



(51) International Patent Classification:

G08B 13/196 (2022.01) G06F 21/62 (2022.01)

(21) International Application Number:

PCT/US2022/013358

(22) International Filing Date:

21 January 2022 (21.01.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

17/234,051 19 April 2021 (19.04.2021) US

(71) Applicant: **WESTERN DIGITAL TECHNOLOGIES, INC.** [US/US]; 5601 Great Oaks Parkway, San Jose, California 95119 (US).

(72) Inventors: **HAHN, Judah Gamliel**; c/o Western Digital Technologies, Inc., 5601 Great Oaks Parkway, San Jose, California 95119 (US). **NAVON, Ariel**; c/o Western Digital Technologies, Inc., 5601 Great Oaks Parkway, San Jose, California 95119 (US). **BENISTY, Shay**; c/o Western Digital Technologies, Inc., 5601 Great Oaks Parkway, San Jose, California 95119 (US).

(74) Agent: **VERSTEEG, Steven H.** et al.; Patterson & Sheridan, LLP, 24 Greenway Plaza, Suite 1600, Houston, Texas 77046 (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).

(54) Title: PRIVACY ENFORCING MEMORY SYSTEM

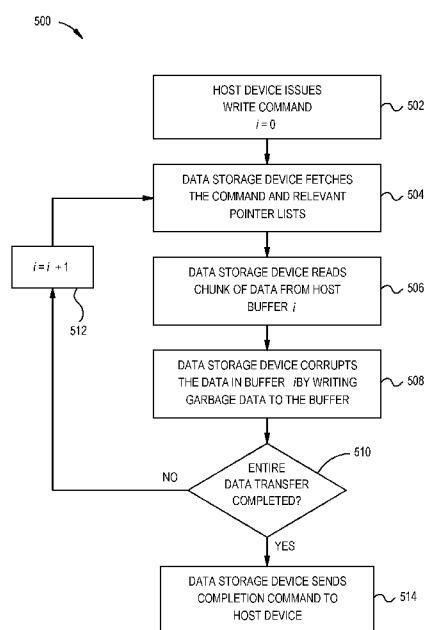


FIG. 5

(57) Abstract: A method and apparatus for enforcing privacy within one or more memories of a data storage system are disclosed. In one embodiment, sensor data containing personally identifiable information (PII) is provided to a memory. In some embodiments, the memory of disclosed systems and methods may be volatile, non-volatile, or a combination. Within the memory, PII is detected in some embodiments by AI-based computer vision, voice recognition, or natural language processing methods. Detected PII is obfuscated within the memory prior to making the sensor data available to other systems or memories. In some embodiments, once PII has been obfuscated, the original sensor data is overwritten, deleted, or otherwise made unavailable.

Published:

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

PRIVACY ENFORCING MEMORY SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Application No.: 17/234,051, filed April 19, 2021, which is assigned to the assignee hereof and incorporated by reference herein in its entirety.

BACKGROUND OF THE DISCLOSURE

Field of the Disclosure

[0002] Embodiments of the present disclosure generally relate to obfuscating personally identifiable information, and more particularly, to obfuscating personally identifiable information in a data storage device.

Description of the Related Art

[0003] Advances in artificial intelligence have led to enhanced capability for the identification of people and objects by computers through the use of computer vision, voice recognition, and natural language processing technologies. In many cases, these capabilities exceed the ability of humans. However, these enhanced capabilities of computers cause challenges in the realm of privacy, or more accurately, maintaining the privacy of individuals in accordance with laws, regulations, and social expectations.

[0004] The same technologies that can identify people and objects may further be used to modify or obfuscate features of people and objects found in sensor data for which privacy is expected or required. However, in conventional approaches, sensor data is stored in an un-obfuscated form, with obfuscation applied prior to displaying on a user interface. As a result, a malicious user may seek to circumvent obfuscation applications to obtain un-obfuscated data from volatile or non-volatile memories.

[0005] What is needed are systems and methods for addressing the shortcomings of conventional approaches.

SUMMARY OF THE DISCLOSURE

[0006] The present disclosure generally relates to systems and methods for enforcing privacy within memories of data storage systems. In one embodiment, sensor data containing personally identifiable information (PII) is provided to a memory. In some embodiments, the memory of disclosed systems and methods may be volatile, non-volatile, or a combination. Within the memory, PII is detected in some embodiments by AI-based computer vision, voice recognition, or natural language processing methods. Detected PII is obfuscated within the memory prior to making the sensor data available to other systems or memories. In some embodiments, once PII has been obfuscated, the original sensor data is overwritten, deleted, or otherwise made unavailable.

[0007] In one embodiment, a system for enforcing data privacy is disclosed, that includes an input/output coupled to a sensor configured to produce sensor data comprising personal identifying data, an intermediate storage configured to receive sensor data from the sensor; and a blur unit coupled to the intermediate storage and configured to identify personal identifying data of the sensor data, produce obfuscated sensor data by obfuscating at least a portion of the personal identifying data, and provide the obfuscated sensor data to the intermediate storage.

[0008] In another embodiment, a system for storing data is disclosed that includes an input/output coupled to a sensor, an intermediate storage (IS), a data storage device, and a processor configured to execute a method for enforcing data privacy. The method includes receiving sensor data from the sensor comprising personal identifying data at the IS, identifying the personal identifying data at the IS, and generating obfuscated sensor data at the IS by obfuscating at least a portion of the personal identifying data.

[0009] In another embodiment, a controller for a data storage system is disclosed that includes a memory means for storing computer-readable instructions, and a processor means configured to read computer-readable instructions that cause the processor to execute a method for enforcing data privacy. The method includes receiving sensor data comprising personal identifying information at an intermediate storage (IS) means; obfuscate at least

a portion of the sensor data comprising personal identifying information at the IS means, to generate obfuscated personal identifying information; and provide the sensor data to a data storage device (DSD) means.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] So that the manner in which the above-recited features of the present disclosure can be understood in detail, a more particular description of the disclosure, briefly summarized above, may be had by reference to embodiments, some of which are illustrated in the appended drawings. It is to be noted, however, that the appended drawings illustrate only typical embodiments of this disclosure and are therefore not to be considered limiting of its scope, for the disclosure may admit to other equally effective embodiments.

[0011] Figure 1 depicts a schematic block diagram illustrating a storage system in which a data storage device may function as a storage device for a host device, according to certain embodiments.

[0012] Figure 2A depicts a schematic block diagram illustrating an implementation of blurring data of a privacy-recording system, according to certain embodiments.

[0013] Figure 2B depicts a schematic block diagram illustrating another implementation of blurring data of a privacy-recording system, according to certain embodiments.

[0014] Figure 3 depicts a schematic block diagram illustrating a memory-level read blocking of unblurred data system, according to certain embodiments.

[0015] Figure 4 depicts a schematic block diagram illustrating an intermediate storage disruptive read of unblurred data system, according to certain embodiments.

[0016] Figure 5 depicts a schematic block diagram illustrating a method of a disruptive read of unblurred data of an NVMe write command flow, according to certain embodiments.

[0017] To facilitate understanding, identical reference numerals have been used, where possible, to designate identical elements that are common to the figures. It is contemplated that elements disclosed in one embodiment may be beneficially utilized on other embodiments without specific recitation.

DETAILED DESCRIPTION

[0018] In the following, reference is made to embodiments of the disclosure. However, it should be understood that the disclosure is not limited to specifically described embodiments. Instead, any combination of the following features and elements, whether related to different embodiments or not, is contemplated to implement and practice the disclosure. Furthermore, although embodiments of the disclosure may achieve advantages over other possible solutions and/or over the prior art, whether or not a particular advantage is achieved by a given embodiment is not limiting of the disclosure. Thus, the following aspects, features, embodiments, and advantages are merely illustrative and are not considered elements or limitations of the appended claims except where explicitly recited in a claim(s). Likewise, a reference to “the disclosure” shall not be construed as a generalization of any inventive subject matter disclosed herein and shall not be considered to be an element or limitation of the appended claims except where explicitly recited in a claim(s).

[0019] The present disclosure generally relates to systems and methods for enforcing privacy within memories of data storage systems. In one embodiment, sensor data containing personally identifiable information (PII) is provided to a memory. In some embodiments, the memory of disclosed systems and methods may be volatile, non-volatile, or a combination. Within the memory, PII is detected in some embodiments by AI-based computer vision, voice recognition, or natural language processing methods. Detected PII is obfuscated within the memory prior to making the sensor data available to other systems or memories. In some embodiments, once PII has been obfuscated, the original sensor data is overwritten, deleted, or otherwise made unavailable.

[0020] Figure 1 depicts a schematic block diagram illustrating a storage system 100 in which data storage device 106 may function as a storage device

for a host device 104, according to certain embodiments. For instance, the host device 104 may utilize a non-volatile memory (NVM) 110 included in data storage device 106 to store and retrieve data. The host device 104 comprises a host DRAM 138. In some examples, the storage system 100 may include a plurality of storage devices, such as the data storage device 106, which may operate as a storage array. For instance, the storage system 100 may include a plurality of data storage devices 106 configured as a redundant array of inexpensive/independent disks (RAID) that collectively function as a mass storage device for the host device 104.

[0021] The host device 104 may store and/or retrieve data to and/or from one or more storage devices, such as the data storage device 106. As illustrated in Figure 1, the host device 104 may communicate with the data storage device 106 via an interface 114. The host device 104 may comprise any of a wide range of devices, including computer servers, network-attached storage (NAS) units, desktop computers, notebook (i.e., laptop) computers, tablet computers, set-top boxes, telephone handsets such as so-called “smart” phones, so-called “smart” pads, televisions, cameras, display devices, digital media players, video gaming consoles, video streaming device, or other devices capable of sending or receiving data from a data storage device.

[0022] The data storage device 106 includes a controller 108, NVM 110, a power supply 111, volatile memory 112, an interface 114, and a write buffer 116. In some examples, the data storage device 106 may include additional components not shown in Figure 1 for the sake of clarity. For example, the data storage device 106 may include a printed circuit board (PCB) to which components of the data storage device 106 are mechanically attached and which includes electrically conductive traces that electrically interconnect components of the data storage device 106 or the like. In some examples, the physical dimensions and connector configurations of the data storage device 106 may conform to one or more standard form factors. Some example standard form factors include, but are not limited to, 3.5” data storage device (e.g., an HDD or SSD), 2.5” data storage device, 1.8” data storage device, peripheral component interconnect (PCI), PCI-extended (PCI-X), PCI Express (PCIe) (e.g., PCIe x1, x4,

x8, x16, PCIe Mini Card, MiniPCI, etc.). In some examples, the data storage device 106 may be directly coupled (e.g., directly soldered) to a motherboard of the host device 104.

[0023] The interface 114 of the data storage device 106 may include one or both of a data bus for exchanging data with the host device 104 and a control bus for exchanging commands with the host device 104. Interface 114 may operate in accordance with any suitable protocol. For example, the interface 114 may operate in accordance with one or more of the following protocols: advanced technology attachment (ATA) (e.g., serial-ATA (SATA) and parallel-ATA (PATA)), Fibre Channel Protocol (FCP), small computer system interface (SCSI), serially attached SCSI (SAS), PCI, and PCIe, non-volatile memory express (NVMe), OpenCAPI, GenZ, Cache Coherent Interface Accelerator (CCIX), Open Channel SSD (OCSSD), or the like. The electrical connection of the interface 114 (e.g., the data bus, the control bus, or both) is electrically connected to the controller 108, providing an electrical connection between the host device 104 and the controller 108, allowing data to be exchanged between the host device 104 and the controller 108. In some examples, the electrical connection of interface 114 may also permit the data storage device 106 to receive power from the host device 104. For example, as illustrated in Figure 1, the power supply 111 may receive power from the host device 104 via interface 114.

[0024] The NVM 110 may include a plurality of memory devices or memory units. NVM 110 may be configured to store and/or retrieve data. For instance, a memory unit of NVM 110 may receive data and a message from controller 108 that instructs the memory unit to store the data. Similarly, the memory unit of NVM 110 may receive a message from controller 108 that instructs the memory unit to retrieve data. In some examples, each of the memory units may be referred to as a die. In some examples, the NVM 110 may include a plurality of dies (i.e., a plurality of memory units). In some examples, each memory unit may be configured to store relatively large amounts of data (e.g., 128MB, 256MB, 512MB, 1GB, 2GB, 4GB, 8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB, 1TB, etc.).

[0025] In some examples, each memory unit of NVM 110 may include any type of non-volatile memory devices, such as flash memory devices, phase-change memory (PCM) devices, resistive random-access memory (ReRAM) devices, magnetoresistive random-access memory (MRAM) devices, ferroelectric random-access memory (F-RAM), holographic memory devices, and any other type of non-volatile memory devices.

[0026] The NVM 110 may comprise a plurality of flash memory devices or memory units. NVM Flash memory devices may include NAND or NOR-based flash memory devices and may store data based on a charge contained in a floating gate of a transistor for each flash memory cell. In NVM flash memory devices, the flash memory device may be divided into a plurality of dies, where each die of the plurality of dies includes a plurality of blocks, which may be further divided into a plurality of pages. Each block of the plurality of blocks within a particular memory device may include a plurality of NVM cells. Rows of NVM cells may be electrically connected using a word line to define a page of a plurality of pages. Respective cells in each of the plurality of pages may be electrically connected to respective bit lines. Furthermore, NVM flash memory devices may be 2D or 3D devices and may be single level cell (SLC), multi-level cell (MLC), triple level cell (TLC), or quad level cell (QLC). Controller 108 may write data to and read data from NVM flash memory devices at the page level and erase data from NVM flash memory devices at the block level.

[0027] The data storage device 106 includes a power supply 111, which may provide power to one or more components of the data storage device 106. When operating in a standard mode, the power supply 111 may provide power to one or more components using power provided by an external device, such as the host device 104. For instance, the power supply 111 may provide power to the one or more components using power received from the host device 104 via interface 114. In some examples, the power supply 111 may include one or more power storage components configured to provide power to the one or more components when operating in a shutdown mode, such as where power ceases to be received from the external device. In this way, the power supply 111 may function as an onboard backup power source. Some examples of the one or

more power storage components include, but are not limited to, capacitors, supercapacitors, batteries, and the like. In some examples, the amount of power that may be stored by the one or more power storage components may be a function of the cost and/or the size (e.g., area/volume) of the one or more power storage components. In other words, as the amount of power stored by the one or more power storage components increases, the cost and/or the size of the one or more power storage components also increases.

[0028] The data storage device 106 also includes volatile memory 112, which may be used by controller 108 to store information. Volatile memory 112 may include one or more volatile memory devices. In some examples, controller 108 may use volatile memory 112 as a cache. For instance, controller 108 may store cached information in volatile memory 112 until cached information is written to the NVM 110. As illustrated in Figure 1, volatile memory 112 may consume power received from the power supply 111. Examples of volatile memory 112 include, but are not limited to, random-access memory (RAM), dynamic random access memory (DRAM), static RAM (SRAM), and synchronous dynamic RAM (SDRAM (e.g., DDR1, DDR2, DDR3, DDR3L, LPDDR3, DDR4, LPDDR4, and the like)).

[0029] The data storage device 106 includes a controller 108, which may manage one or more operations of the data storage device 106. For instance, controller 108 may manage the reading of data from and/or the writing of data to the NVM 110. In some embodiments, when the data storage device 106 receives a write command from the host device 104, the controller 108 may initiate a data storage command to store data to the NVM 110 and monitor the progress of the data storage command. Controller 108 may determine at least one operational characteristic of the storage system 100 and store the at least one operational characteristic in the NVM 110. In some embodiments, when the data storage device 106 receives a write command from the host device 104, the controller 108 temporarily stores the data associated with the write command in the internal memory or write buffer 116 before sending the data to the NVM 110.

[0030] Figure 2A depicts a schematic block diagram illustrating an implementation of blurring data of a privacy-recording system 200, according to certain embodiments. The system 200 includes one or more sensors 202

coupled to an intermediate storage/interface buffer 204. In one non-limiting example, the one or more sensors 202 may be configured to capture sensor data, such as image data. For example, the one or more sensors 202 may be the sensors of a digital video camera, a digital single-lens reflex camera, a mirrorless interchangeable-lens camera, a hybrid camera, a compact system camera, a surveillance system, a security camera, closed-circuit television camera, and the like.

[0031] The sensor data is transferred to the intermediate storage/interface buffer 204 as non-private (unblurred) data, such that the sensor data is unmodified. In the description herein, sensor data may be referred to as image data for exemplary purposes. Rather, private (blurred) data cannot be reconstructed to the original data due to some modification to certain parts of the data. For example, a face is a distinguishable feature of an individual, such that the face may be recognizable to a stranger. In order to protect the privacy (i.e., personally identifiable information (PII)) of the individual, a portion of the image, including the face, may be blurred or obfuscated while the remaining portion of the image not including the face is not blurred. The blurring may be due to a modification of a certain part of the data, where the certain part of the data is associated with image data of the face. In some examples, the intermediate storage/interface buffer 204 is volatile memory, such as the volatile memory 112 of Figure 1. The volatile memory may be SRAM, DRAM, or other applicable non-power safe memory types. In other examples, the intermediate storage/interface buffer 204 is a portion of non-volatile memory, such as the NVM 110 of Figure 1. The portion of the NVM may be an SLC buffer dedicated for fast writes and temporary storage of the image data.

[0032] The intermediate storage/interface buffer 204 is coupled to a storage unit 206. The image data is transferred to the storage unit 206 from the intermediate storage/interface buffer 204. The storage unit 206 may be a memory device or a data storage device configured to store the image data for long-term storage. The storage unit 206 may be power fail-safe, such that the data stored in storage unit 206 is protected against corruption or errors during an ungraceful shutdown event. When the image data is transferred from the

intermediate storage/interface buffer 204 to the storage unit 206, the image data is non-private (unblurred) data. Because the image data stored in the intermediate storage/interface buffer 204 and the storage unit 206 are in the non-private (unblurred) data format, there may be a potential privacy violation, such as when an external entity accesses the intermediate storage/interface buffer 204 and/or the storage unit 206 without permission. In some non-limiting examples, the external entities may be either an individual, a company, or an artificial intelligence (AI) with malicious or unwanted intent.

[0033] The storage unit 206 is coupled to a “blurring” application 208. The data streams between the one or more sensors 202 and the intermediate storage/interface buffer 204, the intermediate storage/interface buffer 204 and the storage unit 206, and the storage unit and the “blurring” application 208 may be intercepted during an attack on the data streams, such that PII is gained by the external entity without permission. When the “blurring” application 208 receives the non-private (unblurred) data, the “blurring” application 208 may be configured to determine which parts of the image data to be blurred or obfuscated and blur or obfuscate the identified parts of the image data. The identified parts of the image data may be related to the PII, such that obfuscating the identified parts of the image data relates to corrupting the data or other similar methods of blurring the data. The “blurring” application 208 is coupled to a user 210. The user 210 may be the host device 104 of Figure 1. The image data is transferred from the “blurring” application 208 to the user 210 in a private “blurred” data format, such that the PII may be protected.

[0034] Figure 2B depicts a schematic block diagram illustrating another implementation of blurring data of a privacy-recording system 250, according to certain embodiments. Aspects of the privacy-recording system 250 may be similar to the aspects of the privacy-recording system 200. Thus, for simplification, common reference numerals are utilized in the privacy-recording system 250 as the privacy-recording system 200, and the description of each aspect is hereby incorporated. Rather than transferring the non-private (unblurred) data to the storage unit 206, such as in the privacy-recording system 200, the non-private (unblurred) data is transferred to the “blurring” application

208 prior to the image data being transferred to the storage unit 206. Rather than having three data streams transferring and two memory locations storing the non-private (unblurred) data, the privacy-recording system 250 only has two data streams transferring and one memory location storing the non-private (unblurred) data. However, the external entity may still gain access to the privacy-recording system 250 and obtain PII without permission.

[0035] Figure 3 depicts a schematic block diagram illustrating a memory-level read blocking of unblurred data system 300, according to certain embodiments. The memory-level read blocking of unblurred data system 300 includes one or more sensors 302, a first storage module 304 coupled to the one or more sensors 302 via an input/output bus 320 configured to transfer sensor data, a second storage module 312 coupled to the first storage module 304, a blur unit 310 coupled to both the first storage module 304 and the second storage module 312, and a user 318 coupled to the second storage module 312. The blur unit 310 may be the “blurring” application 208 of Figures 2A and 2B.

[0036] The first storage module 304 includes an intermediate storage/interface buffer 306 coupled to a blur validation module 308. The intermediate storage/interface buffer 306 may be the intermediate storage/interface buffer 204 of Figures 2A and 2B. The second storage module 312 includes a storage unit 314 coupled to a blur validation module 316. The storage unit 314 may be the storage unit 206 of Figures 2A and 2B. The first storage module 304 and the second storage module 312 may be configured to protect stored data such that the data stored in each respective storage module 304, 312 cannot be accessed by an external entity. The first storage module 304 may have read protection, such that a read of unblurred data is prohibited.

[0037] The blur unit 310 may be configured to corrupt or blur PII data of the image data from the one or more sensors 302, such that obfuscated sensor data is generated by the blur unit 310. Although the blur unit 310 is shown to be coupled to both the intermediate storage/interface buffer 306 and the storage unit 314, in other embodiments, the first storage module 304 and the second storage module 312 each include a blur unit 310. Furthermore, the data paths to and from the blur unit 310 and the blur unit 310 may be part of a read protected area

of the memory-level read blocking of unblurred data system 300, such that the data being transferred to and from the blur unit 310 cannot be accessed by an external entity. The blurring or obfuscating by the blur unit 310 may be completed on-the-fly or offline, such that data may be blurred or obfuscated prior to being stored in the relevant data storage locations. Furthermore, in some embodiments, the blur unit 310 may be configured to retrieve data from the intermediate storage/interface buffer 306 and the storage unit 314.

[0038] The blur validation modules 308, 316 may be configured to generate a flag in response to identifying PII in the original sensor data or the obfuscated sensor data generated by the blur unit 310 and stored in the respective intermediate storage/interface buffer 306 or the storage unit 314. When a flag is generated for the obfuscated sensor data, the blur validation modules 308, 316 may be configured to return the obfuscated sensor data and the flag to the blur unit 310, such that the non-obfuscated PII sensor data may be obfuscated by the blur unit 310 and the PII is no longer identifiable.

[0039] The obfuscated sensor data is passed from the first storage module 304 to the second storage module 312 and from the second storage module 312 to the user 318 in a private (blurred) data format. Thus, rather than having multiple non-private (unblurred) data storage locations or data streams, the memory-level read blocking of unblurred data system 300 includes a single data stream passing non-private (unblurred) data, where the single data stream is between the one or more sensors and the first storage module 304.

[0040] Figure 4 depicts a schematic block diagram illustrating an intermediate storage disruptive read of unblurred data system 400, according to certain embodiments. The intermediate storage disruptive read of unblurred data system 400 includes one or more sensors 402 coupled to a storage module 404, where sensor data or image data is transferred from the one or more sensors 402 to the storage module 404 via an input/output bus 420. The sensor data or image data transferred via the input/output bus 420 is in a non-private (unblurred) data format, such that PII data is not obfuscated or blurred.

[0041] The storage module 404 may be configured to protect stored such that the data stored in the storage module 404 cannot be accessed by an external entity. The storage module 404 may have read protection, such that a read of unblurred data by an external entity without permission is prohibited. The storage module 404 includes an intermediate storage/interface buffer 406, which may be the intermediate storage/interface buffer 204 of Figure 2, coupled to a blur and erase unit 408. It is understood that in some embodiments, the storage module 404 may include the blur and erase unit 408 and a storage unit 410 and exclude the intermediate storage/interface buffer 406. For example, if the interface, such as the interface 114 of Figure 1, is one in which the data storage device, such as the data storage device 106 of Figure 1, is the bus master (e.g., PCIe/NVMe), the intermediate storage/interface buffer 406 may reside together with the one or more sensors 402. Thus, the storage module 404 includes the blur and erase unit 408 and the storage unit 410.

[0042] The blur and erase unit 408 may be configured to obfuscate or blur PII data in the image data and rewrite the obfuscated image data back to the intermediate storage/interface buffer 406, such that the original image data stored in the intermediate storage/interface buffer 406 is erased and replaced with the obfuscated data. In some embodiments, the blur and erase unit 408 includes a blur validation module, such as the blur validation modules 308, 316 of Figure 3. The obfuscated image data is transferred to the storage unit 410, which may be the storage unit 206 of Figures 2A and 2B. The obfuscated image data is provided to a user 412 from the storage unit 410.

[0043] In one non-limiting example, the blur and erase unit 408 modifies, blurs, or obfuscates a portion of the data, such as a size of about 32B or 64B in each 4KB of sensor data stored in the intermediate storage/interface buffer 406. The modification, blur, or obfuscation of the sensor data may be large enough such that the original sensor data is not recoverable.

[0044] The obfuscated sensor data is passed from the storage module 404 to the storage unit 410 and from the storage unit 410 to the user 412 in a private (blurred) data format. Thus, rather than having multiple non-private (unblurred) data storage locations or data streams, the intermediate storage disruptive read

of unblurred data system 400 includes a single data stream passing non-private (unblurred) data, where the single data stream is between the one or more sensors and the storage module 404.

[0045] Figure 5 depicts a schematic block diagram illustrating a method of a disruptive read of unblurred data of an NVMe write command flow 500, according to certain embodiments. The NVMe write command flow 500 may be implemented by the intermediate storage disruptive read of unblurred data system 400 of Figure 4.

[0046] At block 502, a host device, such as the host device 104 of Figure 1, issues a write command. The write command is associated with an initial starting location (i) of data stored in the intermediate storage/interface buffer 406. At block 504, the data storage device, such as the data storage device 106 of Figure 1, utilizing a controller, such as the controller 108 of Figure 1, or firmware fetches the write command and relevant pointer lists from the host device 104. In some examples, controller 108 may include one or more processors configured to execute the firmware. At block 506, the data storage device reads a chunk of data from a host buffer, such as the intermediate storage/interface buffer 406, at the location i . At block 508, the data storage device corrupts the data in the host buffer location i by writing garbage data to the host buffer. The corrupting and writing may be completed by the blur and erase unit 408 of Figure 4. The garbage data may be written to the sensor data so as to overwrite the portion of the sensor data relating to PII data.

[0047] At block 510, the controller 108 or firmware determines if the entire data transfer associated with the write command has finished. If the data transfer has not finished, then at block 512, the location i is incremented to a new value for i , where the new i is defined as $i = i + 1$. The NVMe write command flow 500 returns to block 504, where the data storage device 106 fetches the write command and relevant pointer lists. However, if the entire data transfer is completed at block 510, then the data storage device 106 sends a completion command to the host device 104 at block 514.

[0048] By implementing data protection techniques and obfuscating data at a location near the data source, personally identifying information may be protected from unwanted access, and the security of privacy-recording systems may be improved.

[0049] In one embodiment, a system for enforcing data privacy is disclosed, that includes an input/output coupled to a sensor configured to produce sensor data comprising personal identifying data, an intermediate storage configured to receive sensor data from the sensor; and a blur unit coupled to the intermediate storage and configured to identify personal identifying data of the sensor data, produce obfuscated sensor data by obfuscating at least a portion of the personal identifying data, and provide the obfuscated sensor data to the intermediate storage.

[0050] The intermediate storage further includes a blur validation unit configured to generate a flag responsive to identifying personal identifying data in the obfuscated sensor data. The system further includes a data storage device (DSD) configured to receive obfuscated sensor data from the intermediate storage, the DSD being coupled to the blur unit, the blur unit further configured to identify personal identifying data in the obfuscated sensor data. The DSD further includes a second blur validation unit configured to generate a flag if personal identifying data is identified in the obfuscated sensor data. The system further includes a user interface configured to provide obfuscated sensor data to a user. The DSD is a non-volatile data storage device. The blur unit is further configured to overwrite the personal identifying data. The intermediate storage is a volatile data storage device.

[0051] In another embodiment, a system for storing data is disclosed that includes an input/output coupled to a sensor, an intermediate storage (IS), a data storage device, and a processor configured to execute a method for enforcing data privacy. The method includes receiving sensor data from the sensor comprising personal identifying data at the IS, identifying the personal identifying data at the IS, and generating obfuscated sensor data at the IS by obfuscating at least a portion of the personal identifying data.

[0052] The method further includes validating the obfuscated sensor data with a blur validation unit of the IS device, generating a flag responsive to identifying personal identifying information identified in the obfuscated sensor data. The method further includes receiving, by the data storage device, the obfuscated sensor data, from the IS and identifying personal identifying data in the obfuscated sensor data in the data storage device. The method further includes, responsive to validating the obfuscated sensor data with a second blur validation unit, generating a flag indicating personal identifying data is identified in the obfuscated sensor data. The method further includes providing the obfuscated sensor data to a user interface. The data storage device is a non-volatile data storage device. The IS is a volatile data storage device.

[0053] In another embodiment, a controller for a data storage system is disclosed that includes a memory means for storing computer-readable instructions, and a processor means configured to read computer-readable instructions that cause the processor to execute a method for enforcing data privacy. The method includes receiving sensor data comprising personal identifying information at an intermediate storage (IS) means; obfuscate at least a portion of the sensor data comprising personal identifying information at the IS means, to generate obfuscated personal identifying information; and provide the sensor data to a data storage device (DSD) means.

[0054] The computer-readable instructions further cause the processor to overwrite the personal identifying information. The computer-readable instructions further cause the processor to validate the sensor data at the IS means and flag the sensor data, responsive to determining that the sensor data contains personal identifying information that is not obfuscated. The computer-readable instructions further cause the processor to obfuscate at least a portion of the sensor data that contains personal identifying data that is not obfuscated personal identifying information in the DSD, to generate additional obfuscated personal identifying information. The computer-readable instructions further cause the processor to overwrite personal identifying information.

[0055] While the foregoing is directed to embodiments of the present disclosure, other and further embodiments of the disclosure may be devised

without departing from the basic scope thereof, and the scope thereof is determined by the claims that follow.

WHAT IS CLAIMED IS:

1. A system for enforcing data privacy, comprising:
an input/output (I/O) coupled to a sensor configured to produce sensor data comprising personal identifying data;
an intermediate storage configured to receive sensor data from the sensor;
and
a blur unit coupled to the intermediate storage and configured to identify personal identifying data of the sensor data, produce obfuscated sensor data by obfuscating at least a portion of the personal identifying data, and provide the obfuscated sensor data to the intermediate storage.
2. The system of claim 1, wherein the intermediate storage further comprises a blur validation unit configured to generate a flag responsive to identifying personal identifying data in the obfuscated sensor data.
3. The system of claim 1, further comprising a data storage device (DSD) configured to receive obfuscated sensor data from the intermediate storage, the DSD being coupled to the blur unit, the blur unit further configured to identify personal identifying data in the obfuscated sensor data.
4. The system of claim 3, wherein the DSD further comprises a second blur validation unit configured to generate a flag if personal identifying data is identified in the obfuscated sensor data.
5. The system of claim 3, further comprising a user interface configured to provide obfuscated sensor data to a user.
6. The system of claim 3, wherein the DSD is a non-volatile data storage device.
7. The system of claim 1, wherein the blur unit is further configured to overwrite the personal identifying data.

8. The system of claim 1, wherein the intermediate storage is a volatile data storage device.
9. A system for storing data, comprising:
an input/output coupled to a sensor;
an intermediate storage (IS);
a data storage device; and
a processor configured to execute a method for enforcing data privacy, the method comprising:
receiving sensor data from the sensor comprising personal identifying data at the IS;
identifying the personal identifying data at the IS; and
generating obfuscated sensor data at the IS by obfuscating at least a portion of the personal identifying data.
10. The system of claim 9, the method further comprising validating the obfuscated sensor data with a blur validation unit of the IS, generating a flag responsive to identifying personal identifying information identified in the obfuscated sensor data.
11. The system of claim 9, the method further comprising:
receiving, by the data storage device, the obfuscated sensor data, from the IS; and
identifying personal identifying data in the obfuscated sensor data in the data storage device.
12. The system of claim 9, the method further comprising, responsive to validating the obfuscated sensor data with a second blur validation unit, generating a flag indicating personal identifying data is identified in the obfuscated sensor data.
13. The system of claim 11, the method further comprising providing the obfuscated sensor data to a user interface.

14. The system of claim 9, wherein the data storage device is a non-volatile data storage device.
15. The system of claim 9, wherein the IS is a volatile data storage device.
16. A controller for a data storage system, comprising:
a memory means for storing computer-readable instructions; and
a processor means configured to read computer-readable instructions that cause the processor to execute a method for enforcing data privacy, the method comprising:
receive sensor data comprising personal identifying information at an intermediate storage (IS) means;
obfuscate at least a portion of the sensor data comprising personal identifying information at the IS means, to generate obfuscated personal identifying information; and
provide the sensor data to a data storage device (DSD) means.
17. The controller of claim 16, wherein the computer-readable instructions further cause the processor to overwrite the personal identifying information.
18. The controller of claim 16, wherein the computer-readable instructions further cause the processor to:
validate the sensor data at the IS means; and
flag the sensor data, responsive to determining that the sensor data contains personal identifying information that is not obfuscated.
19. The controller of claim 16, wherein the computer-readable instructions further cause the processor to:
obfuscate at least a portion of the sensor data that contains personal identifying data that is not obfuscated personal identifying information in the DSD, to generate additional obfuscated personal identifying information.
20. The controller of claim 19, wherein the computer-readable instructions further cause the processor to overwrite personal identifying information.

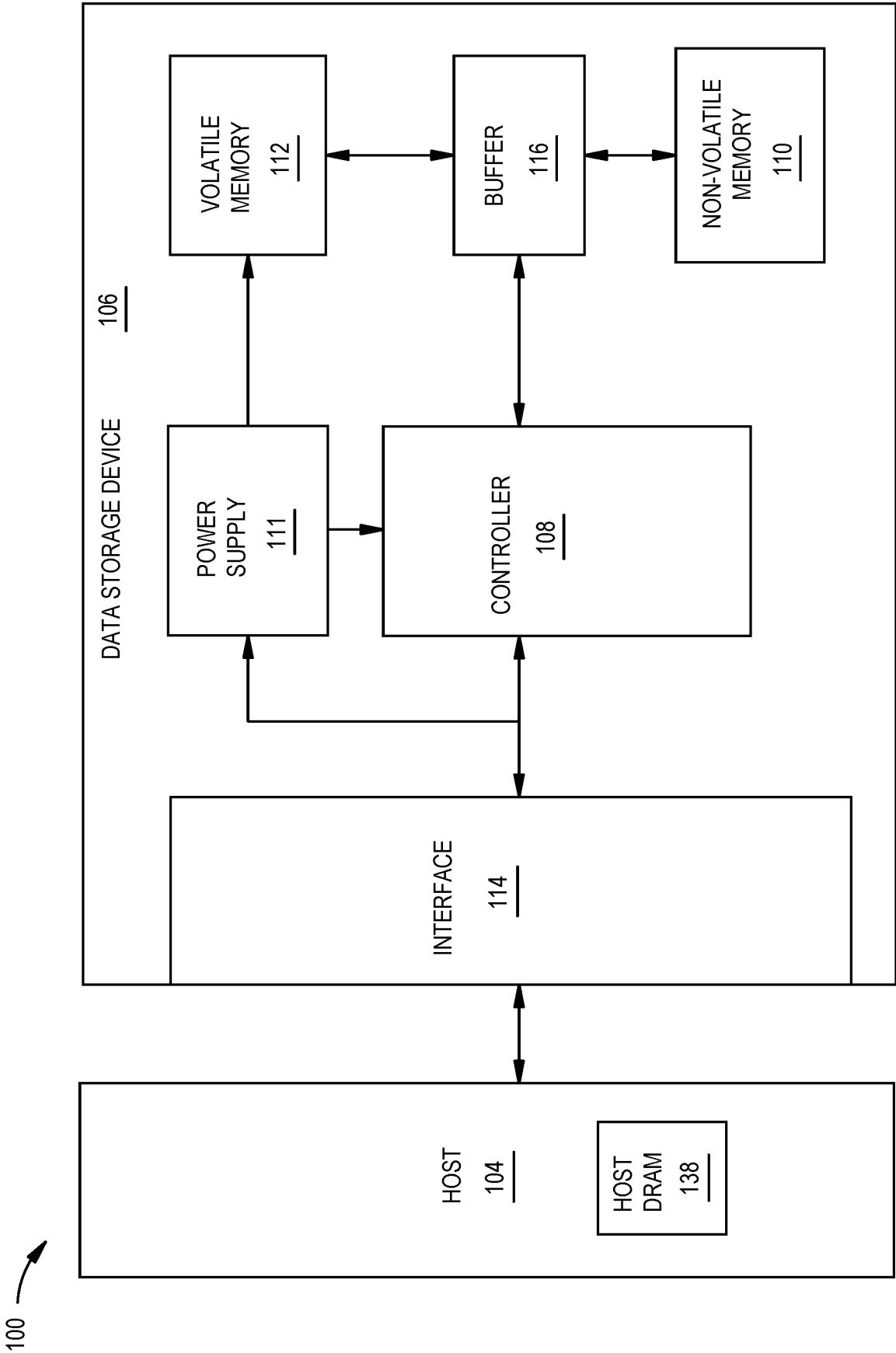


FIG. 1

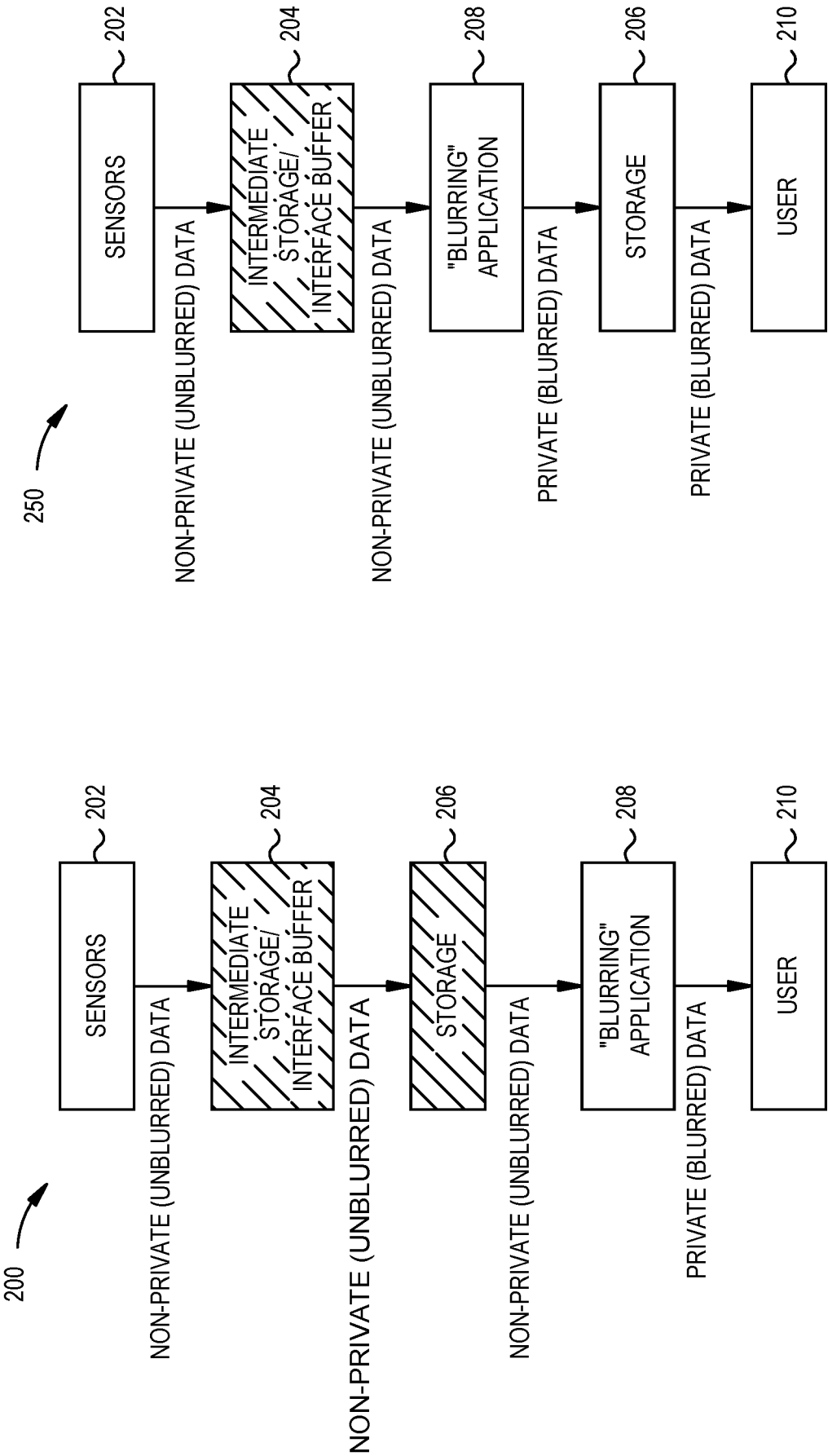


FIG. 2A

FIG. 2B

300 ↗

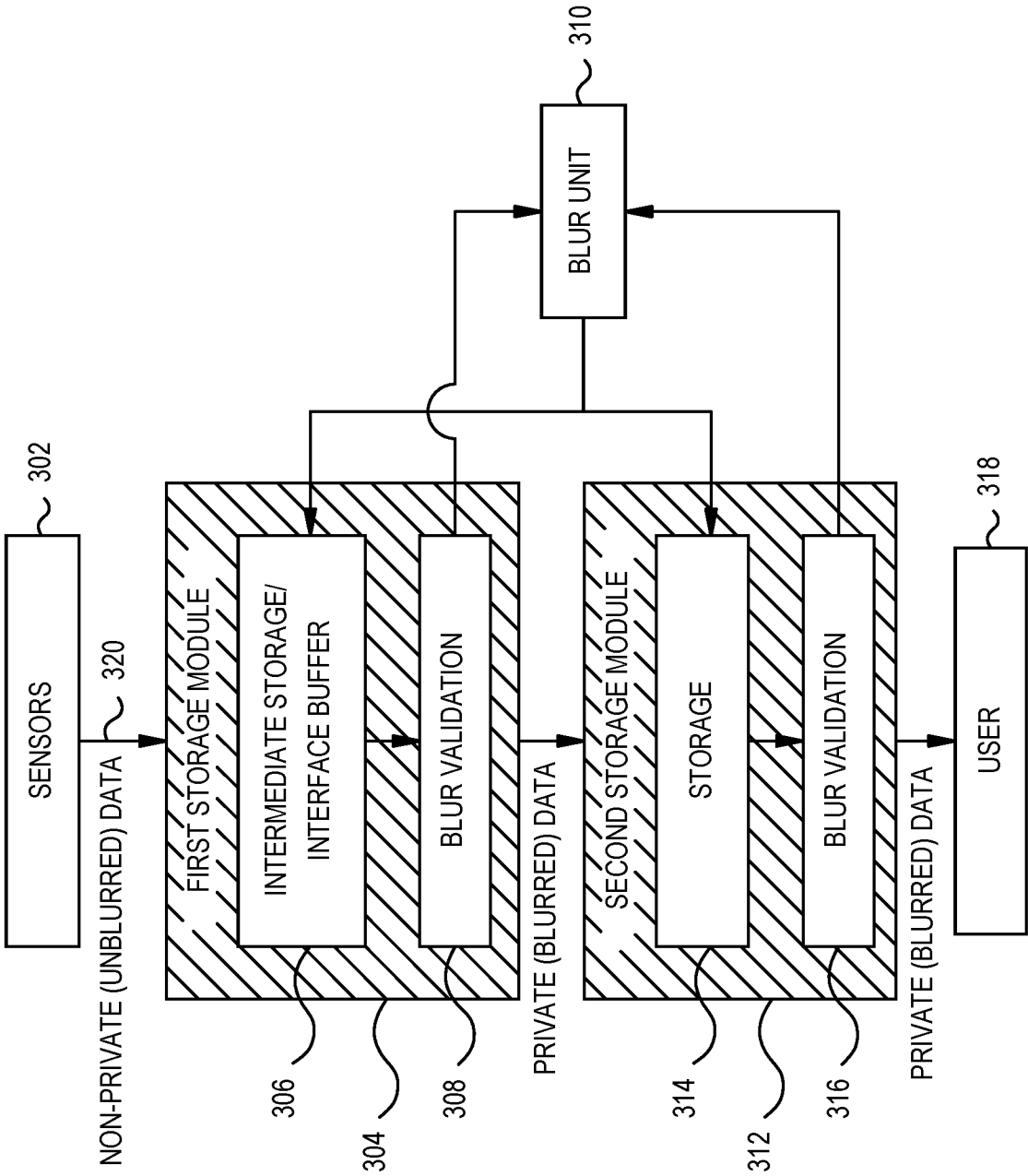


FIG. 3

400

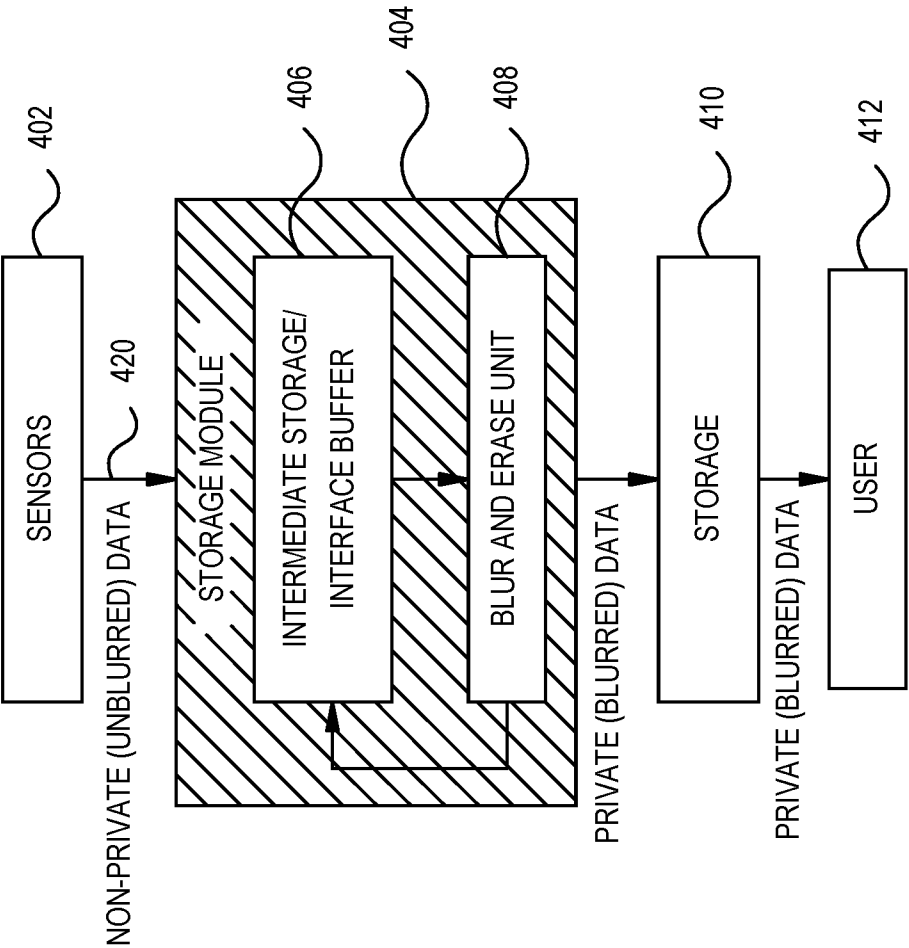


FIG. 4

5/5

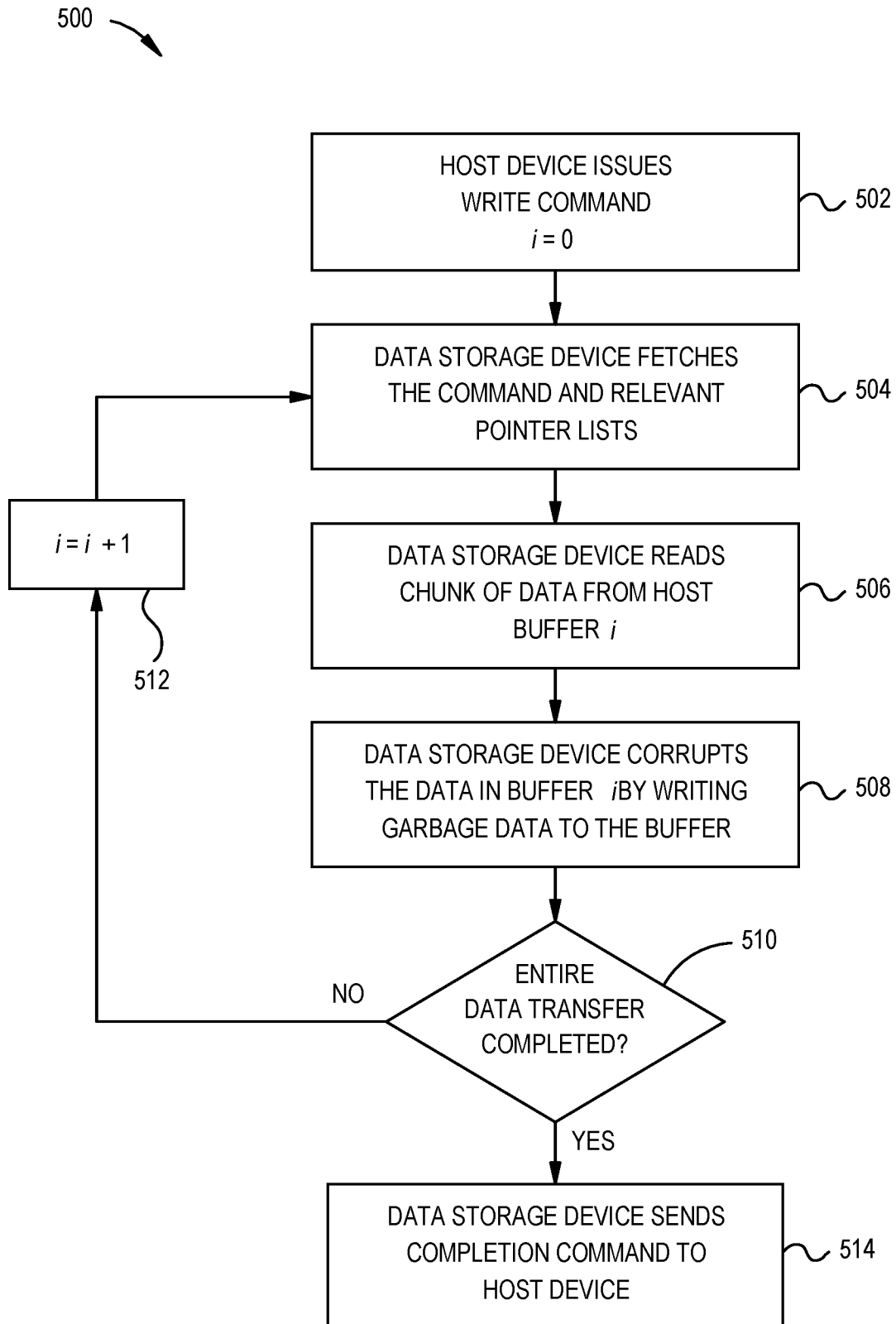


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2022/013358

A. CLASSIFICATION OF SUBJECT MATTER G08B 13/196 (2022.01)i; G06F 21/62 (2022.01)i CPC:G08B 13/19686; G06F 21/6245 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) G08B 13/196; G06F 21/62 CPC:G08B 13/19686; G06F 21/6245 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Databases consulted: Esp@cenet, Orbit		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2016180460 A1 (DEUTSCHE TELEKOM AG [DE]) 17 November 2016 (2016-11-17) ALL DOCUMENT	1,4,5,7-9,13,16,17,20
X	US 2019377958 A1 (BOSCH GMBH ROBERT [DE]) 12 December 2019 (2019-12-12) ALL DOCUMENT	2,4,8,10-12,15,18,19
X	US 2006064384 A1 (THE REGENTS OF THE UNIVERSITY OF CALIFORNIA) 23 March 2006 (2006-03-23) ALL DOCUMENT	1,4,8,15
X	EP 2429182 A2 (SMARTSPECTOR ARTIFICIAL PERCEPTION ENGINEERING GMBH? [AT]) 14 March 2012 (2012-03-14)	3,4,6,8,14,15
☐ 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 “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 09 May 2022		Date of mailing of the international search report 09 May 2022
Name and mailing address of the ISA/IL Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Israel Telephone No. 972-73-3927217 Email: pctoffice@justice.gov.il		Authorized officer POLAT Ofir Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/US2022/013358

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2016180460	A1	17 November 2016	WO	2016180460	A1	17 November 2016
				EP	3295696	A1	21 March 2018
US	2019377958	A1	12 December 2019	US	2019377958	A1	12 December 2019
				US	10956752	B2	23 March 2021
				CN	110036422	A	19 July 2019
				DE	102016223859	A1	30 May 2018
				EP	3549115	A1	09 October 2019
				EP	3549115	B1	29 September 2021
				ES	2901388	T3	22 March 2022
				WO	2018099689	A1	07 June 2018
US	2006064384	A1	23 March 2006	US	2006064384	A1	23 March 2006
				US	7940302	B2	10 May 2011
				WO	2006031988	A2	23 March 2006
				WO	2006031988	A8	04 May 2006
				WO	2006031988	A9	22 June 2006
				WO	2006031988	A3	11 October 2007
EP	2429182	A2	14 March 2012	EP	2429182	A2	14 March 2012
				EP	2429182	A3	08 January 2014
				AT	510352	A1	15 March 2012