SECURE ARTIFICIAL INTELLIGENCE (SAI) SYSTEM

BACKGROUND OF THE INVENTION

[0001] Improvements to privacy, data security, and explainability are needed in computing environments when using artificial intelligence models.

BRIEF SUMMARY OF THE INVENTION

[0002] One embodiment of the invention is a secure computing system comprising: one or more processors, a public subsystem, and a private subsystem. The public subsystem communicatively coupled with a first port and configured to connect to a network, the first port capable of transferring artificial intelligence data to a device that is capable of being communicatively coupled with a second port of the private subsystem. The private subsystem communicatively coupled with the second port, the private subsystem configured to execute an artificial intelligence system configured using the artificial intelligence data and is incapable of connecting to the network.

[0003] Additionally, an embodiment of the invention is a device configured to store data, the device comprising: a housing, a connector configured to connect to and be communicatively coupled with a secure bus port of a secure computing system, the secure computing system including at least two isolated subsystems, and two or more data channels that may send and receive data independently of one another. The device further comprising one or more processors and one or more memory storing instructions. Upon execution of the one or more memory storing instructions by the one or more processors, the device is configured to authenticate a user and simultaneously send and receive data to and from the secure bus port of a public subsystems or a private subsystem of the secure computing system.

[0004] Additionally, an embodiment of the invention is a power splitting system comprising a cord for connection to an electrical power source and a plurality of output modules in electrical connection with the cord. Each output module in the plurality of output modules is independent of all other output modules in the plurality of output modules. The power splitting system further comprising a switch configured to prevent tampering, wherein an activation of the switch

causes the power splitting system to become inoperable. Further, each output module in the plurality of output modules is independent of all other output modules in the plurality of output modules.

[0005] A better understanding of the nature and advantages of embodiments of the invention may be gained with reference to the following detailed description and accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 illustrates a system according to an embodiment.

[0007] FIG. 2 illustrates a system according to an embodiment.

[0008] FIG. 3 illustrates a system according to an embodiment.

[0009] FIG. 4 illustrates a system according to an embodiment.

[0010] FIG. 5 illustrates a system according to an embodiment.

[0011] FIG. 6 illustrates a system according to an embodiment.

[0012] FIG. 7 illustrates a method for transferring data between one subsystem and another, according to an embodiment.

[0013] FIG. 8 illustrates a method for transferring data between one subsystem and another, according to an embodiment.

DETAILED DESCRIPTION OF THE INVENTION

[0014] Current computing environments present a risk of information being shared inadvertently (e.g., sharing happening by design but without knowledge of a user, sharing happening due to an accident of a user, sharing caused by malicious files, etc.). In current systems, there's always a risk of exposure or leakage since all hardware, programs, and machine learning models may be accessible by and/or connected to the internet. In many cases, artificial intelligence models will use user input to create model output and then retain data supplied by the user to continue training one or more models. Thus, input from users may not be kept private and may be used to produce future output of the artificial intelligence model. Further, how and why the artificial intelligence model was developed may not be obvious to the user with current methods of training artificial intelligence models.

[0015] Embodiments of the disclosure address these problems and other problems individually and collectively.

[0016] Current solutions may use antivirus software to increase system security, keep shared data in remote storage that is meant to be secure, completely disconnect a system from the internet, or acknowledge and submit to data sharing altogether. However, these solutions do not sufficiently address the problems and/or are too limiting.

[0017] To solve these problems, an embodiment allows for a secure computing system to include a private subsystem and a public subsystem. The private subsystem may hold important and sensitive data. The private subsystem can operate without a connection to the internet. Thus, in an embodiment, the private subsystem can operate without ever having a direct connection to the internet and still allow for a user to use a model that does not require user data being transferred to a remote location relative to the private subsystem. The public subsystem may be capable of connecting to the internet and may be able to access online resources, network resources, and/or other public data. The public subsystem may be capable of allowing artificial intelligence model to connect to remote systems so that public artificial intelligence models may be enhanced by data used on the local secure computing system.

[0018] FIG. 1 illustrates a system according to an embodiment.

[0019] The secure computing system illustrated as system 100 may include a private subsystem, a public subsystem, a toggle switch 108, a first display system 114, a second display system 112, integrated input devices, a private subsystem bus port set, a public subsystem bus port set, a secure bus port, other peripherals, and a power splitting system 102.

[0020] Further, although not depicted, the secure computing system may also include a central processing unit (CPU), a graphics processing unit (GPU) a storage system, and a memory system. These parts of the secure computing system will be further described herein, such as with respect to FIGS. 5 and 6.

[0021] The public subsystem may be capable of connecting to the internet and can access online resources and public data (e.g., network data). In this mode interactions with artificial intelligence models may be connected to the outside world and directly or indirectly used to enhance the public artificial intelligence models.

[0022] The private subsystem may be designed to hold important and sensitive data.

[0023] The private subsystem may function like a secure vault for storing sensitive data or unique creations. The private subsystem may include independent processing capabilities, it may run artificial intelligence models that are loaded onto it, and may ensure sensitive computations (e.g., data processing, output generation, and/or learning from the data, etc.) occur without risk of exposure.

[0024] In an embodiment, the private subsystem is not capable of connecting to the internet (e.g., no ethernet connectivity, no Wi-Fi connectivity, etc.). When the private subsystem does not have the capability to access the internet, the ability for malicious and/or unauthorized access to the device can be reduced. Further, the capability of the device to transmit data to a remote source is reduced and requires further steps to be taken (typically non-passive steps that require user interaction with the private subsystem).

[0025] In some embodiments, the private subsystem is capable of connecting to a network (e.g., the internet) or connecting with one or more other devices using Wi-Fi, Bluetooth, or another wired or wireless communication technology.

[0026] The private subsystem may be capable of training and/or running artificial intelligence models. The artificial intelligence models being run by the private subsystem may be artificial intelligence models that do not require an internet connection and/or network access. For example, the artificial intelligence models may be run locally on the private subsystem and do not rely on cloud computing resources that are remote to the device and may then require device from the data to be transmitted to a location that is remote from the device.

[0027] By running artificial intelligence models locally to the private subsystem, the ability to retain data locally, not share data (e.g., confidential data, generated data, etc.), not share artificial intelligence model output, etc. is better enabled. Accordingly, the private subsystem has the capability of broadening ways that artificial intelligence models can be used and increasing data protection and privacy.

[0028] Since artificial intelligence models may be trained and run locally to the private subsystem, it is possible that an artificial intelligence model may be trained for specifical tasks that are being completed locally. As such the artificial intelligence models that are trained

locally may be refined to be better suited for the type of tasks that are performed by the secure computing system and/or user of the secure computing system.

[0029] For example, creative professionals (artists, writers, photographers, bakers, chiefs, song writers, video editors, dress designers, freelancers in all fields, etc.) can use the disclosed secure computing system, to create new work streams and art without having to input disclose data to the public and/or cloud-based artificial intelligence models. Creative professionals can download and use the latest available public artificial intelligence models, in a secure and private setting. They can train the downloaded artificial intelligence models in a secure manner in the direction or modality of their choice.

[0030] The private subsystem (or public subsystem) may include a biometric authentication system or other authentication system to increase system security and help restrict access from unauthorized users. The authentication system may be configured to periodically ensure that a user is authorized to be using the subsystem, in an embodiment. In an embodiment, the authentication system checks if a user is authorized to be using the subsystem when the subsystem is becomes activated, when the a artificial intelligence model is used, when data is attempted to be imported, when data is attempted to be exported, etc.

[0031] The private subsystem and the public subsystem may operate completely independently or partially independently of one another. In an embodiment, the private subsystem may have a cooling mechanism, power supply, and/or operating system that is independent of the public subsystem. For example, in an embodiment, the private subsystem runs a different operating system than the public subsystem. In an embodiment, the private subsystem runs a custom operating system built for the specific purpose of functioning with a private subsystem and/or performing functions like those performed by the private subsystem (e.g., optimized for artificial intelligence related operations).

[0032] The private subsystem and public subsystem may also have an airgap and the airgap may be enforced by a non-conductive barrier. Such an air gap may be capable of maintain electrical and/or physical separation between the private subsystem and the public subsystem to increase the security of the secure computing system. In an embodiment, a faraday cage may be used around one or more components (e.g., around one or more components of the private subsystem). The faraday cage may protect the components from external magnetic fields that

could gain information from the components and/or augment the data stored and/or processed by the components.

[0033] Further, in an embodiment, each of the private subsystem and the public subsystem may be housed within its own thermally insulated compartment for heat management. In an embodiment, each of the subsystems may include its own audio drivers and/or codec chips to ensure privacy between the subsystems. In an embodiment, other components may be shared or be duplicative between the private subsystem and the public subsystem. For example, an embodiment may include a separate GPU within each of the public subsystem and the private subsystem.

[0034] Additionally, in an embodiment, each subsystem may operate on encrypted data and/or store encrypted data. In an embodiment, each of the subsystems may perform one or more data encryption techniques.

[0035] In an embodiment, the public subsystem and the private subsystem may be included within separate housing and each respective subsystem may be capable of functioning without the other subsystem being nearby. For example, the public subsystem could operate in a first room and a private subsystem may operate in a second room. In an embodiment, it is possible for the private subsystem and the public subsystem to each be powered on at the same time. One embodiment of the secure computing system or a subsystem of the secure computing system may include a device with the formfactor of a tablet or mobile phone.

[0036] In an embodiment the secure computing system may be more akin to a desktop instead of a laptop and therefore not as easily mobilized. A larger version of the secure computing system (possible without integrated displays or other components) may make it easier for components to be swapped, removed, added, customized, have greater processing capabilities, etc.

[0037] In an embodiment, the secure computing system may include at least one of a public subsystem or a private subsystem. In an embodiment, the secure computing system may include one or more public subsystems and one or more private subsystems. In an embodiment, a single public subsystem may transfer data to and/or from one or more private subsystem and/or secure bus devices simultaneously. An embodiment where there is a many-to-one private subsystem-to-

public subsystem, or vice versa, may be a cost effective and/or resource effective measure for users of such public subsystems and/or private subsystems.

[0038] In an embodiment, the secure computing system may be designed as an add on or a module to be integrated into existing devices like laptops, desktops, tablets, mobile phones, etc.

[0039] The first display system 114 and second display system 112, may be used to project and render the processed or in-process information via the operating system and software. The first display system 114 may be a touchscreen and may be able to swivel and pivot on more than one axis.

[0040] The first display system 114 and/or second display system 112 may be used to display the information that shows the interim status of operations of artificial intelligence models and other in-progress information of other software. Such information may allow a user to re-direct the software and artificial intelligence models that might be 'learning' in an unwanted direction. The first display system 114 and/or second display system 112 may allow a user to observe how an artificial intelligence model is being built and processing the logic of task execution. This transparency allows the user to interrupt and redirect the artificial intelligence model as required.

[0041] Thus, the first display system 114 and/or second display system 112 addresses the so-called "black box" problem in artificial intelligence where the decision-making process is opaque to the user. By allowing users to see which artificial intelligence model is active and its logic when making decisions, it brings a level of transparency to artificial intelligence that's lacking in other systems and may assist the model improve performance (e.g., upon iterations). The decision making process and artificial intelligence model structure may be monitored in real time.

[0042] Through the use of the first display system 114, the second display system 112, and/or user feedback regarding artificial intelligence model(s) the time to desires results can be reduced. Additionally, the chances of artificial intelligence hallucinations can be reduced. A user may be allowed to interact with visually represented portions of an artificial intelligence model (e.g., pathways, neurons, weights, decisions trees, complex data, processes, past performance, past decisions, debug, trends, explanations, etc.) to trigger detailed expositions of selected elements.

Such data may be capable of being logged and then transferred to other private subsystem, public subsystem, and/or other computing systems (e.g., for further analysis).

[0043] In an embodiment, a secure computing system may have one or more display systems (embodiments are not limited to having two display systems).

The user may be able to configure the details, level of detail, the presentation style, etc. they are presented with by the display and/or other output devices. Such configurations may allow for increased artificial intelligence model performance and reduce the time it takes to train the artificial intelligence model. Such user feedback may help an artificial intelligence model learn objectively and/or subjectively more efficiently.

[0044] In an embodiment, before output is produced by a display system or another output device, the secure computing system may perform authentication to confirm that an authorized user is using the secure computing system.

[0045] In an embodiment, the first display system 114, second display system 112, integrated input devices, and/or other peripherals may all be used in each of the public subsystem and private subsystem. In an embodiment, some, none, or all of the firmware, electronics drivers, and related controller electronics for the respective components (e.g., first display system 114, second display system 112, integrated input devices , etc.) may be separately stored on the public subsystem and the private subsystem. Further, in an embodiment, the public subsystem and private subsystem will have separate firmware, electronics drivers, and related controller electronics for a respective component than the other subsystem (private subsystem or public subsystem, respectively).

[0046] Keyboard and Mousepad are common between the public and private AI subsystems, the firmware, electronic drivers, and related controller electronics are separate.

[0047] The first display system 114, second display system 112, and/or other user interfaces that may be included within or attachable to the secure computing system may also be capable of representing the battery status of the secure computing system as a whole, or respectively for each of the private subsystem and the public subsystem, simultaneously or individually. For example, the battery status and other statuses (alerts, activated subsystem (e.g., public subsystem or private subsystem), artificial intelligence model information, hardware information, etc.) of

the active subsystem may be presented on a first display screen, second display screen, LED, via backlights of a keyboard (e.g., color or backlight may correspond to the active subsystem), and/or audibly via a speaker (integrated or external), or another user interface.

[0048] The integrated input devices may be input devices that are not easy for a user to disconnect from the secure computing system or one of the subsystems. For example, an mousepad, touchscreen, a switch, a microphone, a camera, and/or a keyboard that is part of the same housing as the secure computing system or one of the subsystems may be considered to be an integrated input device. In an embodiment, the touchpad may be a vertically-oriented touchpad positioned to the right of the keyboard.

[0049] The secure computing system or one of the subsystems may also include integrated output devices such as a monitor, speaker, light, haptics, etc.

[0050] Other non-integrated input and/or output devices may also be connected to the secure computing system or one of the private subsystem or public subsystem, such as a headset, keyboard, a camera, monitor, lights, speakers, etc. Such devices may be considered to be other peripherals.

[0051] The private subsystem bus port set may be capable of allowing for transferring of information (e.g., untrained artificial intelligence models, trained artificial intelligence models, training datasets, personal data, or other data) to and/or from the public subsystem (e.g., via a secure bus device), secure computing system adapters, peripherals, memory devices, etc.

[0052] The private subsystem bus port set may include one or more bus ports, such as a USB, HDMI, Micro-SD, Ethernet, or any other conventional I/O port. In some embodiments, the secure bus port is an unconventional secure computing system port. The secure bus port is discussed in more detail below.

[0053] The public subsystem bus port set, may be capable of allowing for transferring of information (e.g., untrained artificial intelligence models, trained artificial intelligence models, training datasets, personal data, or other data) to and/or from the private subsystem (e.g., via a secure bus device), secure computing system adapters, peripherals, memory devices, etc. The public subsystem bus port set, may also be capable of allowing for data to be transferred to and/or from other devices on a network (e.g., LAN, WAN, internet, etc.).

[0054] The public subsystem bus port set and/or the private subsystem bus port set may also include ports for transfer of power (e.g., obtaining power from the power splitting system 102, obtaining power from a power source, charging a mobile device, etc.).

[0055] None, some, or all of the bus ports that are a part of the public subsystem bus port set may also be part of the private subsystem bus port set.

[0056] The secure computing system adapters may be hexagonally shaped, in some embodiments. The secure computing system adapters may accommodate adapters for external accessories such as webcams, headphones, motion sensor devices, and microphones. The secure computing system adapters may be stored in a flip-out compartment on the right side of the system.

[0057] The secure bus port may be capable of allowing for transferring of information (e.g., artificial intelligence models, training datasets, personal data, or other data) between the private subsystem and public subsystem. In an embodiment, the secure bus port can have a secure bus device connected to it. In an embodiment, the secure bus device has additional security technology such as biometrics (e.g., fingerprint recognition) The secure bus device is discussed in more detail with respect to at least FIGS. 7 and 8. The secure bus port is capable of facilitating control of what data is transferred between the public subsystem and the private subsystem, and when. In some embodiments, the secure computing system includes at least one secure bus port for the private subsystem and at least one other secure bus port for the public subsystem. The secure computing system port may be shaped to allow for more data to be sent and/or received in a given amount of time. In an example, the secure bus port may be a shaped hexagonally. The secure bus port may have more than one data channel (e.g., may have 6 independent data channels). Increasing the amount of data channels may enable an increase in the rates of data transfers. Further, independent data channels may allow for simultaneous read and write operations to occur between a secure bus port and a secure bus device. Such designs may drastically reduce the time spent on data-intensive tasks. Reducing the time to transfer data between the secure bus port and the secure bus device (and possibly, thereby between the public subsystem and private subsystem) is greatly beneficial for environments where large amount of data may be transferred (e.g., in environments reliant on large amounts of data such as artificial intelligence environments).

[0058] In an embodiment, data across all of the channels of the secure bus port is equivalent or close to equivalent to increase data transfer rates. Further, in an embodiment, the secure bus port may be designed with heat management features to reduce the temperature of the secure computing system, public subsystem, private subsystem, and/or the secure bus device.

[0059] Individual ports of the secure computing system may be located on any side of the secure computing system apparatus and the secure computing system may have any number of each type of port.

[0060] The toggle switch 108 may be a manual toggle switch 108 (e.g., manually moved using a finger). The toggle switch 108 (e.g., having a Single-Pole, Double Throw (SPDT) design) or another switching mechanism (e.g., toggle button, physical reconfiguration of components, etc.) may be capable of ensuring that a single subsystem of the secure computing system is operating at a single time. The toggle switch 108 may facilitate enabling input methods (e.g., integrated peripherals, peripherals), memory devices, displays, etc. to interact with the currently active subsystem (e.g., private subsystem or public subsystem). The toggle switch 108 may include a safety lock mechanism to decrease the likelihood of an unintended toggling of the switch and thereby the active subsystem. In some embodiments, the toggle switch 108 is in the form of a software switch. For example, upon bootup of the secure computing system, a decision may be made (e.g., using onscreen prompts and/or selection) whether to use the private subsystem or the public subsystem.

[0061] The switch may enable the power splitting system 102 to ensure one subsystem (e.g., public subsystem) can be powered down while another subsystem (e.g., private subsystem) powers up. Such a mechanism may allow for reducing the risk of data loss and power surges. The manual toggle switch 108 or another switching mechanism may also be capable of controlling the power supplied to peripheral devices of the secure computing system and may be capable of ensuring that secure computing system components and peripherals operate in harmony.

[0062] The power splitting system 102 may be connected to a power source. The power splitting system 102 may be capable of splitting power from one power source into two power outputs that each connect to the secure computing system. One of the two power outputs may connect to a power reception system for the public subsystem. The other of the two power

outputs may connect to a power reception system for the private subsystem. Further, in some embodiments, the each of the private subsystem and public subsystem may include a battery supply that is independent of the other subsystem. Thus, each battery of each respective subsystem may be independently charged and/or depleted. In some embodiments, the private subsystem and the public subsystem share the same power reception system and/or battery. The power splitting system 102 is capable of reducing the risk of electrical interference between the private subsystem and the public subsystem due to the independent power pathways after the power source energy is split by the power splitting system 102.

[0063] In an embodiment, the at least a portion of the power cord is encapsulated within a thermally insulated and/or flame retarded material to increase the safety of the system. Such a designs also helps promote the efficient transmission of power and minimizes heat generated during operation of the secure computing system.

[0064] In an embodiment where the public subsystem and the private subsystem each receive a separate and independent power supply, each arm of the bifurcated cord from stemming from the power splitting system 102 may be regulated by individual power supply units (PSUs). The PSUs may be located within the power splitting system 102 or the secure computing system. Each PSU may be housed within a thermally insulated compartment, which may prevent heat transfer between the PSU and other components.

[0065] In an embodiment, the power splitting mechanism supplies power to one of the public subsystem or private subsystem at a single time. The power splitting system 102 may also facilitate a self-destruct feature of the secure computing system, one of the subsystems, and/or the power splitting system 102, and may include other features to reduce or avoid tampering.

[0066] Thus, embodiments of the power splitting system 102 may allow for increased energy efficiency.

[0067] Further, ends of the cords extending from the power splitting system 102 may include mechanisms to prevent the cords from being easily and/or accidentally disconnected so that the supply of power is not accidentally interrupted.

[0068] FIG. 2 illustrates a system according to an embodiment.

[0069] System 200 provides a different viewpoint perspective of system 100. The placement of the components, displays, ports, plugs, etc. may be configured differently and one of ordinary skill in the art would recognize with the benefit of this disclosure.

[0070] System 200 illustrates that a side of the secure computing system may include various ports, one or more of which may be a secure bus port. Further, one or more ports may be capable of interfacing with one of or both of the private subsystem and the public subsystem.

[0071] The housing of the secure computing system and/or one of the subsystems may include a window into the device so that a user may be able to see one or more components, lights, fans, etc. within the housing.

[0072] The housing of the secure computing system and/or one of the subsystems may include a panel, door, etc. that is removable so that one or more parts can more easily be swapped out, fixed, viewed, inserted, etc. The panel or other access controlling part of the housing may include screws, bolts, clips, etc. so that the housing cannot accidentally be opened and/or to ensure that they are not able to be opened too quickly. Material used for the housing of the secure computing system and/or the subsystems may be strong enough to withstand some impacts (e.g., anodized aluminum, reinforced plastics) and may be easily cleaned.

[0073] Either one of, or both of, the private subsystem and the public subsystem may additionally include a backup storage system (e.g., encrypted backup storage). Such storage may be useful for redundant data storage and/or additional data storage.

[0074] FIG. 3 illustrates a system according to an embodiment.

[0075] System 300 illustrates how the private subsystem 302 and public subsystem 304 may be situated with respect to one another. As can be seen, in an embodiment, the subsystems may be separated from one another with respect to an axis of the device. Thus, system 300 provides an example where the components of the private subsystem 302 are between the integrated input devices (e.g., keyboard, mouse trackpad, etc.) of the secure computing system and the public subsystem 304 of the secure computing system.

[0076] System 300 also illustrates that in an embodiment, the power splitting system 102 may be integrated into the secure computing system.

[0077] The power source may be a wall outlet, battery bank, wireless charger, or other form of power source.

[0078] FIG. 4 illustrates a system according to an embodiment.

[0079] Like system 300, system 400 also illustrates how the private subsystem 302 and public subsystem 304 may be situated with respect to one another. As can be seen, in an embodiment, the subsystem may be separated from one another with respect to an axis of the device. Thus, system 300 provides an example where the components of the private subsystem 302 and public subsystem 304 are located near each other, but neither is between the other subsystem and the integrated input devices.

[0080] Although, the integrated input devices (e.g., keyboard, num pad, trackpad) are shown in this figure to be on the portion of the secure computing system that would be akin to where a keyboard and trackpad may be on a traditional laptop computer, one of ordinary skill in the art would recognize that the integrated input devices may include other peripherals (e.g., lights, speakers, etc.), and some or all of them may be located on a different portion of the secure computing system. In an embodiment, all of the integrated input devices may be located on a different portion of the secure computing system or the secure computing system may not contain any integrated peripherals.

[0081] As illustrated in system 400, the power splitting system 102 may be external to the secure computing system in some embodiments.

[0082] FIG. 5 illustrates a system according to an embodiment.

[0083] System 500 illustrates an embodiment of a public subsystem (e.g., public subsystem 304).

[0084] A GPU 508 may be the central controlling unit for the processing of data. The GPU 508 may be used when running artificial intelligence models and may be used for display rendering.

[0085] A CPU 506 is also included in system 500. In some embodiments, the CPU 506 is used to aid the GPU 508 in processing tasks. In some cases, the GPU 508 may perform more

processing that the CPU 506. In some embodiments, the CPU 506 may be relied on for computational tasks that occur in series.

[0086] The user input signal to the GPU 508 and/or CPU 506 may be given via an integrated input device 306 (e.g., keyboard, mousepad, etc.), or peripherals 512 connected to the processing unit via a bus port set 504 (e.g., bus port set 106a and bus port set 106b).

[0087] External-public data may be transferred via an external wired/wireless connection 502 capability (e.g., external ethernet and/or wireless connection). The transfer of data to a public domain/internet may be accomplished via the external wired/wireless connection 502.

[0088] Transferring data from the public subsystem to the private subsystem may be accomplished by using a secure bus port 516 and a secure bus device 514.

[0089] Data may be stored in a permanent manner in a storage system 510 (e.g., internal SSD Storage System).

[0090] Volatile data that may be used as a buffer to speed up operations may be stored in a memory system 518 (e.g., DRAM).

[0091] Any number of display systems may also be included in system 500. System 500 depicts a first display system 114 and a second display system 112. Any of the included display systems may be used to project and render processed or in-process information computed by the operating system and software. Any of the included display systems may be used to display information showing the interim status of the operations of the artificial intelligence models and other in-progress information of other software. Such information allows the user to re-direct the software and artificial intelligence models that might be 'learning' in an unwanted direction. Any of the included display systems may be used to allow a user to observe how one or more artificial intelligence models are being trained and/or processing the logic of task execution. This transparency allows the user to interrupt and redirect the artificial intelligence model(s) as required.

[0092] The components discussed above (e.g., GPU 508), and others (fans, speakers, etc.) described herein may be configured to reduce the cross talk between one or more components. Such reduction in cross talk is capable of increasing data processing efficiency.

[0093] FIG. 6 illustrates a system according to an embodiment.

[0094] System 500 illustrates an embodiment of a private subsystem (e.g., private subsystem 302).

[0095] The private subsystem may not have connectivity via ethernet or wireless technology to the outside world, in some embodiments. Thus, in some embodiments the only source of connection for data transfer to and from the private subsystem may be via a secure bus port 616 using a secure bus device 514. In some embodiments, a secure bus port 616 is not required to transfer data to and/or from a secure bus device 514. In some embodiments, a secure bus device 514 is not required to transfer data to and/or from a secure bus port 616. In some embodiments, the private subsystem and/or the public subsystem does not include a secure bus port 616. In an embodiment, a secure bus port in the secure bus port(s) 616 may be a same or different bus port in the secure bus port(s) 516.

[0096] The private subsystem may include a CPU 606, a GPU 608, a storage system 610 (e.g., SSD storage system), a memory system 618, one or more bus ports in a bus port set 604, and/or one or more secure bus ports 616.

[0097] One or more of the components in the public subsystem and the private subsystem may be shared between the two systems (e.g., the first display system 114, the second display system 112, integrated input devices, peripherals, GPU, cameras, bus ports, secure bus ports, etc.). In some embodiments, none of the components of the public subsystem and private subsystem are shared (each subsystem has independent components).

[0098] Like the public subsystem, the private subsystem may include one or more display systems (e.g., first display system 114, second display system 112), integrated input devices 306, and peripherals 602. Such components may behave in a similar fashion as they had been described with respect to system 500. In some embodiments, even if components are shared between the public subsystem and the private subsystem, the firmware, electronic drivers, and/or related controller electronics may be separate and independent for each of the subsystems.

[0099] In some embodiments, one or more components of the private subsystem may be housed inside a Faraday cage, as illustrated by the dashed line in system 600. The faraday cage may provide additional privacy and data security compared to not including a faraday cage.

[0100] In some embodiments, the private subsystem will include a separate (and possibly different) operating system than the public subsystem. Some or all of the operating system, applications, artificial intelligence models, etc. used in operating the private subsystem may be preloaded onto the private subsystem during the process of manufacturing. In some embodiments, the software used by the private subsystem and/or the public subsystem may be downloaded via a software marketplace focused on providing software to such subsystems (e.g., artificial intelligence models that are capable of running in an offline environment, software optimized for the hardware included in the public subsystem and/or private subsystem, datasets (labeled and/or unlabeled), trusted software).

[0101] FIG. 7 illustrates a method for transferring data between one subsystem and another, according to an embodiment.

[0102] At step 702, a secure bus device is inserted into a first port of a first subsystem of a secure computing system. In an embodiment, the first port is a secure bus port. The first subsystem may be a private subsystem or a public subsystem. In an embodiment, instead of a secure bus device being used, another storage device is used for this step and the subsequent steps.

[0103] A secure bus device may be a device that is capable of transferring data at high speed to and from a computing system, may be password protected, may be protected using biometrics such as a fingerprint scanner (or other forms of authentication), may connect to a secure bus port, may be able to store large amounts of data, may have a heat sync (or other heat management system), may store encrypted data, may be shock resistant, may be water resistant, may be resistant to high velocity impacts, may be configured to consumer lower amounts of power, may be configured to not transfer data to more than one private subsystem, may be configured to only transfer data to specific secure computing systems, private subsystem, or public subsystem, and/or may include indicators (e.g., LED indicator) to signal when data transfer, authentication, etc. is occurring. As previously mentioned, the secure processing device may be designed to handle high speed data transfer (e.g., having six data channels, being hexagonally shaped, being able to read and write data at the same time, etc.).

[0104] In some embodiments, one or more secure processing devices are capable of being stored within a housing of a secure computing system and/or within a public subsystem or a private subsystem.

[0105] In an embodiment, the secure bus device may be configured to not transfer data to computing systems that are not a public subsystem or a private subsystem.

[0106] In an embodiment, the secure bus device may store terabytes of data. In an embodiment, a biometric sensor included within the secure bus device may be designed with liveness detection to prevent spoofing.

[0107] At step 704, data is transferred to the secure bus device from the first subsystem of the secure computing system using the first port. For example, the data may be artificial intelligence models, training data, software updates, applications, or other data.

[0108] At step 706, the secure bus device is removed from the first port of the first subsystem.

[0109] At step 708, the secure bus device is inserted into the secure bus of a second subsystem of the secure computing system.

[0110] In an embodiment, data cannot be transferred to the private subsystem from a memory device (e.g., secure bus device) unless the memory device was last, recently, or once before plugged into a corresponding public subsystem. The public subsystem may correspond to the private subsystem if the public subsystem is on an authorized subsystems list of the private subsystem, or if the private subsystem is part of the same secure computing system of the public subsystem, for example.

[0111] At step 710, the data stored on the secure bus device is transferred to the second subsystem (e.g., private subsystem or public subsystem) using the second port. The second port may be the same port as the first port. The second port may be a secure bus port.

[0112] Method 700 may allow for the private subsystem to have sensitive data and/or works (e.g., patient data, legal documents, unreleased songs, unreleased artwork, video, etc.) transferred to it in a private and efficient manner. Data may be created at the public subsystem (e.g., generated, downloaded, etc.). The data may include training data, artificial intelligence models, applications, etc. Once data is loaded on the private subsystem, the configuration of the private

subsystem may be capable of functioning completely offline and not require an internet connection. In some embodiments, the private subsystem is unable to be connected to the internet or another network. In an embodiment, data from the private subsystem that a user would like to send over a network or store on a device that is not a secure bus device may first need to be transferred to the public subsystem.

[0113] FIG. 8 illustrates a method for transferring data between one subsystem and another, according to an embodiment.

[0114] Method 800 illustrates another example method of using the public subsystem and the private subsystem of a secure computing system. Although method 800 illustrates using a secure bus port and a secure bus device, a non-secure bus port and/or a non-secure bus device may be used in some embodiments.

[0115] Thus, method 800 and other embodiments may allow for the private subsystem to be used in a more secure environment than the public subsystem. For example the private subsystem may have reduced risk or no risk of training data, input data, output data, or other data being accidentally and/or unknowingly sent to a source that is remote to the private subsystem. Further, embodiments may allow for models operating on the private subsystem to be further optimized, trained, and/or developed using data local to the private subsystem. Thus, a local and unique version of an artificial intelligence model originally obtained from a public or semi-public source is capable of being privately developed through the use of the private subsystem and the configuration of the secure computing system.

[0116] A non-exhaustive list of example regarding how the secure computing system may be used are considered below.

[0117] HealthCare professionals, law professionals, and other businesses can use the secure computing system and to keep patient and client information secure while using artificial intelligence models and software for improved productivity.

[0118] As a further example, government establishments, including military and confidential researchers could use this secure computing system to maintain the secrecy of the work streams while continuing to use the generative and other artificial intelligence technologies, currently

available and not yet available, for faster decisions, more accurate decisions, and/or increased security,

[0119] This secure computing system can be deployed in other applications where it is important to keep client, customer, and/or personal data secure and/or away from public or third party cloud storage/compute infrastructure. This secure computing system may also be beneficial to any data set that a user does not want to transmit over the wired or wireless networks. Further, the secure computing system can be used in other instances where a user wants a customized or personalized artificial intelligence model to run specific tasks to improve productivity in a secure manner.

[0120] Other embodiments of a secure computing system, public subsystem, and private subsystem are also considered. For example, it is beneficial to have embodiments where the secure computing system does not have a public subsystem but still includes a private subsystem.

WHAT IS CLAIMED IS:

1. A device configured to store data, the device comprising:

a housing;

a connector configured to connect to and be communicatively coupled with a secure bus port of a secure computing system, the secure computing system including at least two isolated subsystems;

two or more data channels that may send and receive data independently of one another;

one or more processors; and

one or more memory storing instructions that, upon execution by the one or more processors, configure the device to:

authenticate a user; and

simultaneously send and receive data to and from the secure bus port of a public subsystems or a private subsystem of the secure computing system.

2. A secure computing system comprising:

one or more processors;

a public subsystem, the public subsystem communicatively coupled with a first port and configured to connect to a network, the first port capable of transferring artificial intelligence data to a device that is capable of being communicatively coupled with a second port of a private subsystem; and

the private subsystem communicatively coupled with the second port, the private subsystem configured to execute an artificial intelligence system configured using the artificial intelligence data and is incapable of connecting to the network.

3. The secure computing system of claim 2, wherein the artificial intelligence system is configured to run artificial intelligence models and display information to a user that is informative about running processes of the artificial intelligence models as they are being trained.

4. The secure computing system of claim 2, wherein the second port is a secure bus port and includes six independent data channels, the data channels capable of independently receiving and transmitting data from a secure bus device.

5. The secure computing system of claim 2, wherein the first port and the second port can fit male plugs.

6. The secure computing system of claim 2, wherein an indicator indicates whether the public subsystem or the private subsystem is activated.

7. The secure computing system of claim 2, wherein the public subsystem is powered off when the private subsystem is powered on.

8. A power splitting system comprising:

a cord for connection to an electrical power source;

a plurality of output modules in electrical connection with the cord, wherein each output module in the plurality of output modules is independent of all other output modules in the plurality of output modules; and

a switch configured to prevent tampering, wherein an activation of the switch causes the power splitting system to become inoperable.