 3. HPC System to DSS: An HPC file is sent to the MCM over PCIe. The MCM recognizes the file as one of the storage file types and encrypts it using the DARE function. The encrypted storage file is then passed to the DSS through the MACsec tunnel. The encrypted file is then written to the storage media.

[0026] In various embodiments, a MILS HPC DSS system uses the MCM design above. This system leverages, for example, 100 Gbps DARE and 100 Gbps MACSec components for use with the MCM, which enables a dynamically-reallocated HPC center and single data storage system. The system includes MCMs, HPC, DSS, and a key manager system.

[0027] In one embodiment, the key/node manager configures each MCM through a secure out-of-band connection. In one example, there are three actions performed by the key/node manager each time a node is reallocated. First, a clearing procedure is commanded, next an identity is assigned, and finally keys are issued to the MCM.

[0028] **FIG. 4** shows an example application for the MILS network appliance as a cross-domain viewer (e.g., presented on a user display of a computing device, as

illustrated). In this embodiment, a local storage is preloaded with encrypted information over an external network. Multiple MCM elements are then used to provide cryptographic isolation between CPUs at different classification levels, yet sharing a single encrypted data store.

[0029] **FIG. 5** shows an example network with multiple MCM applications working to form a secure multi-level security data center with application connections. In this embodiment, HPC cluster nodes can be assigned to different networks while networking, infrastructure, and storage are shared. The MCM maintains cryptographic network isolation and cryptographic isolation between data elements on the data storage unit (e.g., a data repository managed by a computing device). This allows elements to be geographically distanced, while maintaining strong cryptographic security.

[0030] **FIG. 6** shows a detailed view of a tactical network encryptor. In this embodiment, the MCM low speed interfaces (e.g., 10 Mbps to 1Gbps) are used for the red and black network interfaces. Key fill can be done through either the red network, black network, or a dedicated key fill interface. This allows for a significantly smaller unit that can be used in space and weight-constrained situations.

[0031] **FIG. 7** shows a single multi-level data center that can be used to replace any number of traditionally-isolated security domain data centers including isolated high performance computing systems. Because peak loads can be shared in the multi-level data center, the amount of resources required in the multi-level data center is less than the aggregate amount of resources required in isolated data centers. This results in capital and/or recurring cost savings.

[0032] **FIG. 8** shows how isolated domain specific data stores can be consolidated into a single network attached data store.

[0033] **FIG. 9** shows how multiple complete security domain specific isolated HPC systems can be consolidated to a single system using MCM technology as described herein.

Variations

[0034] In one embodiment, a networked computing system (e.g., including HPC and DSS as described above) includes: a plurality of data input ports, each port corresponding to one of a plurality of different levels of security classification; a

security device (e.g., an MCM as described above), configured for cryptographic processing, coupled to receive incoming data from each of the plurality of input ports, wherein the incoming data includes first data having a first classification level, wherein the security device comprises a plurality of cryptographic modules, wherein each cryptographic module is configured to perform security processing for at least one of the different levels of security classification, and wherein each of the cryptographic modules comprises a cryptographic engine configured for data processing using a systolic array; and a key manager configured to select a first set of keys from a plurality of key sets, each of the key sets corresponding to one of the different levels of security classification, wherein the first set of keys is used by the security device to encrypt the first data; wherein the security device is further configured to send the encrypted first data to a storage device.

[0035] In one embodiment, each multiple cryptographic module (MCM) as implemented above (e.g., each MCM in **FIGs. 1-3**) is a cryptographic module as described in U.S. Non-Provisional Application Serial No. 14/177,392, filed February 11, 2014, entitled "SECURITY DEVICE WITH PROGRAMMABLE SYSTOLIC-MATRIX CRYPTOGRAPHIC MODULE AND PROGRAMMABLE INPUT/OUTPUT INTERFACE," by Richard J. Takahashi, the entire contents of which application is incorporated by reference as if fully set forth herein.

[0036] In one embodiment, each security device above is configured for use in the HPC system and/or data storage system as described herein (e.g., as described for an MCM above). Each security device is configured to provide a different security level for each of several domains. Each domain is defined by a key manager.

[0037] In one embodiment, data and/or file objects are securely communicated over the Ethernet network in the HPC system and data storage system as described in U.S. Non-Provisional Application Serial No. 15/688,743, filed August 28, 2017, entitled "CLOUD STORAGE USING ENCRYPTION GATEWAY WITH CERTIFICATE AUTHORITY IDENTIFICATION," by Anderson et al., the entire contents of which application is incorporated by reference as if fully set forth herein.

[0038] In one embodiment, the MILS network appliance with different security domains and the use of the MCM above can be used with or in a system as described in U.S. Non-Provisional Application Serial No. 15/332,059, filed October 24, 2016, entitled "MULTI-INDEPENDENT LEVEL SECURE (MILS) STORAGE

ENCRYPTION," by Richard J. Takahashi, the entire contents of which application is incorporated by reference as if fully set forth herein.

[0039] In one embodiment, the MILS network appliance with different security domains and the use of the MCM above can be used with or in a system as described in U.S. Non-Provisional Application Serial No. 14/198,097, filed March 5, 2014, entitled "MULTI-LEVEL INDEPENDENT SECURITY ARCHITECTURE," by Richard J. Takahashi, the entire contents of which application is incorporated by reference as if fully set forth herein.

Closing

[0040] The disclosure includes various devices which perform the methods and implement the systems described above, including data processing systems which perform these methods, and computer-readable media containing instructions which when executed on data processing systems cause the systems to perform these methods.

[0041] The description and drawings are illustrative and are not to be construed as limiting. Numerous specific details are described to provide a thorough understanding. However, in certain instances, well-known or conventional details are not described in order to avoid obscuring the description. References to one or an embodiment in the present disclosure are not necessarily references to the same embodiment; and, such references mean at least one.

[0042] As used herein, "coupled to" or "coupled with" generally refers to a connection between components, which can be an indirect communicative connection or direct communicative connection (e.g., without intervening components), whether wired or wireless, including connections such as electrical, optical, magnetic, etc.

[0043] Reference in this specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the disclosure. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Moreover, various features are described which may be exhibited by some embodiments and not by others. Similarly, various requirements are described which may be

requirements for some embodiments but not other embodiments.

[0044] In this description, various functions and/or operations may be described as being performed by or caused by software code to simplify description. However, those skilled in the art will recognize what is meant by such expressions is that the functions and/or operations result from execution of the code by one or more processing devices, such as a microprocessor, Application-Specific Integrated Circuit (ASIC), graphics processor, and/or a Field-Programmable Gate Array (FPGA). Alternatively, or in combination, the functions and operations can be implemented using special purpose circuitry (e.g., logic circuitry), with or without software instructions. Embodiments can be implemented using hardwired circuitry without software instructions, or in combination with software instructions. Thus, the techniques are not limited to any specific combination of hardware circuitry and software, nor to any particular source for the instructions executed by a computing device.

[0045] While some embodiments can be implemented in fully functioning computers and computer systems, various embodiments are capable of being distributed as a computing product in a variety of forms and are capable of being applied regardless of the particular type of computer-readable medium used to actually effect the distribution.

[0046] At least some aspects disclosed can be embodied, at least in part, in software. That is, the techniques may be carried out in a computing device or other system in response to its processing device, such as a microprocessor, executing sequences of instructions contained in a memory, such as ROM, volatile RAM, non-volatile memory, cache or a remote storage device.

[0047] Routines executed to implement the embodiments may be implemented as part of an operating system, middleware, service delivery platform, SDK (Software Development Kit) component, web services, or other specific application, component, program, object, module or sequence of instructions (sometimes referred to as computer programs). Invocation interfaces to these routines can be exposed to a software development community as an API (Application Programming Interface). The computer programs typically comprise one or more instructions set at various times in various memory and storage devices in a computer, and that, when read and executed by one or more processors in a computer, cause the computer to perform operations necessary to execute elements involving the various

aspects.

[0048] A computer-readable medium can be used to store software and data which when executed by a computing device causes the device to perform various methods. The executable software and data may be stored in various places including, for example, ROM, volatile RAM, non-volatile memory and/or cache. Portions of this software and/or data may be stored in any one of these storage devices. Further, the data and instructions can be obtained from centralized servers or peer to peer networks. Different portions of the data and instructions can be obtained from different centralized servers and/or peer to peer networks at different times and in different communication sessions or in a same communication session. The data and instructions can be obtained in entirety prior to the execution of the applications. Alternatively, portions of the data and instructions can be obtained dynamically, just in time, when needed for execution. Thus, it is not required that the data and instructions be on a computer-readable medium in entirety at a particular instance of time.

[0049] Examples of computer-readable media include, but are not limited to, recordable and non-recordable type media such as volatile and non-volatile memory devices, read only memory (ROM), random access memory (RAM), flash memory devices, solid-state drive storage media, removable disks, magnetic disk storage media, optical storage media (e.g., Compact Disk Read-Only Memory (CD ROMs), Digital Versatile Disks (DVDs), etc.), among others. The computer-readable media may store the instructions. Other examples of computer-readable media include, but are not limited to, non-volatile embedded devices using NOR flash or NAND flash architectures. Media used in these architectures may include un-managed NAND devices and/or managed NAND devices, including, for example, eMMC, SD, CF, UFS, and SSD.

[0050] In general, a non-transitory computer-readable medium includes any mechanism that provides (e.g., stores) information in a form accessible by a computing device (e.g., a computer, mobile device, network device, personal digital assistant, manufacturing tool having a controller, any device with a set of one or more processors, etc.). A “computer-readable medium” as used herein may include a single medium or multiple media (e.g., that store one or more sets of instructions).

[0051] In various embodiments, hardwired circuitry may be used in combination with software and firmware instructions to implement the techniques. Thus, the

techniques are neither limited to any specific combination of hardware circuitry and software nor to any particular source for the instructions executed by a computing device.

[0052] Various embodiments set forth herein can be implemented using a wide variety of different types of computing devices. As used herein, examples of a “computing device” include, but are not limited to, a server, a centralized computing platform, a system of multiple computing processors and/or components, a mobile device, a user terminal, a vehicle, a personal communications device, a wearable digital device, an electronic kiosk, a general purpose computer, an electronic document reader, a tablet, a laptop computer, a smartphone, a digital camera, a residential domestic appliance, a television, or a digital music player. Additional examples of computing devices include devices that are part of what is called "the internet of things" (IOT). Such "things" may have occasional interactions with their owners or administrators, who may monitor the things or modify settings on these things. In some cases, such owners or administrators play the role of users with respect to the "thing" devices. In some examples, the primary mobile device (e.g., an Apple iPhone) of a user may be an administrator server with respect to a paired “thing” device that is worn by the user (e.g., an Apple watch).

[0053] In some embodiments, the computing device can be a computer or host system, which is implemented, for example, as a desktop computer, laptop computer, network server, mobile device, or other computing device that includes a memory and a processing device. The host system can include or be coupled to a memory sub-system so that the host system can read data from or write data to the memory sub-system. The host system can be coupled to the memory sub-system via a physical host interface. In general, the host system can access multiple memory sub-systems via a same communication connection, multiple separate communication connections, and/or a combination of communication connections.

[0054] In some embodiments, the computing device is a system including one or more processing devices. Examples of the processing device can include a microcontroller, a central processing unit (CPU), special purpose logic circuitry (e.g., a field programmable gate array (FPGA), an application specific integrated circuit (ASIC), etc.), a system on a chip (SoC), or another suitable processor.

[0055] In some embodiments, each MCM is a computing device, or includes a processing device. Other components of the HPC or DSS system can be

implemented using computing devices.

[0056] Although some of the drawings illustrate a number of operations in a particular order, operations which are not order dependent may be reordered and other operations may be combined or broken out. While some reordering or other groupings are specifically mentioned, others will be apparent to those of ordinary skill in the art and so do not present an exhaustive list of alternatives. Moreover, it should be recognized that the stages could be implemented in hardware, firmware, software or any combination thereof.

[0057] In the foregoing specification, the disclosure has been described with reference to specific exemplary embodiments thereof. It will be evident that various modifications may be made thereto without departing from the broader spirit and scope as set forth in the following claims. The specification and drawings are, accordingly, to be regarded in an illustrative sense rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A system comprising:
   at least one processing device; and
   at least one memory containing instructions configured to instruct the at least one processing device to configure cryptographic modules, each module configured to encrypt communications in a networked system, each module configured to support different security levels for each of multiple domains, and each domain defined by a key manager.

2. A method comprising configuring cryptographic modules, each module configured to encrypt communications in a networked system, each module configured to support different security levels for each of multiple domains.

3. A non-transitory computer-readable medium storing instructions which, when executed on at least one computing device, cause the at least one computing device to configure cryptographic modules in a network, each module configured to encrypt communications in the network.

4. A system comprising a plurality of MCMs to provide end-to-end multi-independent level security (MILS), wherein each MCM is configured to enable computation of different security domains with associated security level keys from at least one key/node manager.

5. The system of claim 4, wherein the system is configured for dynamic re-allocation to different security level domain(s) by the key/node manager.

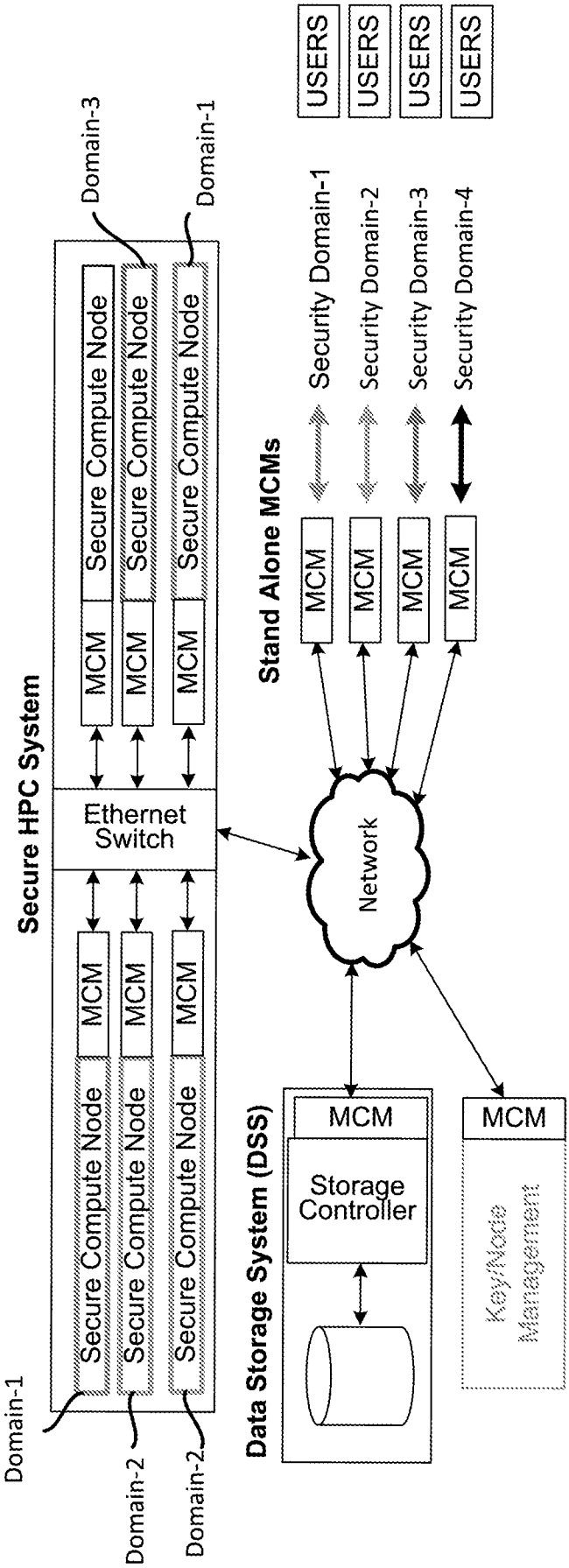
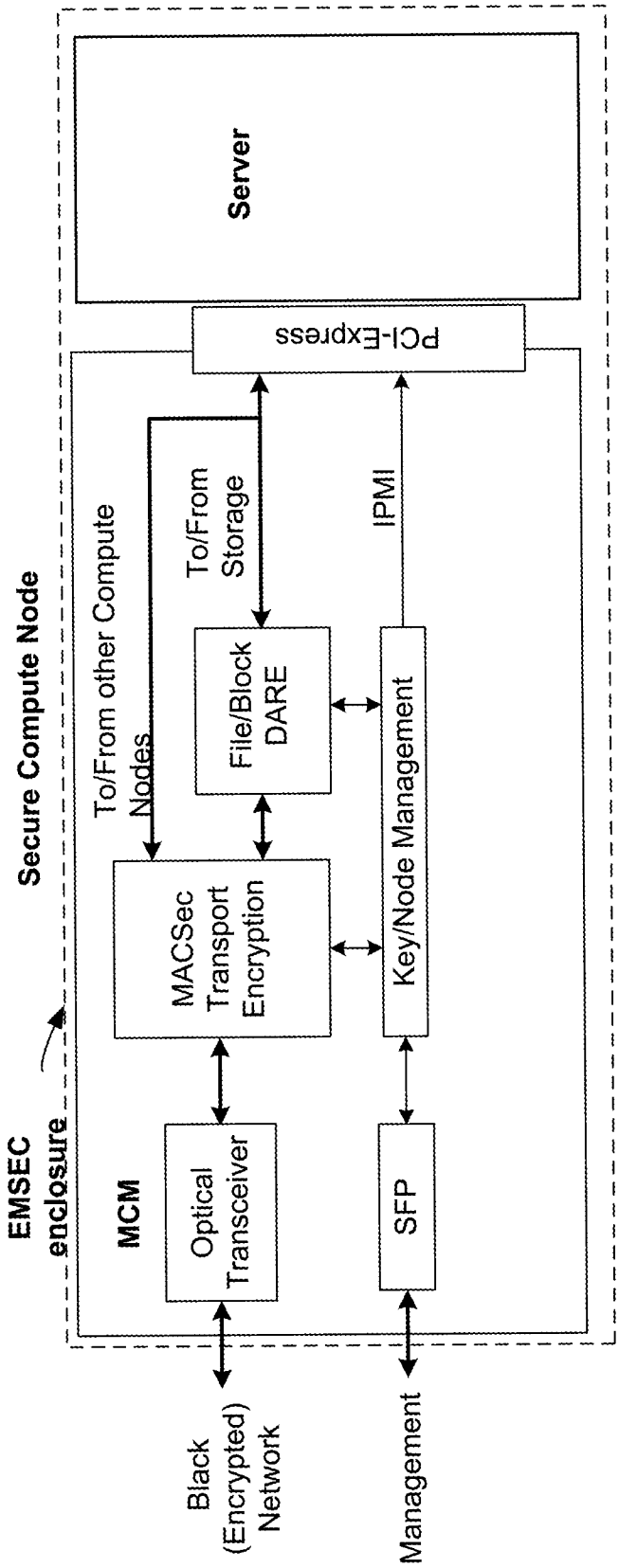

USERS
USERS
USERS
USERS
Security Domain-1
Security Domain-2
Security Domain-3
Security Domain-4
Stand Alone MCMs
MCM
MCM
MCM
MCM
Network
Secure HPC System
Domain-3
Domain-1
Secure Compute Node
Secure Compute Node
Secure Compute Node
MCM
MCM
MCM
Ethernet Switch
Secure Compute Node
Secure Compute Node
Secure Compute Node
MCM
MCM
MCM
Domain-1
Domain-2
Domain-2
Data Storage System (DSS)
MCM
Storage Controller
MCM
Key/Note Management

FIG. 1



Multi-Crypto Network Interface Card

- Boots thru MC-NIC from encrypted image
- Sanitized before and after each use by the MC-NIC
- No I/O except thru MC-NIC card

FIG. 2

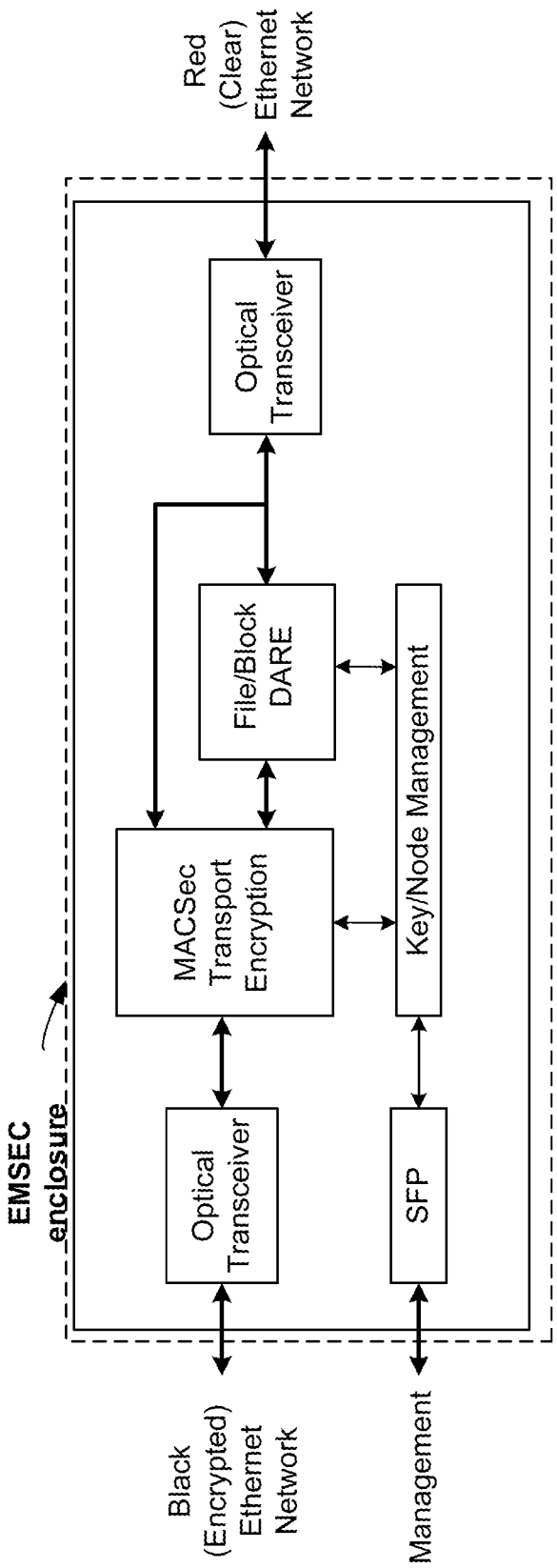

Red (Clear) Ethernet Network
Optical Transceiver
File/Block DARE
MACSec Transport Encryption
Key/Node Management
EMSEC enclosure
Optical Transceiver
SFP
Black (Encrypted) Ethernet Network
Management

FIG. 3

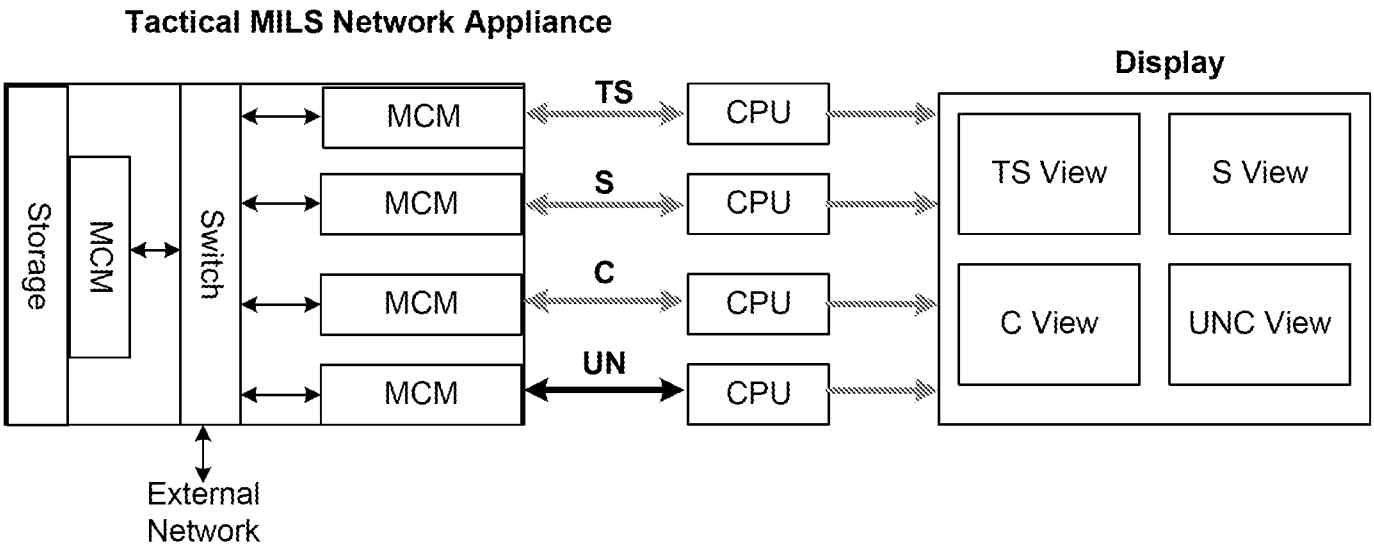

Tactical MILS Network Appliance
Storage
MCM
Switch
MCM
MCM
MCM
MCM
TS
S
C
UN
CPU
CPU
CPU
CPU
Display
TS View
S View
C View
UNC View
External
Network

FIG. 4

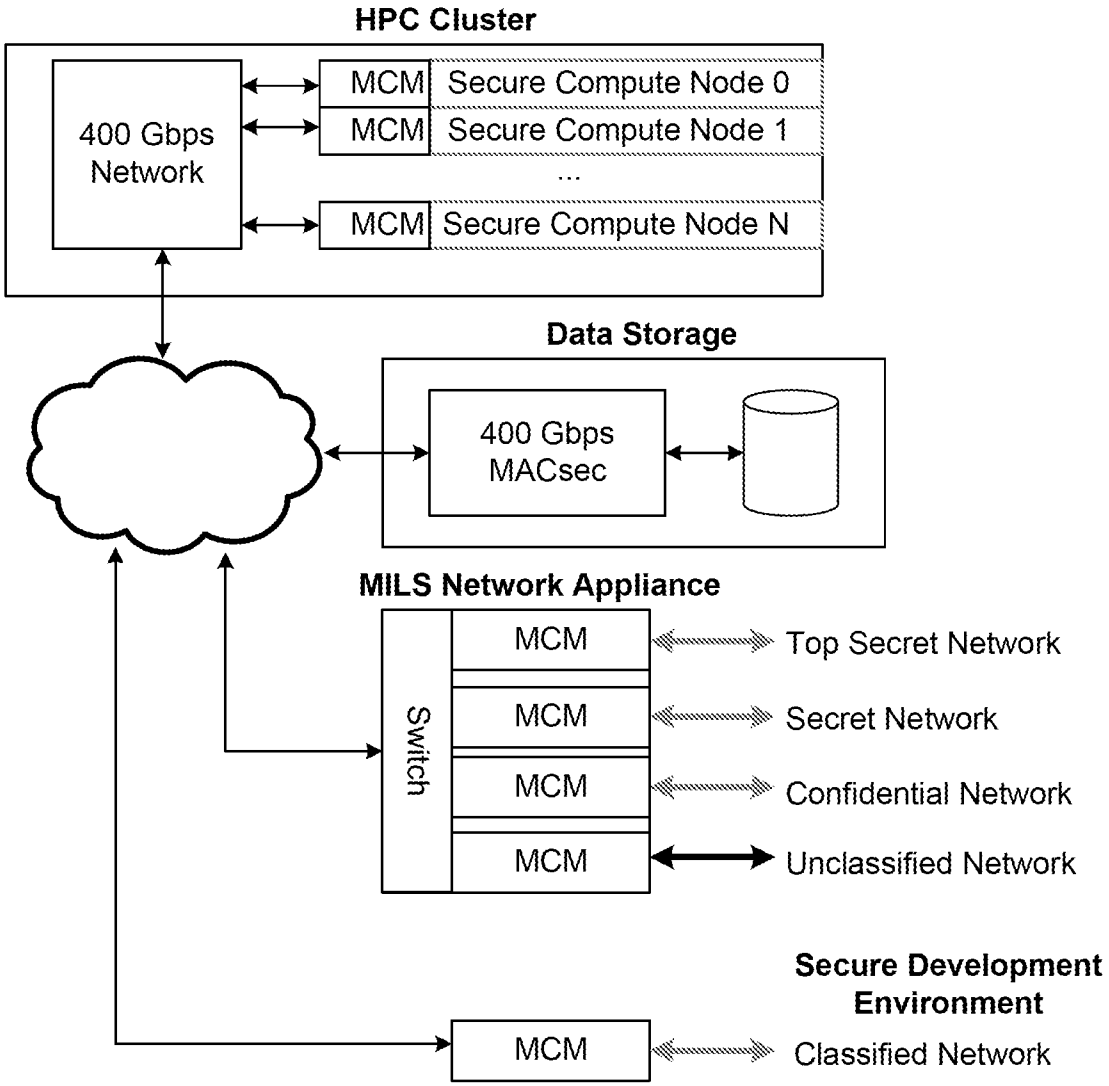

HPC Cluster
400 Gbps Network
MCM
Secure Compute Node 0
MCM
Secure Compute Node 1
...
MCM
Secure Compute Node N
Data Storage
400 Gbps MACsec
MILS Network Appliance
Switch
MCM
Top Secret Network
MCM
Secret Network
MCM
Confidential Network
MCM
Unclassified Network
Secure Development Environment
MCM
Classified Network

FIG. 5

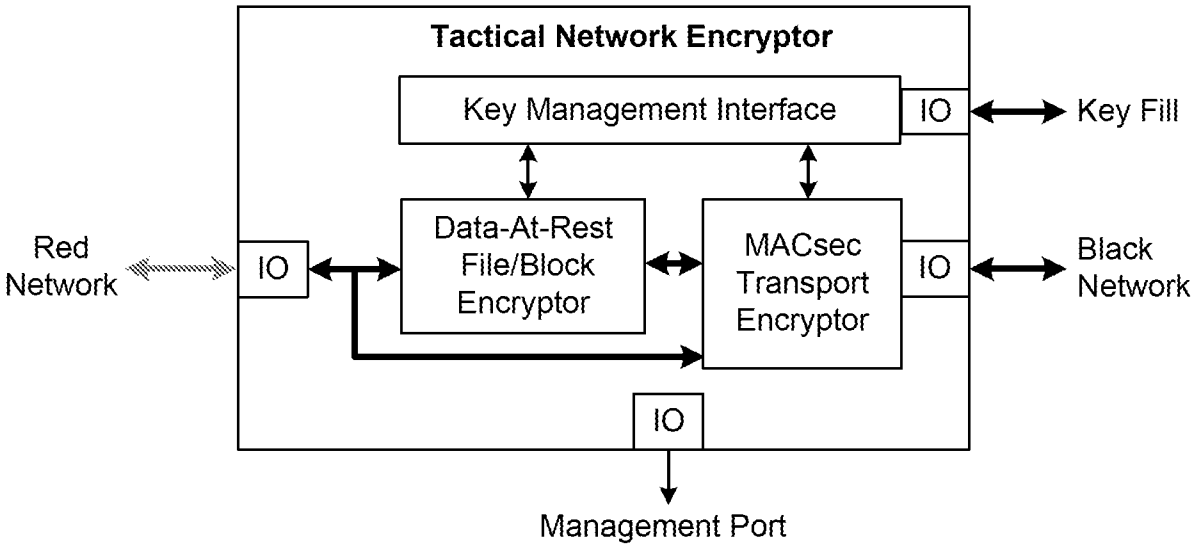

Tactical Network Encryptor
Key Management Interface
IO
Key Fill
Red
Network
IO
Data-At-Rest
File/Block
Encryptor
MACsec
Transport
Encryptor
IO
Black
Network
IO
Management Port

FIG. 6

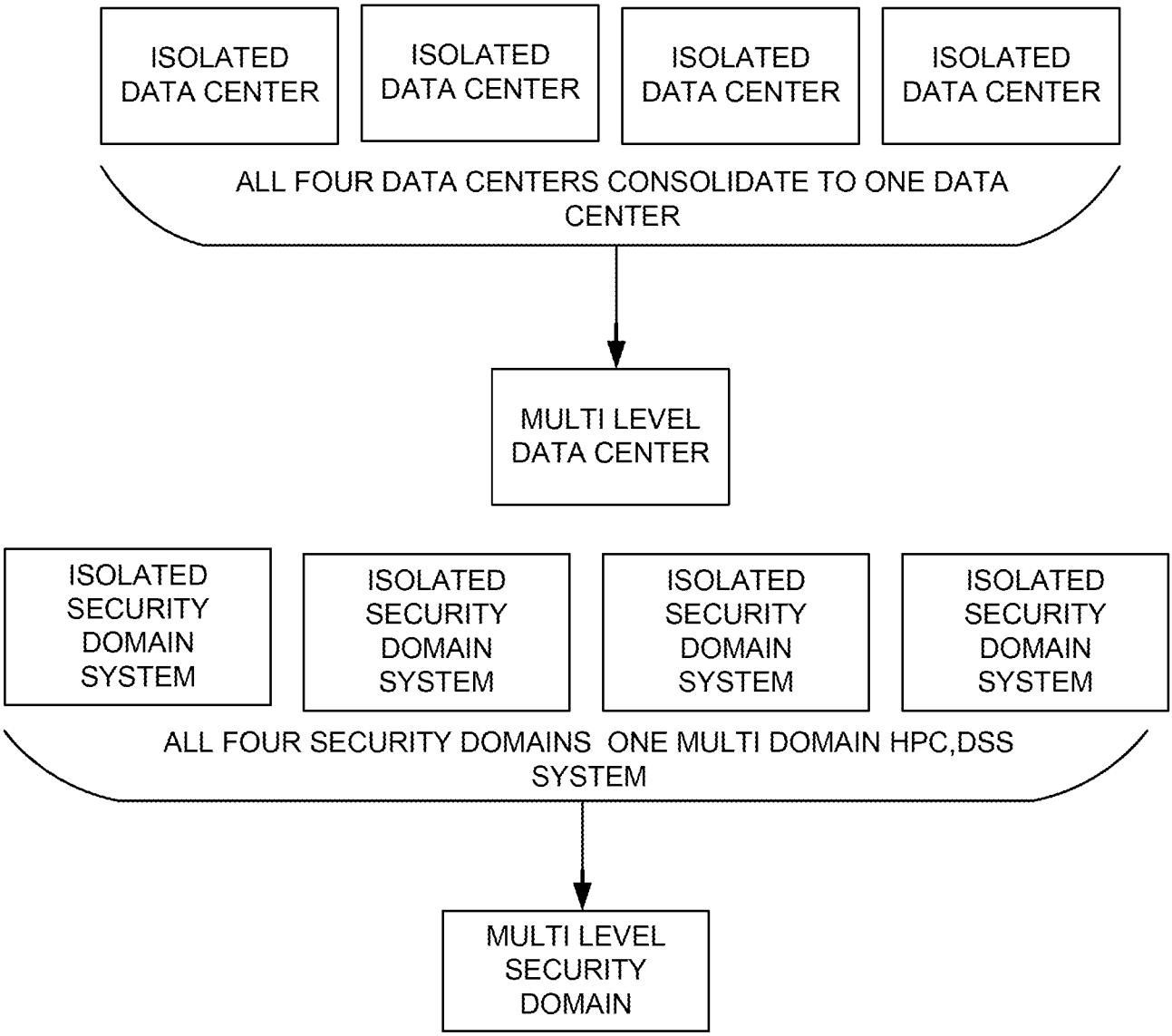

ISOLATED DATA CENTER
ISOLATED DATA CENTER
ISOLATED DATA CENTER
ISOLATED DATA CENTER
ALL FOUR DATA CENTERS CONSOLIDATE TO ONE DATA CENTER
MULTI LEVEL DATA CENTER
ISOLATED SECURITY DOMAIN SYSTEM
ISOLATED SECURITY DOMAIN SYSTEM
ISOLATED SECURITY DOMAIN SYSTEM
ISOLATED SECURITY DOMAIN SYSTEM
ALL FOUR SECURITY DOMAINS ONE MULTI DOMAIN HPC,DSS SYSTEM
MULTI LEVEL SECURITY DOMAIN

FIG. 7

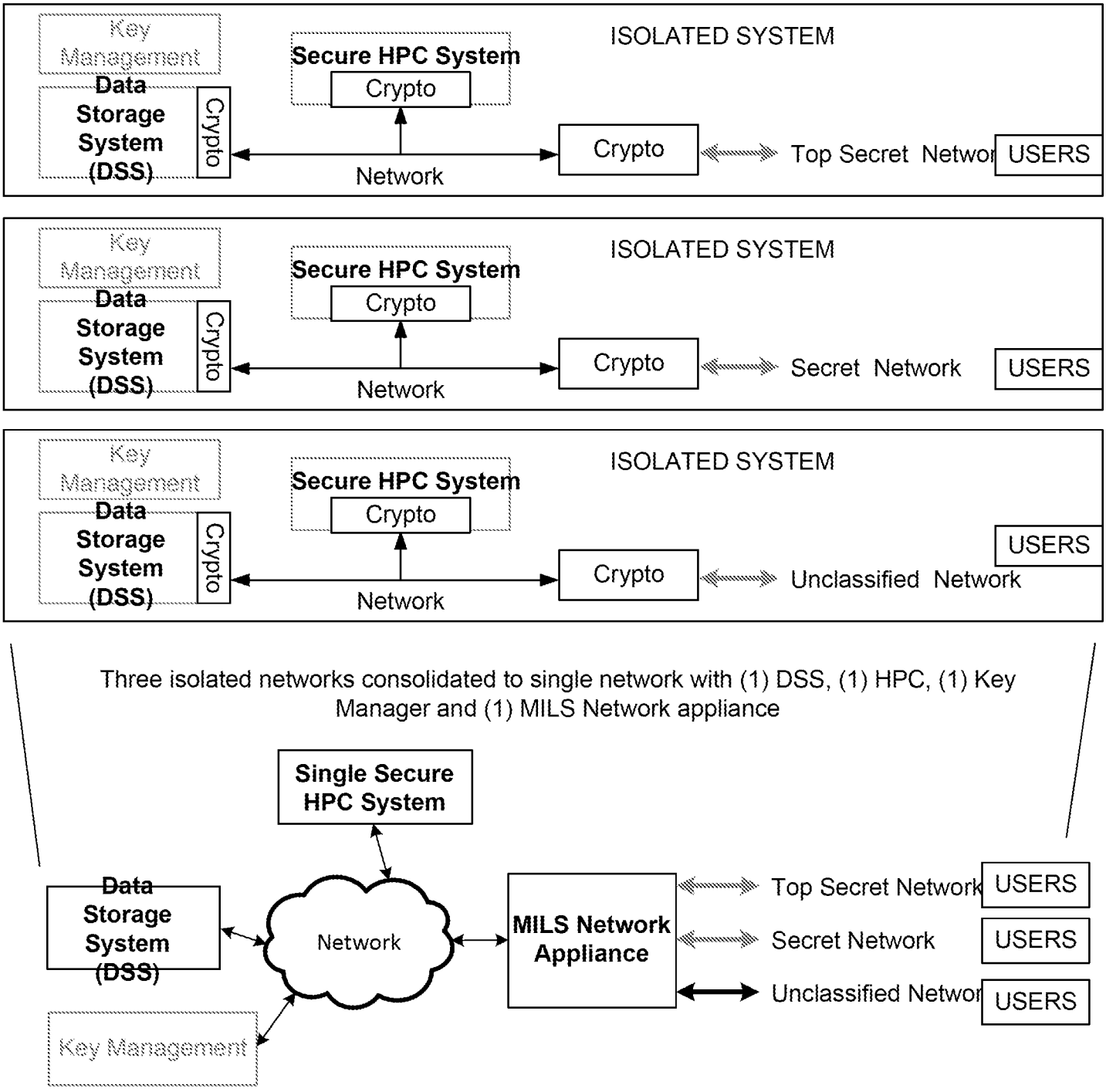

Key Management
Data Storage System (DSS)
Crypto
Secure HPC System
Crypto
ISOLATED SYSTEM
Network
Crypto
Top Secret Networ
USERS
Key Management
Data Storage System (DSS)
Crypto
Secure HPC System
Crypto
ISOLATED SYSTEM
Network
Crypto
Secret Network
USERS
Key Management
Data Storage System (DSS)
Crypto
Secure HPC System
Crypto
ISOLATED SYSTEM
Network
Crypto
Unclassified Network
USERS
Three isolated networks consolidated to single network with (1) DSS, (1) HPC, (1) Key Manager and (1) MILS Network appliance
Single Secure HPC System
Data Storage System (DSS)
Network
MILS Network Appliance
Top Secret Network
Secret Network
Unclassified Networ
USERS
USERS
USERS
Key Management

FIG. 8

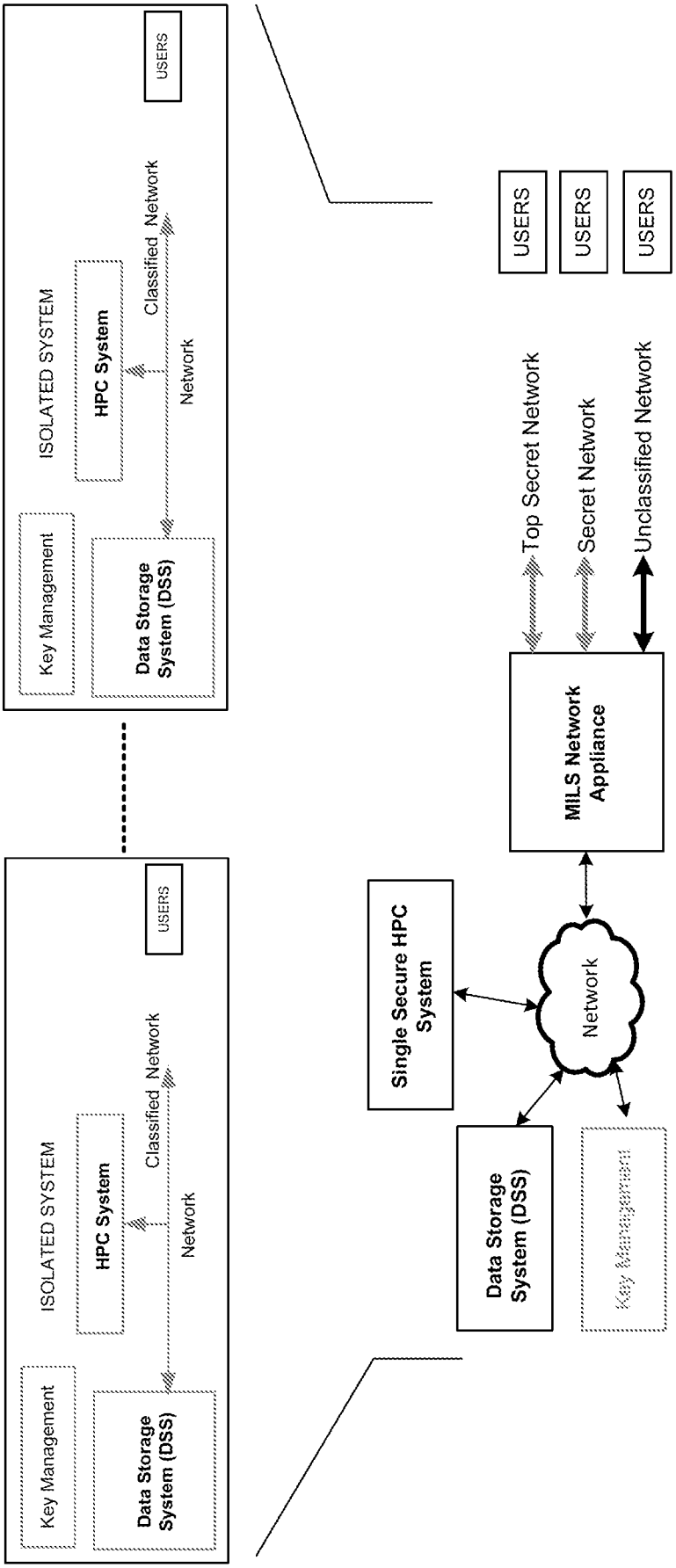

ISOLATED SYSTEM
HPC System
Classified Network
Network
USERS
Key Management
Data Storage System (DSS)
ISOLATED SYSTEM
HPC System
Classified Network
Network
USERS
Key Management
Data Storage System (DSS)
Single Secure HPC System
Network
Data Storage System (DSS)
Key Management
MILS Network Appliance
Top Secret Network
Secret Network
Unclassified Network
USERS
USERS
USERS

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2021/055956

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i; **H04L 9/14**(2006.01)i

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)

H04L 9/08(2006.01); G06F 12/14(2006.01); G06F 21/00(2006.01); H04L 29/06(2006.01); H04L 9/00(2006.01); H04L 9/14(2006.01)

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: cryptographic modules, different security levels, multiple domains, key manager

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2017-074887 A1 (SECTURION SYSTEMS, INC.) 04 May 2017 (2017-05-04) paragraphs [0036], [0139], [0154]; claims 1, 9; and figure 1	2-4
Y		1,5
Y	US 2017-0075821 A1 (SECTURION SYSTEMS, INC.) 16 March 2017 (2017-03-16) claim 1	1,5
A	US 2008-0181406 A1 (SREE M. IYER et al.) 31 July 2008 (2008-07-31) paragraphs [0064]-[0069]; and figure 3A	1-5
A	US 2011-0283339 A1 (MICHAEL R. SMITH) 17 November 2011 (2011-11-17) paragraphs [0079]-[0087]; and figure 9	1-5
A	US 2003-0005331 A1 (TIMOTHY C. WILLIAMS) 02 January 2003 (2003-01-02) paragraphs [0198]-[0200]; and figure 10	1-5

☐ 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	Date of mailing of the international search report
07 February 2022	**07 February 2022**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **189 Cheongsa-ro, Seo-gu, Daejeon** **35208, Republic of Korea**	**YANG, Jeong Rok**
Facsimile No. **+82-42-481-8578**	Telephone No. **+82-42-481-5709**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2021/055956

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2017-074887 A1	04 May 2017	US 10708236 B2	07 July 2020
		US 2017-0118180 A1	27 April 2017
US 2017-0075821 A1	16 March 2017	US 10114766 B2	30 October 2018
		US 2019-0050348 A1	14 February 2019
		US 9524399 B1	20 December 2016
US 2008-0181406 A1	31 July 2008	CN 101246529 A	20 August 2008
		CN 101246530 A	20 August 2008
		CN 101419576 A	29 April 2009
		EP 1953668 A2	06 August 2008
		EP 1953668 A3	16 December 2009
		EP 1953669 A2	06 August 2008
		EP 1953669 A3	23 December 2009
		EP 1993058 A1	19 November 2008
		JP 2008-187718 A	14 August 2008
		JP 2008-219871 A	18 September 2008
		JP 2009-076045 A	09 April 2009
		KR 10-2008-0071529 A	04 August 2008
		KR 10-2008-0071530 A	04 August 2008
		KR 10-2008-0101799 A	21 November 2008
		TW 200832181 A	01 August 2008
		TW 200834375 A	16 August 2008
		TW 200846970 A	01 December 2008
		US 2008-0288782 A1	20 November 2008
		US 2009-0046858 A1	19 February 2009
		US 2011-0087889 A1	14 April 2011
		US 8230207 B2	24 July 2012
		WO 2008-094837 A1	07 August 2008
		WO 2008-094839 A1	07 August 2008
		WO 2008-094839 A8	16 October 2008
		WO 2008-144280 A1	27 November 2008
US 2011-0283339 A1	17 November 2011	CN 1864390 A	15 November 2006
		CN 1864390 B	27 October 2010
		EP 1692840 A2	23 August 2006
		EP 1692840 B1	05 September 2012
		US 2005-0097357 A1	05 May 2005
		US 7836490 B2	16 November 2010
		US 8539571 B2	17 September 2013
		WO 2005-046178 A2	19 May 2005
		WO 2005-046178 A3	15 December 2005
US 2003-0005331 A1	02 January 2003	AU 2000-15954 A1	06 March 2000
		AU 2000-15954 B2	01 August 2002
		CA 2339637 A1	24 February 2000
		CA 2422268 A1	24 February 2000
		EP 1101161 A2	23 May 2001
		EP 1101161 A4	14 September 2005
		IL 140902 A	05 July 2006
		NZ 509570 A	28 March 2003
		US 6304973 B1	16 October 2001
		US 7069437 B2	27 June 2006

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2021/055956

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
		WO 00-10278 A2	24 February 2000
		WO 00-10278 A3	13 July 2000
		WO 00-10278 B1	13 July 2000