January 2020

INTELLIGENTLY LOCKING A DEVICE BASED ON CONTEXTUAL SIGNALS

Jonathan D. Hurwitz

Christina Gilbert

INTELLIGENTLY LOCKING A DEVICE BASED ON CONTEXTUAL SIGNALS

ABSTRACT

A system is described that enables a computing device (e.g., a mobile phone, smartwatch, tablet computer, etc.) to detect or couple with a companion computing device to detect various contextual signals and automatically lock the computing device based on the various contextual signals. The computing device may use one or more sensors (e.g., infrared cameras, near-field microwave sensors, cameras, microphones, etc.) to detect user inputs, measure wireless signal characteristics, capture images, determine a location of the computing device, etc. as contextual signals. The computing device may analyze these contextual signals to lock the computing device automatically (i.e., change the computing device from operating in a first access state to operating in a second access state that restricts usage of one or more features, applications, or other functionalities of the computing device relative to the first access state). For example, if a user walks away from the computing device, the computing device may use a radio detection and ranging (radar) system to detect that the user is no longer in front of the computing device and, in response, may automatically lock the computing device. In various instances, a companion computing device may couple with the computing device to detect or otherwise determine contextual signals which may be provided to and used by the computing device to lock the device automatically.

DESCRIPTION

Computing devices may include an auto-unlock feature to allow a user to unlock the computing devices without password entry. While the auto-unlock feature may be a common feature for computing devices, a user of the computing devices may want the computing devices

to be automatically locked as the user walks away from the devices. As such, it may be desirable to enable a computing device to detect various contextual signals and automatically lock the computing device based on the various contextual signals.

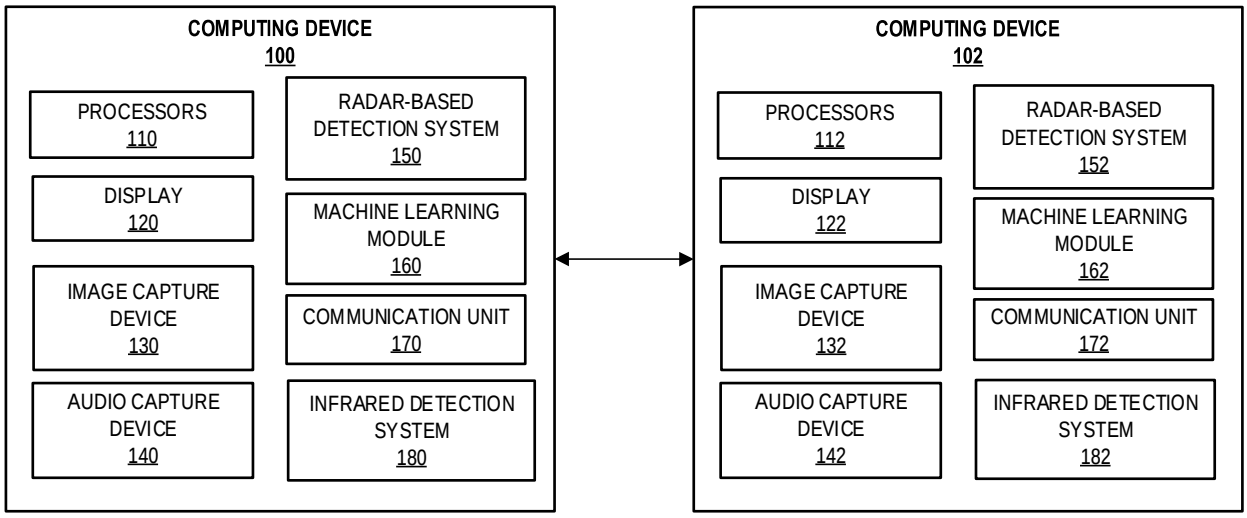

FIG. 1

Figure 1 above is a conceptual diagram illustrating an example computing device configured to detect or be coupled with a companion computing device to detect various contextual signals and automatically lock the computing device based on the various contextual signals. In the example of FIG. 1, each computing device 100 and companion computing device 102 represents an individual mobile or non-mobile computing device. Examples of computing device 100 include a mobile phone, a tablet computer, a laptop computer, a desktop computer, a server, a mainframe, a set-top box, a television, a wearable device (e.g., a computerized watch, a computerized eyewear, a computerized glove, etc.), a home automation device or system (e.g., an intelligent thermostat or a home assistant device), a personal digital assistant (PDA), a gaming system, a media player, an e-book reader, a mobile television platform, an automobile navigation or infotainment system, or any other type of mobile, non-mobile, wearable, and non-wearable computing device that contains a radar-based detection system which are configured to detect

various contextual signals and automatically lock the computing device based on the various contextual signals.

Computing device 100 includes processors 110, display 120, image capture device 130, audio capture device 140, radar-based detection system 150, machine learning module 160, communication unit 170, and infrared detection system 180. Examples of display 120 include a liquid crystal display (LCD), a thin-film-transistor display (TFT), an organic light-emitting diode display (OLED), etc.

Computing device 100 may receive various contextual signals from image capture device 130, audio capture device 140, radar-based detection system 150, and infrared detection system 180, after receiving explicit permission from the user. For example, image capture device 130 may function as an input device (e.g., a camera) to capture still images or videos. Audio capture device 140 may function as an input device (e.g., a microphone) to capture audio data from the ambient environment. Radar-based detection system 150 may provide a localized radar field, which may allow radar-based detection system 150 to detect the presence of a user or user inputs. Infrared detection system 180 may project infrared light dots onto the face of a user to create a dot pattern of the user's facial landscape and may capture images of the dot pattern that has been reflected back from the user's face. The captured or detected information may be provided to computing device 100 as contextual signals.

In response to receiving contextual signals, computing device 100 may automatically lock the device. For example, radar-based detection system 150 may use a microwave radio element to emit modulated radiation, ultra-wideband radiation, or sub-millimeter-frequency radiation at a predetermined frequency (e.g., 5GHz) to provide a localized radar field and may use an antenna element to detect interactions in the localized radar field. When radar-based

detection system 150 detects interactions in the localized radar field, processors 110 may process the detected interactions to provide behavioral data usable by machine learning module 160 to determine a behavior from the detected interactions in the localized radar field. Based on the determined behavior, computing device 100 may automatically lock the device. For example, if a user walks away from computing device 100, the computing device may use radar-based detection system 150 to detect that the user is no longer in front of computing device 100 and, in response, computing device 100 may automatically lock the device based on the detected behavior.

In another example, computing device 100 may use infrared detection system 180 to capture face images from the user and may automatically lock the device based on the captured face images. Infrared detection system 180 may include a proximity sensor and an ambient light sensor, a flood illuminator, a dot projector, and an infrared camera. Infrared detection system 180 may use the proximity sensor and the ambient light sensor to determine how much infrared light will be needed to illuminate the user's face for face recognition. The flood illuminator may produce infrared light to illuminate the user's face. The dot projector may project infrared dots onto the user's face to create a dot pattern of the user's facial landscape. Infrared detection system 180 may then use the infrared camera to capture a facial image of the dot pattern that has been reflected back from the user's face. Processors 110 may process the captured facial image to provide image data usable by machine learning module 160 to verify the identity of the user. If machine learning module 160 does not find a match with registered faces, computing device 100 may automatically lock the device.

In various instances, computing device 100 may use audio capture device 140 to capture audio data from the ambient environment periodically and automatically lock the device based

on the captured audio data. For example, audio capture device 140 may be configured to capture audio inputs from the current user of computing device 100 periodically, and processors 110 may process the audio inputs to provide audio data usable by machine learning module 160 to determine whether the current user is a known user. Based on the determination, computing device 100 may automatically lock the device.

Computing device 100 may also couple with companion computing device 102 to detect various contextual signals and automatically lock the computing device based on the various contextual signals. Communication unit 170 of communication device 100 may communicate with communication unit 172 of companion computing device 102 via one or more wired and/or wireless networks by transmitting and/or receiving network signals on the one or more networks. Examples of communication unit 170 include a network interface card (e.g., such as an Ethernet card), an optical transceiver, a radio frequency transceiver, or any other type of device that can send and/or receive information.

In one example, computing device 100 and companion computing device 102 may be communicatively coupled with each other using Bluetooth® low energy (BLE). For example, computing device 100 may determine that a detected BLE signal is from companion computing device 102 and may calculate a distance between computing device 100 and companion computing device 102 using received signal strength indicator (RSSI) for the BLE signal received from companion computing device 102. Computing device 100 may then automatically lock the device based on the calculated distance. For example, computing device 100 may automatically lock the device based on a determination that the distance between computing device 100 and companion computing device 102 exceeds a predetermined distance (e.g., 5 meters, 10 meters, etc.).

In another example, computing device 100 and companion computing device 102 may be communicatively coupled with each other using a network. The network may be a combination of any one or more public or private communication networks, for instance, television broadcast networks, cable or satellite networks, cellular networks, Wi-Fi® networks, broadband networks, and/or other type of networks for transmitting data (e.g., telecommunications and/or media data) between various computing devices. Companion computing device 102 may send device status (e.g., locked, unlocked) of companion computing device 102 to computing device 100 via the network. Computing device 100 may then automatically lock the device based on the received device status. For example, computing device 100 may automatically lock the device if companion computing device 102 is locked.

Computing device 100 may also automatically lock the device based on a combination of data received from image capture device 130, audio capture device 140, radar-based detection system 150, infrared detection system 180, and data received from companion computing device 102. For example, computing device 100 may use radar-based detection system 150 to detect the presence of a user or user inputs. Based on the detection of the presence of a user or user inputs, computing device 100 may verify the identity of the user using audio capture device 140 or infrared detection system 180. For example, in response to the detection of the presence of a user or user inputs from radar-based detection system 150 and after receiving explicit authorization from the user, computing device 100 may use audio capture device 140 to capture audio spoken by the user (i.e., a sample of the user's voice). Processors 110 may then process the captured audio to provide audio data usable by machine learning module 160 to determine whether the user is a known user.

In another example, in response to the detection of a user or user inputs from radar-based detection system 150, computing device 100 may use infrared detection system 180 to capture a pattern of the object (e.g., the user's face or other object) located in front of a dot projector of infrared detection system 180. The dot projector projects a grid of infrared dots onto the object located in front of the dot projector and an infrared camera captures images of the dot pattern. Using the images of the dot pattern, infrared detection system 180 generates a three-dimensional map of the object and may compare the three-dimensional map to a previously generated three-dimensional map of an authorized user. For example, infrared detection system 180 may provide the captured three-dimensional map of the object to machine learning module 160, which uses machine learning to determine if the captured three-dimensional map matches the three-dimensional map of the authorized user. If machine learning module 160 determines the user is not a known user, computing device 100 may automatically lock the device. In some examples, infrared detection system 180 is only used after detection of the presence of a user or user inputs, which may enable computing device 100 to save battery power by reducing the amount of time infrared detection system 180 may need to be powered to identity the user of computing device 100.

Computing device 100 may train machine learning module 160 by using data collected from a user. For example, computing device 100 may collect audio or image data of the user during each user identification process, and may use the collected audio or image data to refine a machine-learned model. For example, machine learning module 160 may generate an initial machine-learned model using a set of audio data that describes various characteristics of sound waves. Only upon receiving explicit authorization from the user, computing device 100 may capture a user's voice during a user identification process and machine learning module 160 may

apply the user's voice to the initial machine-learned model to refine the machine-learned model using various machine learning algorithms (e.g., clustering algorithms, recurrent neural network algorithms, decision-tree algorithms, regression algorithms, etc.).

In general, prior to beginning to collect data from a user, computing device 100 requests approval from a user to collect data from or about the user. Computing device 100 may request authorization before initiating a user identification process and may periodically request reauthorization. For example, computing device 100 may send a notification to the user to request authorization to record audio each time before capturing a sample of the user's voice. That is, computing device 100 is configured to only collect data from the user if the user of computing device 100 explicitly authorizes computing device 100 and audio recording application module 110 to collect data from the user. Absent the user's explicit authorization, computing device 100 will not collect data from the user.

Additionally, computing device 100 may use various methods to preserve a user's privacy. In one example, computing device 100 may associate different types of data with different security levels (e.g., high-sensitive, middle-sensitive, low-sensitive), and may take different privacy-preserving approaches based on the security level. Privacy-preserving approaches may include one or more of automatically wiping out data after a predetermined period based on the security level, continually removing data based on the security level, storing data in an encrypted format or within an encrypted portion of a memory or other data storage device, or other suitable privacy-preserving approaches.

As discussed above, computing device 100 may analyze various contextual signals, including biometric data and non-biometric data, to determine whether to automatically lock computing device 100. Computing device 100 may assign biometric data with a relatively

higher security level than non-biometric data. For example, computing device 100 may assign audio data with a relatively higher security level (e.g., middle-sensitive) than data from a keyboard or touchpad (e.g., low-sensitive) and may more frequently wipe out audio data (e.g., every minute, every hour, every day, etc.) than data from a keyboard or touchpad (e.g., every week, every month, etc.). In addition, computing device 100 may assign a captured image with a relatively higher security level (e.g., high-sensitive) than image data (e.g., middle-sensitive) and may constantly delete captured images after processing the captured images to usable image data. Furthermore, computing device 100 may sandbox data with a high-sensitive security level and may prevent applications from reaching data with a high-sensitive security level.

It is noted that the techniques of this disclosure may be combined with any other suitable technique or combination of techniques. As one example, the techniques of this disclosure may be combined with the techniques of U.S. Patent Application Publication 2014/0282877 A1. As another example, the techniques of this disclosure may be combined with the techniques of U.S. Patent Application Publication 2015/0347738 A1. Such a combination may be made for any suitable purpose, including, but not limited to, enabling a computing device to detect or couple with a companion computing device to detect various contextual signals and automatically lock the computing device based on the various contextual signals.