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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
06 December 2018 (06.12.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/222866 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *G06F 3/041* (2006.01)
G06F 3/048 (2006.01)

(21) International Application Number:
PCT/US2018/035386

(22) International Filing Date:
31 May 2018 (31.05.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/514,203 02 June 2017 (02.06.2017) US

(72) Inventors; and

(71) Applicants: **SUMMERLIN, William Christopher** [US/US]; 2000 Broadway Street, Redwood City, CA 94063 (US). **WESTERHOFF, David Michael** [US/US]; 2000 Broadway Street, Redwood City, CA 94063 (US). **CO, Timothy Chiheng** [US/US]; 2000 Broadway Street, Redwood City, CA 94063 (US).

(74) Agent: **BOWLEY, Chris C.**; Fish & Richardson P.C., P.O. Box 1022, Minneapolis, MN 55440-1022 (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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

(54) Title: TOUCH INPUT DEVICE FOR USER AUTHENTICATION AND SYSTEMS USING THE SAME

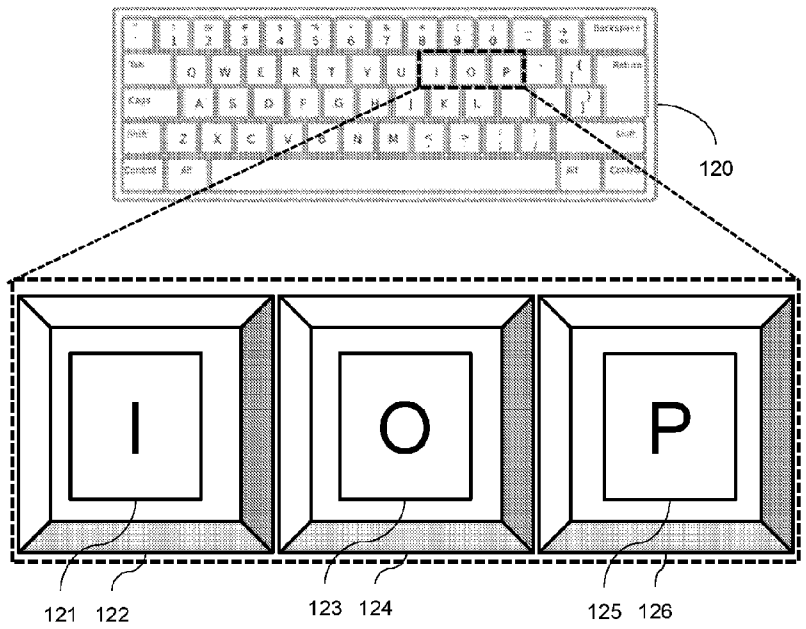

FIG. 1B

(57) Abstract: A computer system includes an input interface having a plurality of touch input elements through which a user of the computer system interacts with the computer system, the input interface including a plurality of biometric sensors and a user authentication module in communication with the plurality of biometric sensors of the input interface. During use of the input interface by a user, the input interface provides biometric data to the user authentication module for every interaction with the user interface by the touch input elements and the user authentication module continuously authenticates an identity of the user based on the biometric data.

WO 2018/222866 A1

[Continued on next page]

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).

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

TOUCH INPUT DEVICE FOR USER AUTHENTICATION AND SYSTEMS USING THE SAME

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a non-provisional of and claims priority to U.S. Provisional Patent Application No. 62/514,203, filed June 2, 2017, the entire contents of which are hereby incorporated by reference.

FIELD OF THE INVENTION

[0002] The invention relates to touch input devices for user authentication and systems using the same. In certain implementations, the invention addresses the problem of securely authenticating an end user, even when credentials may be compromised.

BACKGROUND

[0003] Traditionally, computer systems (e.g., a personal computer or a networked computer) use a knowledge-based authentication scheme at login time to authenticate the user. This approach generally assumes that the credentials (e.g., username and password) are known only to the genuine user, and that the system stores them securely (e.g., hashed). With this approach, the computer system cannot distinguish a genuine user providing the correct credentials from an intruder providing those same credentials. In addition, once a session is authenticated, an intruder can 'hijack' the session by taking control after the point of authentication.

[0004] More recently, biometric approaches to user authentication have been tried. This includes, for example, using cameras for face recognition, microphones for speaker recognition, or other biometric sensors such as a fingerprint sensor to verify the user. These systems typically have some drawbacks, however. In the case of face recognition, for example, the user may be in low light conditions or cameras are not allowed on premises. Also face recognition can fail in cases such a two similar looking individuals, such as for identical twins. Face or speaker recognition systems

also can be easily spoofed, for example by showing a photo of the genuine user or playing a recording of the end user in case of voice recognition.

[0005] Fingerprint sensors are generally unable to accurately detect when a session has been hijacked, because the user only presents their finger at the time of login via a dedicated sensor.

[0006] In the related field of keystroke dynamics, systems generally look at the typing rhythm of the user to authenticate, however the features used (e.g., flight time and dwell time) are not enough to quantifiably prove that it is the genuine user and not an imposter. That is to say that the odds of two users typing sufficiently similarly are too high to use keystroke dynamics as the sole means of reliably authenticating a user.

SUMMARY

[0007] Touch input devices for user authentication and systems using such touch input devices are disclosed. The disclosed systems employ sensor technologies in a way that provide robust ways of authenticating a user.

[0008] One example of a touch input device is a keyboard. Conventional keyboards are simply an array of contact buttons, sending signals corresponding to 'key down' or 'key up' to issue commands to the machine. While the keyboards disclosed herein have conventional form factors, they provide a ‘smart’ interface which generates an abundance of signals useful for building a powerful authentication system.

[0009] The disclosed touch input interfaces can provide the attribution necessary to securely authenticate a user based on the way that people already use a keyboard. With enough sensor data being collected from key presses, there is sufficient attribution that every user has a “globally unique” biometric signature.

[0010] The disclosed touch input devices include sensor-rich versions of otherwise conventional devices. For example, in disclosed keyboards, keys can have a conventional form factor while including one or more additional “touch sensitive” sensors. In other words, the keys behave as they conventionally would except that they collect many attributes about the touch that occurs when a key is pressed. These attributes can include, for example, force of the touch, the geometric shape of the

fingertip, the fingerprint, sub dermal vein structure, position of the touch, and the yaw and pitch angles of impact.

[0011] The necessary sensors can be coupled individually in each key, but alternatively for a non-traditional design the entire keyboard itself can be one unibody touch sensitive piece of hardware and the technology can work in a very similar fashion.

[0012] In general, in one aspect, the invention features a computer system that includes an input interface having a plurality of touch input elements through which a user of the computer system interacts with the computer system, the input interface including a plurality of biometric sensors; and a user authentication module in communication with the plurality of biometric sensors of the input interface. During use of the input interface by a user, the input interface provides biometric data to the user authentication module for every interaction with the user interface by the touch input elements and the user authentication module continuously authenticates an identity of the user based on the biometric data.

[0013] Embodiments of the computer system can include one or more of the following features and/or features of other aspects.

[0014] For example, the input interface can be a keyboard, a keypad, a mouse, or a touch panel.

[0015] Each touch input element can include at least one of the biometric sensors.

[0016] At least one of the touch input elements can include at least two different sensors of the biometric sensors.

[0017] In general, in another aspect, the invention features a method for authenticating a user of a touch input interface of a computer system, which includes: receiving biometric data from the user from every interaction of the user with the user interface; and continuously authenticating the user's identity based on the received biometric data.

[0018] Implementations of the method can include one or more features of other aspects.

[0019] In general, in a further aspect, the invention features an input interface for a computer system, including a plurality of touch input elements through which a user of the computer system interacts with the computer system, and each of the touch input elements includes a first biometric sensor and a second biometric sensor different from the first biometric sensor.

[0020] At least one of the first and second biometric sensors can be a behavioral biometric sensor, such as a keystroke sensor.

[0021] At least one of the first and second biometric sensors can be a physiological biometric sensor, such as a fingerprint sensor or a vein structure sensor.

[0022] In some embodiments, the plurality of touch input elements consists of every touch input element of the input interface.

[0023] The first and second types of sensor can be selected from the group of: a fingerprint sensor, a vein structure sensor, a touch sensor with the ability to read the touch point, the shape of the touch, a touch force, or a rotation angle of a finger touching the sensor.

[0024] The first and second types of sensor can be selected from the group of an optical sensor, a capacitive sensor, an ultrasonic sensor, and an accelerometer.

[0025] Each touch input element can include at least one additional sensor in addition to the first and second sensors.

[0026] With respect to the touch surface of the touch input element, the first and second sensors can be side-by-side or stacked.

[0027] The touch input elements can be keys (e.g., physical keys or each key can correspond to a different location on a touchscreen.

[0028] The touch input elements can include at least one button.

[0029] The input interface can be a keyboard, a keypad, a touch panel, or a mouse.

[0030] In general, in a further aspect, the invention features a keyboard or keypad, including a plurality of keys each having at least one biometric sensor, wherein the keyboard is configured to provide biometric data for every possible key stroke during use of the keyboard. Embodiments of the keyboard or keypad can include one or more features of other aspects.

[0031] In general, in another aspect, the invention features a keyboard or keypad, including a key having at least two different types of biometric sensors. Embodiments of the keyboard or keypad can include one or more features of other aspects.

[0032] In general, in a further aspect, the invention features a method of authenticating an identity of a user of a keyboard or keypad, including sensing biometric information of the user with every keystroke by the user of the keyboard or keypad and authenticating the identity of the user based on the biometric information.

[0033] Among other advantages, implementations of the technology may be used to attribute a user entering credentials to a particular person to prevent fraudulent authentication. Secure touch input devices are able to protect sensitive information stored on a computer system in cases where a user's credentials have been compromised, because the system does not look at just what is typed (e.g., a password) it looks at the unique way that the input is typed. This makes system's using such touch input devices robust to intrusion. In other words, system's using the disclosed touch input devices can address the question "is this truly the genuine user inputting the password to the system?" instead of "is this password correct?"

[0034] The technology may be used to continuously authenticate a user during a session and generate an audit trail for forensic analysis. For example, because keyboards are used continuously throughout a session the proposed secure keyboard is an ideal candidate for continuous authentication. The system has the ability to detect if a session has been hijacked and after detecting the genuine user is no longer the one controlling the system, it is able to react accordingly and lock out the intruder.

[0035] Systems using secure touch input devices can perform 1:1 verification or l:N identification, where N is a number (e.g., a large number) of known people. For example, in a shared computing environment like a university library, a secure keyboard can make several user-authentication claims with accuracy, even without an account login. For example, based on use of the keyboard, a system can determine: (i) whether the user is a student or staff member of the institution; (ii) whether the user has the permission to use the machine; and (iii) which user (i.e., out of N possible users affiliated with the institution) exactly is this.

[0036] Other possible benefits include, for a computer or server, systems can provide a comprehensive audit trail that can forensically prove who was using the system at specific times. This is notably different from conventional situations where the system simply tracks which user's credentials were used to issue a certain command.

[0037] Alternatively, or additionally, secure touch input devices can be used to do other security tasks as well, such as cryptographically 'signing' or 'encrypting' data that only a specified person(s) can decrypt or verify. Traditionally, encryption suffers the same problem as authentication, once the secret is compromised the security integrity is immediately lost.

[0038] The details of one or more implementations of the subject matter of this disclosure are set forth in the accompanying drawings and the description below. Other features, aspects, and advantages of the subject matter will become apparent from the description, the drawings, and the claims.

DESCRIPTION OF DRAWINGS

[0039] FIGS. 1A-B are schematic diagrams of an embodiment of a computer system that includes a secure keyboard, wherein FIG. 1B is an enlarged view of a portion of the keyboard of FIG. 1A.

[0040] FIGS. 2A-C are a schematic diagrams of embodiments of a key of a secure keyboard, wherein FIG. 2A shows side-by-side configuration of sensors, FIG. 2B shows one sensor stacked on top of a second sensor, and FIG. 2C shows a mosaic-like configuration of sensors.

[0041] FIG. 3 is a diagram of an embodiment of a mouse with sensors.

[0042] FIG. 4 is a diagram of an embodiment of a numeric keypad with sensors.

[0043] FIG. 5 is a diagram of an embodiment of a trackpad with sensors.

[0044] FIG. 6 is a diagram of an embodiment of a laptop with a secure keyboard.

[0045] FIG. 7 is a diagram of an embodiment of a tablet computer with integrated biometric sensors.

[0046] FIG. 8 is a schematic diagram of another embodiment of a system for securely and continuously authenticating with a networked server.

[0047] FIG. 9 is a schematic diagram of a further embodiment of a system for peer-to-peer authentication using secure keyboards.

[0048] FIG. 10 is a schematic diagram of an example computer system.

[0049] Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0050] Referring to FIGS. 1A and 1B, a computer system 100 includes a computer terminal 110 and a secure keyboard 120 connected to terminal 110. Computer terminal 110 includes an authentication module 130. Keyboard 120 is a QWERTY-type keyboard and includes keys 121, 123, and 125. Each key of keyboard 120 contains a sensor. Keys 121, 123, and 125, for example, contain sensors 122, 124, and 126, respectively.

[0051] In a typical computing session, a user makes frequent use of a keyboard to type or issue various commands. A conventional keyboard detects the key-press events, processes the events in a processor, and transmits the data to the computer terminal that typically acts upon all received keyboard events. Ordinarily, the data provided by the keyboard is simply a sequence of keystroke events. However, a conventional keyboard may also provide additional information, such as key dwell time, relative timing of key strokes, and key error rate (e.g., as indicated by use of backspaces or acceptance of auto-correct). Such information are examples of behavioral biometric data, which refers to data characterizing how a specific user interacts with an interface such as a keyboard. Behavioral data alone, however, is typically insufficient for unambiguous attribution.

[0052] Secure keyboard 120 augments conventional keyboards with sensors (e.g., sensors 122, 124, and 126) that produce additional biometric data that can include either or both behavioral biometric data and physiological biometric data upon contact with user's fingers. Examples of behavioral biometric data that the sensors can provide include touch force and contact footprint (e.g., ellipse shape and orientation),

in addition to the behavioral biometric data discussed previously. Physiological biometric data refers to physical characteristics of a person's body. Examples of physiological biometric data include fingerprints, palm or finger vein structures, skin moisture level, skin temperature, heartrate, and blood oxygenation level.

[0053] In general, sensors 122,124, and 126 can be one of a variety of different types of sensors. For example, each sensor can be a fingerprint sensor, a vein structure sensor, a contact force sensor, an accelerometer, a multi-axis accelerometer, a moisture sensor, a temperature sensor, a pulse sensor, an oximeter, or a skin conductance sensor. Some of these sensors are commercially available in form factors conducive for integration into a key, and use of such off-the-shelf components is beneficial for cost reasons.

[0054] Fingerprint sensors typically operate by imaging the ridges that are present on a human finger, and fingerprints have been proven effective as a uniquely identifying feature of a person. Fingerprint sensors can image these ridges in a number of ways, including optical, ultrasonic, or capacitive method. An optical fingerprint sensor uses an optical image sensor in a manner similar to a digital camera to capture a visual image of a fingerprint. The resulting image is typically confined to the surface details of a finger as a finger has limited transmissivity to light. An ultrasonic sensor transduces ultrasonic waves and detects the reflected ultrasonic waves to reconstruct an image of the fingerprint. An ultrasonic sensor is less prone to superficial dirt or scars on a finger making it more robust, and it may also capture details beneath the skin surface for additional biometric details. A capacitive sensor images the finger surface by mapping out the distances between the sensor surface and the ridges by electrical means to capture a fingerprint image. These different implementations of fingerprint sensors have similar form factors, which typically consists of a top plate that comes in contact with the user's finger, and sensor electronics that sits beneath the top plate. Fingerprint sensors typically require direct contact with the user's finger for proper operation.

[0055] Vein structure sensors typically operate by illuminating subcutaneous veins through the skin with an infrared (IR) light source and capturing a transmitted or reflected IR image. Hemoglobin in blood absorbs infrared light and this property

gives contrast to the veins with respect to their surroundings. A transmission-mode imaging can be implemented with an IR imaging sensor and associated optics, relying on ambient lighting to provide the requisite IR illumination. Reflective imaging does not require ambient IR illumination as an IR light source can be co-integrated with the imaging sensor to provide the requisite illumination. Similar to a fingerprint sensor, a vein structure sensor typically consists of a top plate that comes in contact with the user's finger, and sensor electronics that sits beneath the top plate. Vein structure sensors typically require direct contact with the user's finger for proper operation.

[0056] Contact force sensors typically operate by using a force-sensing resistor. In response to an applied force, the resistor changes its resistance, a property that can be readily measured with compact electronic circuits. The resistors are typically thin, flexible, and adaptable in shape, allowing for easy integration.

[0057] Accelerometers measure acceleration or a change in velocity per unit time. Modern accelerometers are typically implemented as a micro electro-mechanical system (MEMS), and are robust, inexpensive, and compact. Accelerometers can be single-axis or multi-axis. A single-axis accelerometer, for example, is capable of characterizing the way a key is pressed along the key's vertical axis. In contrast, a 3-axis accelerometer may be used to characterize a movement of a key in all three axes. Accelerometers do not require direct contact with the user's finger, and can therefore be integrated anywhere within a key.

[0058] The presence of the sensors makes the keys 'touch-sensitive' - they behave normally during interaction with the user, but collect attributes about the touch that are, individually and/or collectively, unique to the user that occurs when a key is pressed. Such collected attributes can include one or more of the following: force of the touch; three dimensional direction of the keystroke; dwell time; relative timing between key strokes; geometric shape of the fingertip (major and minor radii); rotation of the ellipse while pressing a key; fingerprint; subdermal vein structure; position of the touch; and the yaw and pitch angles of impact. Attributes may also include pulse rate, amount of perspiration, skin temperature, and blood oxygenation level.

[0059] While sensors for three keys are shown in the drawing, it is to be understood that all keys of keyboard 120 have the same sensors. Having all keys

equipped with sensors enables generation of biometric data from every keystroke. Moreover, because the sensors are embedded in the keys, the system obtains biometric data without any superfluous interaction with the system beyond what the user would do using a conventional interface (e.g., the system does not require interaction with a dedicated sensor separate from the keys).

[0060] During operation, keyboard 120 sends signals containing both key-sequence information and biometric data to computer terminal 110, where authentication module 130 processes the data to authenticate the user. Accordingly, computer system 100 can continuously authenticate the identity of a user as the user interacts with the computer system.

[0061] In particular, system 100 collects a combination of attributes from each key press, which authentication module 130 uses to construct a unique biometric signature for every user. This constructed biometric signature is then used by the module to authenticate the user.

[0062] In some embodiments, a baseline biometric signature is established for use as a basis for future authentication decisions by the module. The process of establishing a baseline biometric signature can include collecting sufficient keystrokes and associated biometric data from a wide variety of keys during a controlled user-profile generation process. This collected data is then used to construct a biometric signature. The analysis may include among others the following: indexing fingerprints from all ten fingers; determining which fingers are used for each keys; determining the time elapsed in transition between key-pairs; constructing a dataset for each types of collected biometric data; and determining whether the constructed dataset is statistically significant. If the constructed dataset from the analysis is determined to be not statistically significant, further collection of keystrokes may be prompted and the process above repeated.

[0063] Authentication module 130 uses stored baseline biometric signatures to make authentication decisions. The authentication module receives biometric data from keystrokes, and constructs a 'local' biometric signature from a limited sequence of one or more keystrokes. This local biometric signature is then scored with respect to the baseline or 'global' biometric signature associated with a user profile. The

resulting score is typically a measure of confidence that the local biometric signature is in agreement with the user's baseline biometric signature. The authentication module compares this score to a threshold and makes an authentication decision.

[0064] In general, scoring can be performed using a variety of technologies suitable for the specific biometric data to be scored. For example, various machine learning technologies can be applied to score either the key dwell time data and/or key error rate. These can include artificial neural network algorithms (e.g., perceptron, back-propagation, hopfield network, radial basis function network), regression algorithms (e.g., ordinary least squares regression, linear regression, stepwise regression, logistic regression, locally estimated scatterplot smoothing, and multivariate adaptive regression splines), instance-based algorithms (e.g., k-nearest neighbor, learning vector quantization, self-organizing map, locally weighted learning), decision tree algorithms (e.g., classification and regression tree, conditional decision trees, decision stump), Bayesian algorithms (e.g., Naive Bayes, Gaussian Naive Bayes, Multinomial Naive Bayes, Averaged One-dependence estimators, Bayesian Belief Network, Bayesian Network), clustering algorithms (e.g., k-means, k-medians, expectation maximization, hierarchical clustering), deep learning models (e.g., deep boltzmann machine, deep belief networks, convolutional neural network, stacked auto-encoders), and ensemble algorithms (e.g., random forest, boosting, bootstrapped aggregation, adaboost, stacked generalization, gradient boosting machines, gradient boosted regression trees). In some implementations, scoring can be performed using a one-class Support Vector Machine, Elliptic Envelope, a replicator neural network (e.g., for anomaly detection), and/or an ensemble technique.

[0065] Scoring methods may also include proprietary, commercially-available, or freely available software. Some examples are softwares from BehavioSec (https://www.behaviosec.com), KeyTrac (https://www.keytrac.net), and/or WatchfulSoftware (https://www.watchfulsoftware.com/en/solutions/keystroke-dynamics).

[0066] This addition of biometric signature enables protection against improper access even in cases where a user's credential has been compromised. The system does not only evaluate what is typed (e.g., a password), but also the unique way that

the input is typed (e.g., biometric signature). This combination of password and biometric signature forms a multifactor authentication system in which the additional authentication factor is extremely difficult, if not impossible, to duplicate, making the system extremely robust against intrusion. In effect, the invention solves one of the hardest problems in security, which is 'is this truly the genuine user inputting the correct password to the system?'

[0067] In addition, system 100 is capable of continuously authenticating a user during the actual use of the system through user's use of the keyboard, an ideal candidate for continuous authentication interface as keyboard is continuously used in most sessions. Therefore, the system has the ability to detect whether a session has been hijacked and is no longer controlled by the authorized user, and take appropriate measures including locking out the intruder.

[0068] Furthermore, system 100 can also perform 1: n identification where n is the number of known people. This 1: n identification is useful in many scenarios, including password-less authentication. Because the biometric signature obtained from the secure keyboard 120 is globally unique due to use of multiple biometric data obtained from a plurality of sensors, a system can authenticate a user without individual passwords by simply collecting the user's biometric signature, which can be done, as an example, by prompting the user to type in the displayed text. Another use of the 1: n identification is in recording a comprehensive audit trail that can forensically prove which human was behind the machine during any particular interaction during a session, which is far more valuable than knowing which person's credentials were used in issuing the command.

[0069] Another use of the biometric signature available to system 100 is in cryptographically signing a data to prove authenticity of the source, or encrypting data so that only the specified person(s) can decrypt of verify. One thing to note is that in cryptographic scenarios, security is lost immediately when the private 'key' is compromised. Therefore, use of a biometric signature is superior to a traditional 'key', as biometric signature is inherent to a user and therefore less likely to be compromised.

[0070] While the foregoing keyboard includes a single sensor in each key, other implementations are also possible. More than one sensor can be built into one or more of the keys, for example. Quality of attribution based on a biometric signature generally improves with the number of different types of collected biometric data. Therefore, it is advantageous to integrate more than one type of sensor into the keys, with the goal of having each type of sensor generate corresponding biometric data from each key stroke.

[0071] Generally, multiple sensors can be integrated into a single key in a variety of ways. For example, referring to Fig. 2A, in one integration approach, a key 200 includes two sensors 201 and 202 which are arranged side-by-side on the top surface of the key. Such arrangements can include sensors that are arranged top and bottom (with respect to the keyboard), or a left and right as shown. As the two sensors maintain their respective top contact surfaces and do not obstruct one another in any way, commercial sensors can be used off-the-shelf without any customizations. In some embodiments, the two sensors are a fingerprint sensor and a contact force sensor. In other embodiments, the two sensors can be a fingerprint sensor and a vein structure sensor. Generally, the two sensors can be any combination of available biometric sensors that are sufficiently compact to be combined inside a single key.

[0072] FIG. 2B shows another way of integrating sensors. In particular, a key 210 includes sensors 211 and 212 which are stacked on top of one another. Generally, sensor stacking is possible where at least one of the sensors is not required to contact the user's finger to obtain biometric data. In some embodiments, sensor 211 that is in contact with the finger can be a fingerprint sensor or a vein structure, and sensor 212 can be a multi-axis accelerometer. Such a combination of may enable capturing of a fingerprint or a vein structure image while recording the speed and direction of the keystroke. While stacking of two sensors is shown, it is to be understood that more than two sensors can be stacked.

[0073] Other integration architectures are also possible. For example, FIG. 2C shows a key 220 that includes a sensor mosaic 221 on its top surface. The mosaic is composed of a two-dimensional array of two different types of sensor interleaved with each other. This configuration ensures that both type of sensor collects information in

instances where the user's finger only contacts a portion of the key surface. In certain embodiments, the interleaved sensors are a vein structure sensor and a fingerprint sensor. This approach can also be extended to more than two sensors, by interleaving additional sensor pixels.

[0074] So far, sensors have been integrated on keys of a keyboard to enable generation of biometric data. Other touch input device form-factors, however, are also possible. For example, referring to FIG. 3, in some embodiments, a mouse 300 includes one or more touch sensors. In some embodiments, mouse buttons 311 and 312 each contain a fingerprint sensor. In other embodiments, scroll wheel 314 contains a fingerprint sensor. Additional sensors can be integrated into buttons 311 and 312 using side-by-side, stacked, or mosaic configurations. In other embodiments, sensors are further integrated on body 320 to collect biometric data from palm that are unique from fingertip data. Such data include palm prints, principal lines, wrinkles, epidermal ridges, indents, marks, and palm vein structures, which may be captured using a palm print sensor, an array of fingerprint sensors, or a vein structure sensor.

[0075] In addition to physiological biometric data, a mouse may capture unique behavioral biometric data such as lateral acceleration and scrolling characteristics. Therefore, combined use of keyboard 120 with mouse 300 may provide a broader range of biometric data than is possible with either one alone.

[0076] Another implementation is a numeric keypad 400 shown in FIG. 4. Key 410 of this keypad is analogous to the sensor-integrated keys of keyboard 120. Much like secure keyboard 120, this keypad can provide a continuous stream of biometric data. However, the reduced number of keys of a numeric keypad may make it more economic for specific applications such as use for a telephone keypad or a point-of-sale machine where a majority of the key interactions are limited to the numeric keys.

[0077] Referring to FIG 5, another implementation is a trackpad 500 with integrated sensors. In addition to buttons 511 and 512 that may contain sensors, touchpad 520 presents an alternative input interface to a user that can be integrated with sensors. Trackpad captures touch gestures such as a tap, swipe, drag, or a pinch and generates both behavioral and physiological data. The generated behavioral data is

expected to be significantly different from that of a keyboard or a mouse, providing further biometric data diversity for improved authentication.

[0078] In system 100, computer terminal 110 and secure keyboard 120 are two separate objects. More generally, other implementations are also possible. For example, referring to FIG. 6, the two can be combined into an integrated computer system in the form of laptop 600 that integrates both a terminal, a keyboard 610, and a trackpad 620 into a single object. Portability of laptops and their uses in public areas make laptops particularly vulnerable to theft and passwords being compromised by onlookers. Secure authentication using biometric signature combined with continuous authentication greatly improves security of laptops, as stolen laptops cannot be authenticated with a password alone. Even in the event that a laptop is stolen during an authenticated session, the system is protected by measures such as automatic lockout enabled by continuous authentication.

[0079] Referring to FIG. 7, secure tablet computer system 700 can be implemented by integrating the sensors as a part of, or under touch panel 710 to capture a unique set of biometric data for continuous authentication. Such data include taps, swipes, drags, pinches and other various gestures of a trackpad, but also include keyboard-like interaction with an on-screen virtual keyboard for added biometric data diversity. Portability of tablet computers and their use in public areas make tablet computers particularly vulnerable to theft and passwords being compromised by onlookers. Secure authentication using biometric signature combined with continuous authentication greatly improves security of tablet computers, as stolen tablet computers cannot be authenticated with a password alone. Even in the event that a tablet computer is stolen with a pre-authenticated session, the system is protected by automatic lockout enabled by continuous authentication.

[0080] Referring to FIG. 8, secure keyboard 120 can also be used in client-server system 800, where network access point 810 provides access to the authentication server 840 through network 830. This way, server 840 can be accessed remotely and still benefit from continuous authentication and audit trail generation provided by the secure keyboard system, as if the user is physically present at the remote computer system with the secure keyboard. In other embodiments,

authentication server 840 is a third party server performing biometric authentication tasks on behalf of other servers. In such embodiments, the authentication server may simply pass along determinations of attribution with the associated keystrokes for downstream processing.

[0081] FIG. 9 shows a peer-to-peer setup, where secure keyboards 901 on respective peer devices 910 and 920 can be used for proving identity of oneself to a peer. Traditionally, it is very difficult to ascertain the identity of a remote user due to limitations of traditional authentication methods that have been previously discussed. This problem can be solved by extending the concept of continuous authentication through biometric signature verification to peer to peer network connections.

[0082] Special considerations may be necessary to maintain integrity of the system as whole, which include establishing hardware root of trust, encrypted transport, and secure enclave. Hardware root of trust may be required so that all machines involved in an authentication event can be trusted by one another to prevent a malicious node from obtaining attribution data that can be used as a basis for a spoofing attack. Such issues have been addressed by the industry in the form of a Trusted Platform Module (TPM), which is a physical chip that securely stores a unique key that can be used by an installed piece of hardware to authenticate itself and the system to check for the integrity of its hardware configuration to verify that the system has not been tampered with. For example, TPM can be used by the system to ascertain the identity of a connected keyboard, and the system can then determine whether the connected device is on a list of pre-approved or 'paired' devices. Once the system verifies that the keyboard is an authentic secure keyboard and that the keyboard has been approved for use on that particular system, it accepts the keyboard for use. Such measure protects the system against, for instance, swapping out of a secure keyboard with a tampered device that can be used for a basis for malicious actions such as phishing, eavesdropping, and spoofing.

[0083] Encrypted transport by establishing a secure channel may be necessary to maintain security of the biometric signature. A non-secure channel is open to sniffing of the data during transport from the keyboard to the terminal and terminal to a peer, which compromises the secrecy of the biometric signature. Such compromised

biometric signatures can be used in a man-in-the-middle attack to relay false biometric signature to compromise the security of the entire system. Furthermore, each node may need to establish trustworthiness before establishing an encrypted channel to ensure that no node is spoofed.

[0084] Secure enclave may also be necessary to maintain security of the biometric signature. The attribution data (i.e. biometric signature) should be secure at rest and unrecoverable so that the system only answers the question of whether someone is authorized or not without actually disclosing the underlying biometric template used for authentication under any circumstances. To enhance the security of the attribution data, it should be stored away from the main memory in a TPM or a secure enclave to protect against malicious code or bad actors from obtaining the data through run-time vulnerabilities.

[0085] FIG. 10 is a schematic diagram of an example computer system 1000. The system 1000 can be used to carry out the operations described in association the implementations described previously. In some implementations, computing systems and devices and the functional operations described above can be implemented in digital electronic circuitry, in tangibly-embodied computer software or firmware, in computer hardware, including the structures disclosed in this specification (e.g., system 1000) and their structural equivalents, or in combinations of one or more of them. The system 1000 is intended to include various forms of digital computers, such as laptops, desktops, workstations, personal digital assistants, servers, blade servers, mainframes, and other appropriate computers, including vehicles installed on base units or pod units of modular vehicles. The system 1000 can also include mobile devices, such as personal digital assistants, cellular telephones, smartphones, and other similar computing devices. Additionally, the system can include portable storage media, such as, Universal Serial Bus (USB) flash drives. For example, the USB flash drives may store operating systems and other applications. The USB flash drives can include input/output components, such as a wireless transmitter or USB connector that may be inserted into a USB port of another computing device.

[0086] The system 1000 includes a processor 1010, a memory 1020, a storage device 1030, and an input/output device 1040. Each of the components 1010, 1020,

1030, and 1040 are interconnected using a system bus 1050. The processor 1010 is capable of processing instructions for execution within the system 1000. The processor may be designed using any of a number of architectures. For example, the processor 1010 may be a CISC (Complex Instruction Set Computers) processor, a RISC (Reduced Instruction Set Computer) processor, or a MISC (Minimal Instruction Set Computer) processor.

[0087] In one implementation, the processor 1010 is a single-threaded processor. In another implementation, the processor 1010 is a multi-threaded processor. The processor 1010 is capable of processing instructions stored in the memory 1020 or on the storage device 1030 to display graphical information for a user interface on the input/output device 1040.

[0088] The memory 1020 stores information within the system 1000. In one implementation, the memory 1020 is a computer-readable medium. In one implementation, the memory 1020 is a volatile memory unit. In another implementation, the memory 1020 is a non-volatile memory unit.

[0089] The storage device 1030 is capable of providing mass storage for the system 1000. In one implementation, the storage device 1030 is a computer-readable medium. In various different implementations, the storage device 1030 may be a floppy disk device, a hard disk device, an optical disk device, or a tape device.

[0090] The input/output device 1040 provides input/output operations for the system 1000. In one implementation, the input/output device 1040 includes a keyboard and/or pointing device. In another implementation, the input/output device 1040 includes a display unit for displaying graphical user interfaces.

[0091] The features described can be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. The apparatus can be implemented in a computer program product tangibly embodied in an information carrier, e.g., in a machine-readable storage device for execution by a programmable processor; and method steps can be performed by a programmable processor executing a program of instructions to perform functions of the described implementations by operating on input data and generating output. The described features can be implemented advantageously in one or more computer programs that

are executable on a programmable system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data storage system, at least one input device, and at least one output device. A computer program is a set of instructions that can be used, directly or indirectly, in a computer to perform a certain activity or bring about a certain result. A computer program can be written in any form of programming language, including compiled or interpreted languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment.

[0092] Suitable processors for the execution of a program of instructions include, by way of example, both general and special purpose microprocessors, and the sole processor or one of multiple processors of any kind of computer. Generally, a processor will receive instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for executing instructions and one or more memories for storing instructions and data. Generally, a computer will also include, or be operatively coupled to communicate with, one or more mass storage devices for storing data files; such devices include magnetic disks, such as internal hard disks and removable disks; magneto-optical disks; and optical disks. Storage devices suitable for tangibly embodying computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The processor and the memory can be supplemented by, or incorporated in, ASICs (application-specific integrated circuits).

[0093] To provide for interaction with a user, the features can be implemented on a computer having a display device such as a CRT (cathode ray tube) or LCD (liquid crystal display) monitor for displaying information to the user and a keyboard and a pointing device such as a mouse or a trackball by which the user can provide input to the computer. Additionally, such activities can be implemented via touchscreen flat-panel displays and other appropriate mechanisms.

[0094] The features can be implemented in a computer system that includes a back-end component, such as a data server, or that includes a middleware component, such as an application server or an Internet server, or that includes a front-end component, such as a client computer having a graphical user interface or an Internet browser, or any combination of them. The components of the system can be connected by any form or medium of digital data communication such as a communication network. Examples of communication networks include a local area network ("LAN"), a wide area network ("WAN"), peer-to-peer networks (having ad-hoc or static members), grid computing infrastructures, and the Internet.

[0095] The computer system can include clients and servers. A client and server are generally remote from each other and typically interact through a network, such as the described one. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0096] While this specification contains many specific implementation details, these should not be construed as limitations on the scope of any inventions or of what may be claimed, but rather as descriptions of features specific to particular implementations of particular inventions. Certain features that are described in this specification in the context of separate implementations can also be implemented in combination in a single implementation. Conversely, various features that are described in the context of a single implementation can also be implemented in multiple implementations separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a subcombination or variation of a subcombination.

[0097] Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Moreover, the separation of various system

components in the implementations described above should not be understood as requiring such separation in all implementations, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

[0098] Thus, particular implementations of the subject matter have been described. Other implementations are within the scope of the following claims. In some cases, the actions recited in the claims can be performed in a different order and still achieve desirable results. In addition, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In certain implementations, multitasking and parallel processing may be advantageous.

[0099] Other embodiments are in the following claims.

What is claimed is:

1. A computer system, comprising:

an input interface comprising a plurality of touch input elements through which a user of the computer system interacts with the computer system, the input interface comprising a plurality of biometric sensors; and

a user authentication module in communication with the plurality of biometric sensors of the input interface,

wherein during use of the input interface by a user, the input interface provides biometric data to the user authentication module for every interaction with the user interface by the touch input elements and the user authentication module continuously authenticates an identity of the user based on the biometric data.

2. The computer system of claim 1, wherein the input interface is a keyboard, a keypad, a mouse, or a touch panel.

3. The computer system of claim 1, wherein each touch input element comprises at least one of the biometric sensors.

4. The computer system of claim 1, wherein at least one of the touch input elements comprise at least two different sensors of the biometric sensors.

5. A method for authenticating a user of a touch input interface of a computer system, the method comprising:

receiving biometric data from the user from every interaction of the user with the user interface; and

continuously authenticating the user's identity based on the received biometric data.

6. An input interface for a computer system, comprising:

a plurality of touch input elements through which a user of the computer system interacts with the computer system; and

each of the touch input elements comprising a first biometric sensor and a second biometric sensor different from the first biometric sensor.

7. The input interface of claim 6, wherein at least one of the first and second biometric sensors is a behavioral biometric sensor.

8. The input interface of claim 7, wherein the behavioral biometric sensor is a keystroke sensor.

9. The input interface of claim 6, wherein at least one of the first and second biometric sensors is a physiological biometric sensor.

10. The input interface of claim 9, wherein the physiological biometric sensor is a fingerprint sensor.

11. The input interface of claim 9, wherein the physiological biometric sensor is a vein structure sensor.

12. The input interface of claim 6, wherein the plurality of touch input elements consists of every touch input element of the input interface.

13. The input interface of claim 6, wherein the first and second types of sensor are selected from the group consisting of: a fingerprint sensor, a vein structure sensor, a touch sensor with the ability to read the touch point, the shape of the touch, a touch force, or a rotation angle of a finger touching the sensor.

14. The input interface of claim 6, wherein the first and second types of sensor are selected from the group consisting of an optical sensor, a capacitive sensor, an ultrasonic sensor, and an accelerometer.

15. The input interface of claim 6, wherein each touch input element comprises at least one additional sensor in addition to the first and second sensors.

16. The input interface of claim 6, wherein, with respect to the touch surface of the touch input element, the first and second sensors are side-by-side.

17. The input interface of claim 6, wherein, with respect to the touch surface of the touch input element, the first and second sensors are stacked.

18. The input interface of claim 6, wherein the touch input elements are keys.

19. The input interface of claim 18, wherein the keys are physical keys.

20. The input interface of claim 18, wherein each key corresponds to a different location on a touchscreen.

21. The input interface of claim 6, wherein the touch input elements comprise at least one button.

22. The input interface of claim 1, wherein the input interface is a keyboard.

23. The input interface of claim 1, wherein the input interface is a keypad.

24. The input interface of claim 1, wherein the input interface is a touch panel.

25. The input interface of claim 1, wherein the input interface is a mouse.

26. A keyboard or keypad, comprising:

a plurality of keys each comprising at least one biometric sensor,

wherein the keyboard is configured to provide biometric data for every possible key stroke during use of the keyboard.

27. A keyboard or keypad, comprising:

a key comprising at least two different types of biometric sensors.

28. A method of authenticating an identity of a user of a keyboard or keypad, comprising:

sensing biometric information of the user with every keystroke by the user of the keyboard or keypad; and

authenticating the identity of the user based on the biometric information.

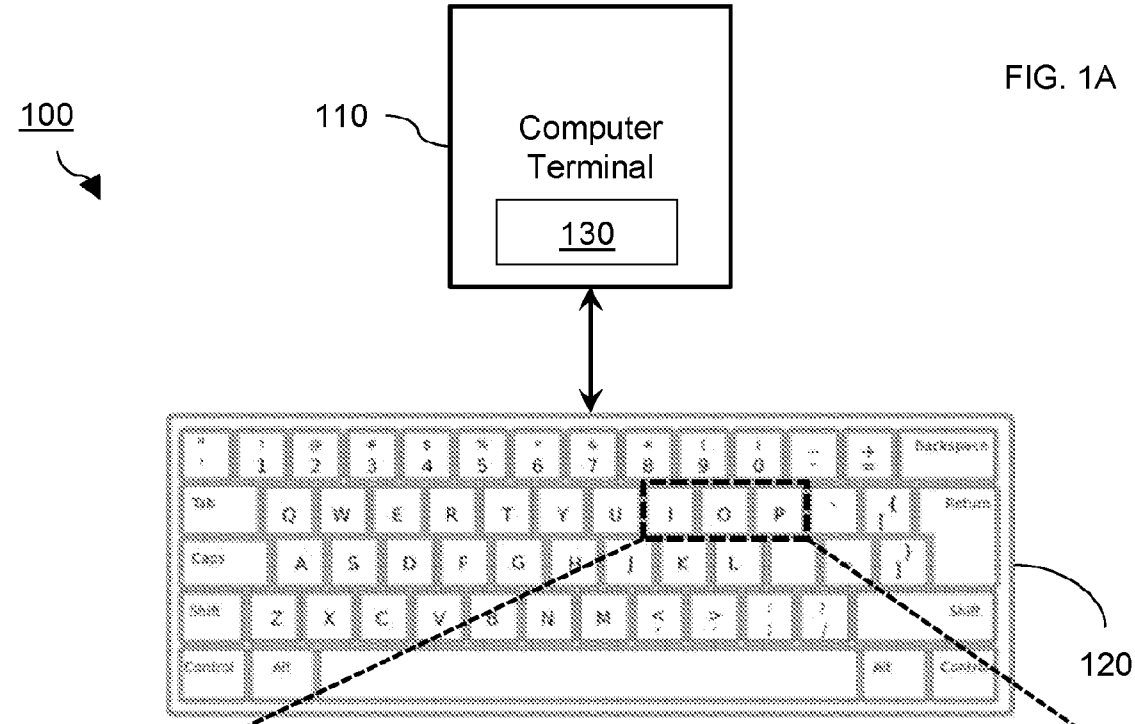

FIG. 1A

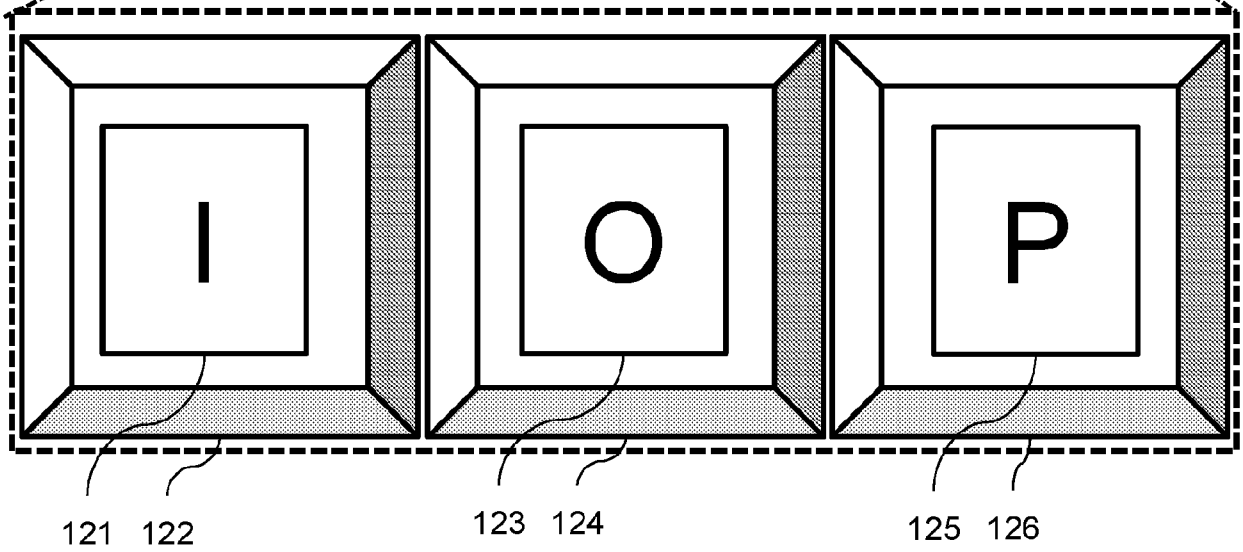

FIG. 1B

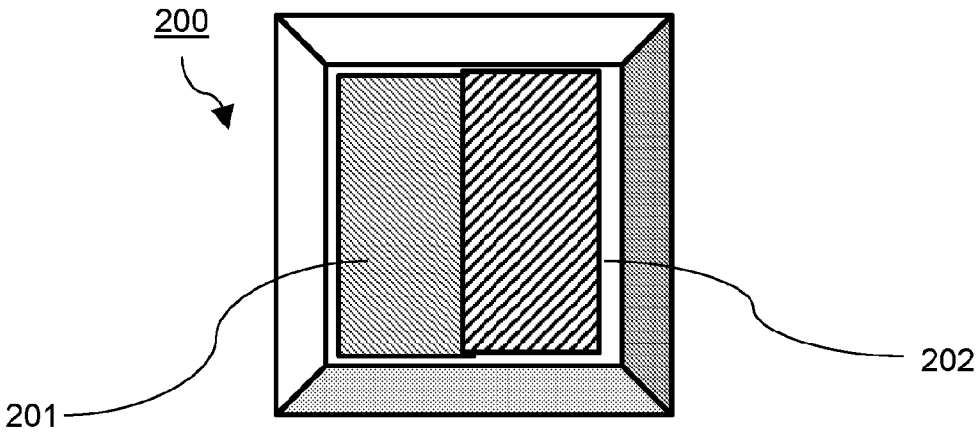

FIG. 2A

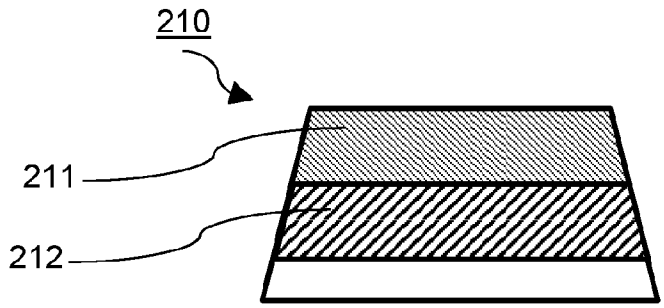

FIG. 2B

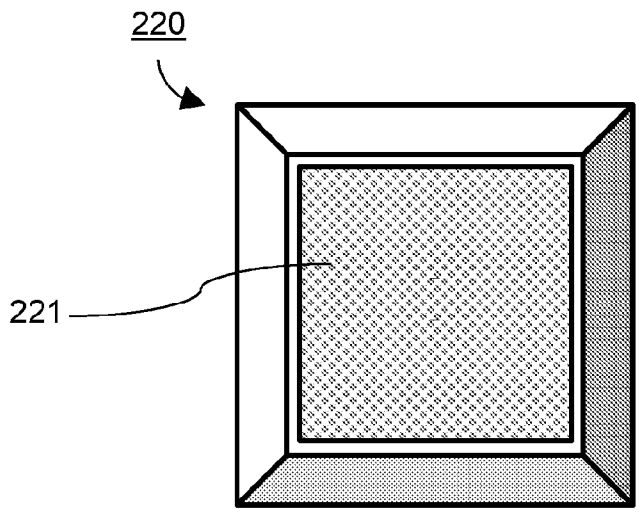

FIG. 2C

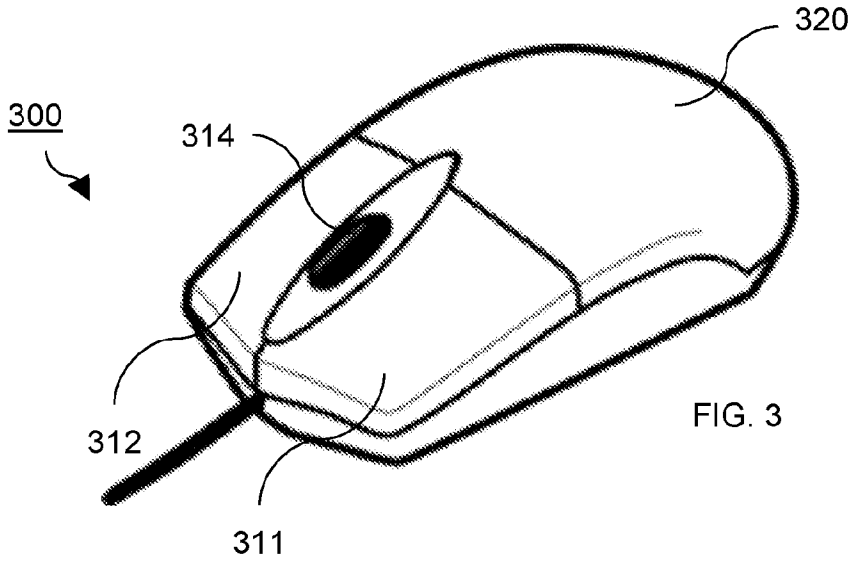
320
300
314
312
311

FIG. 3

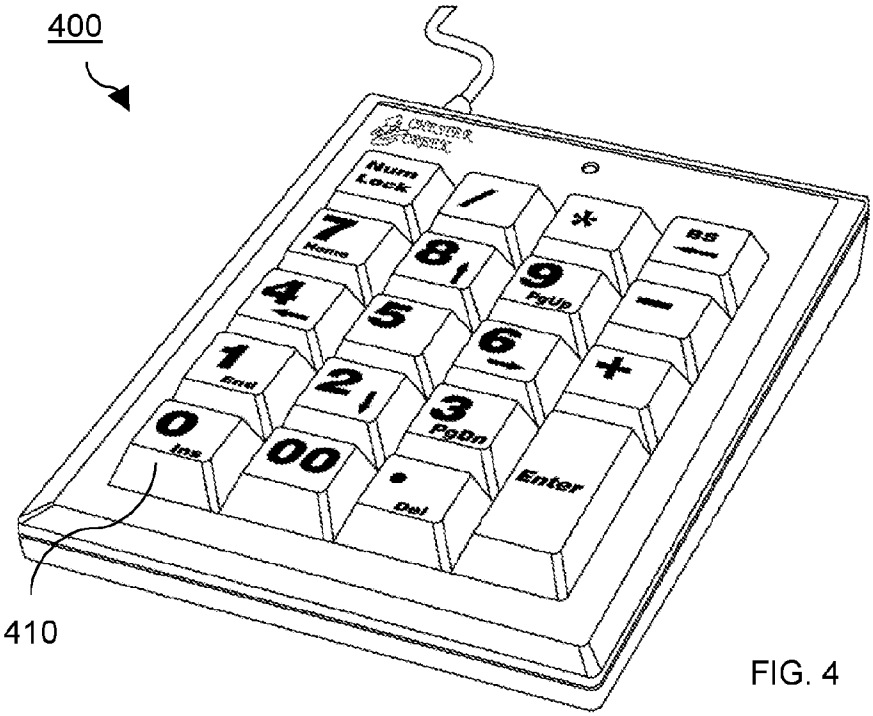
400
Num Lock
/
*
7 Home
8
9 PgUp
4
5
6
1 End
2
3 PgDn
0 Ins
00
Del
Enter
410

FIG. 4

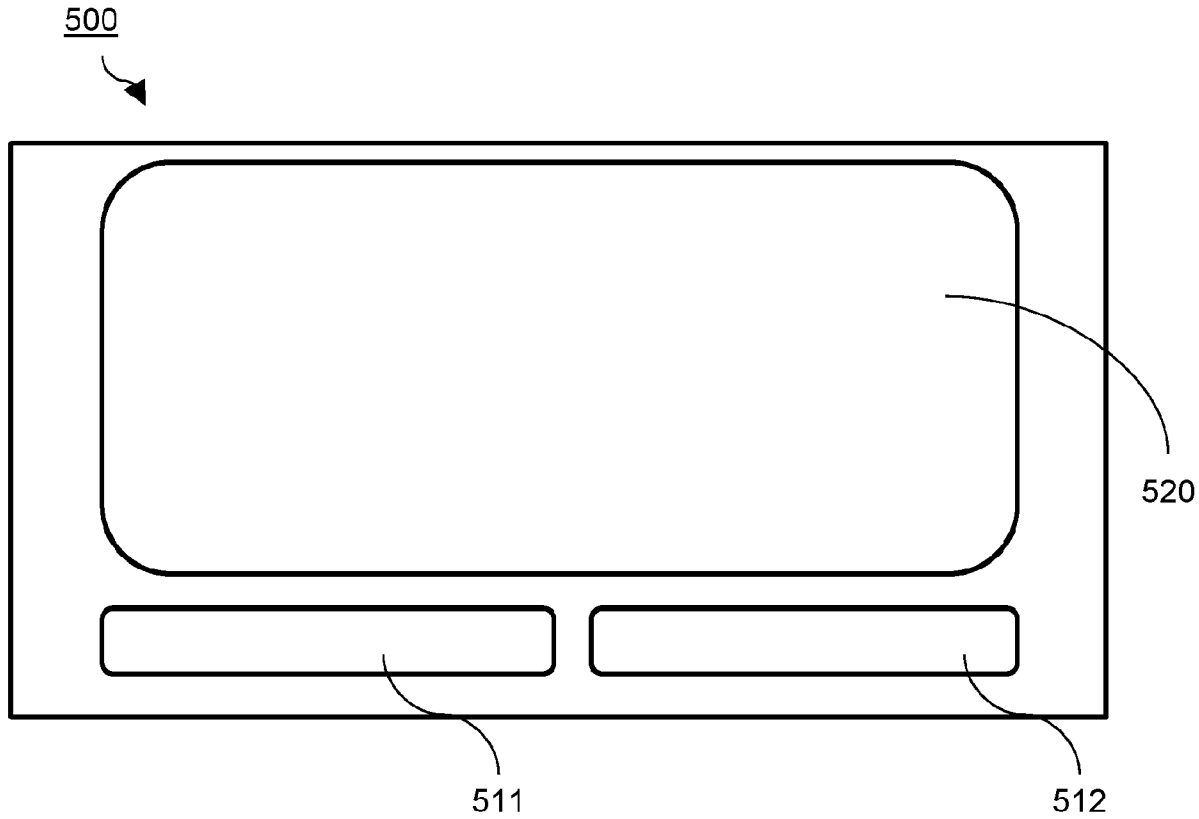

FIG. 5

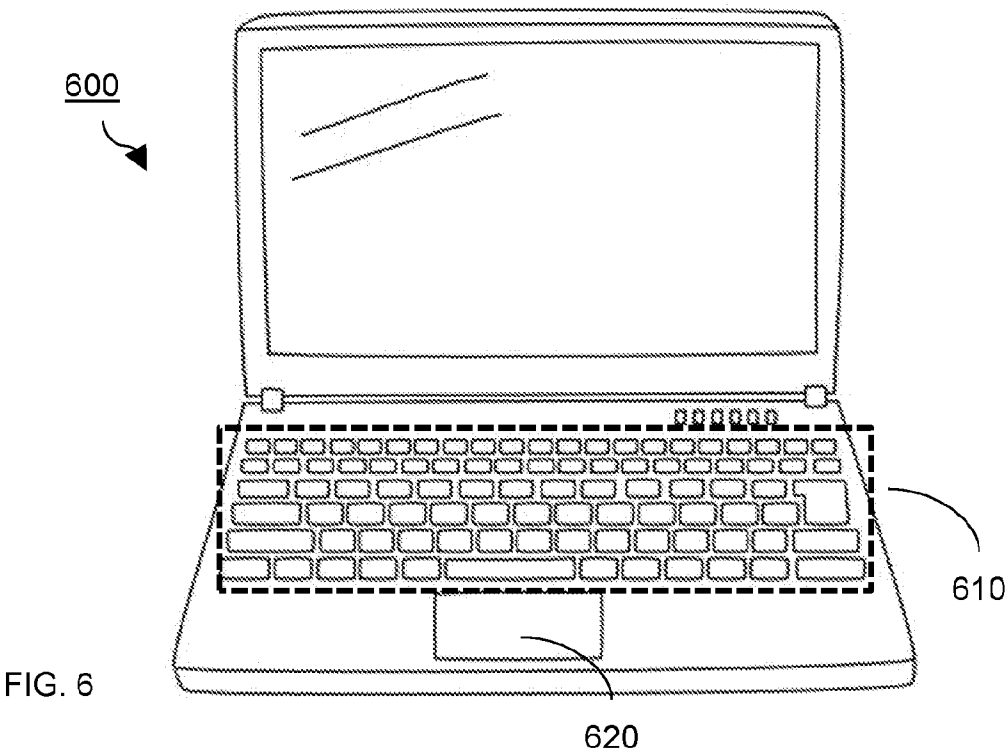

FIG. 6

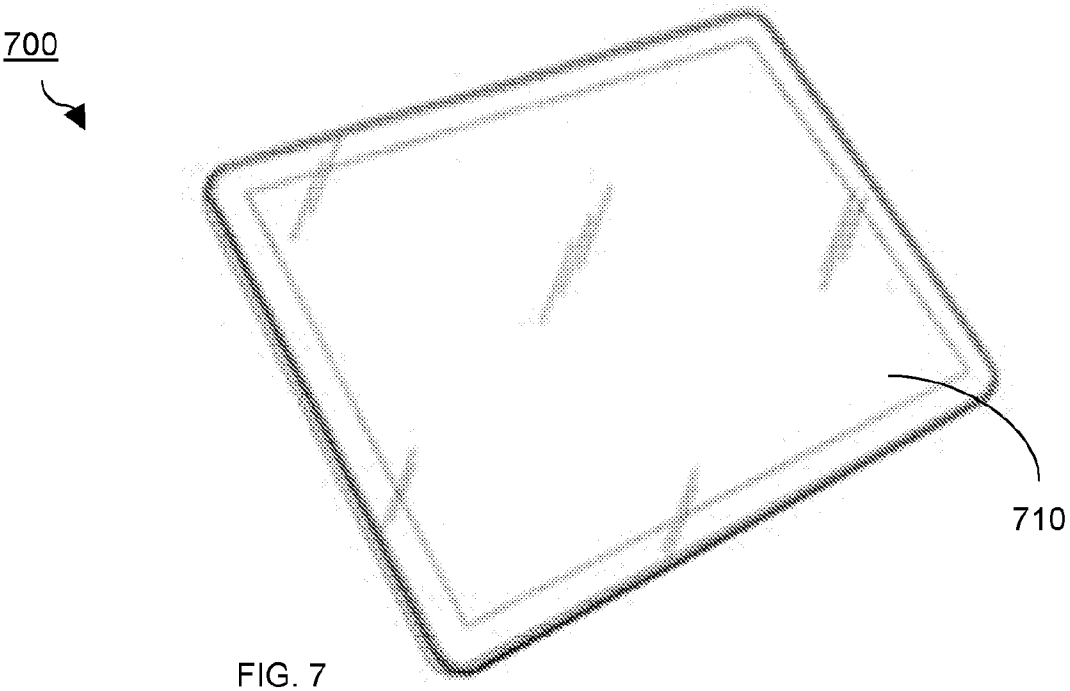

FIG. 7

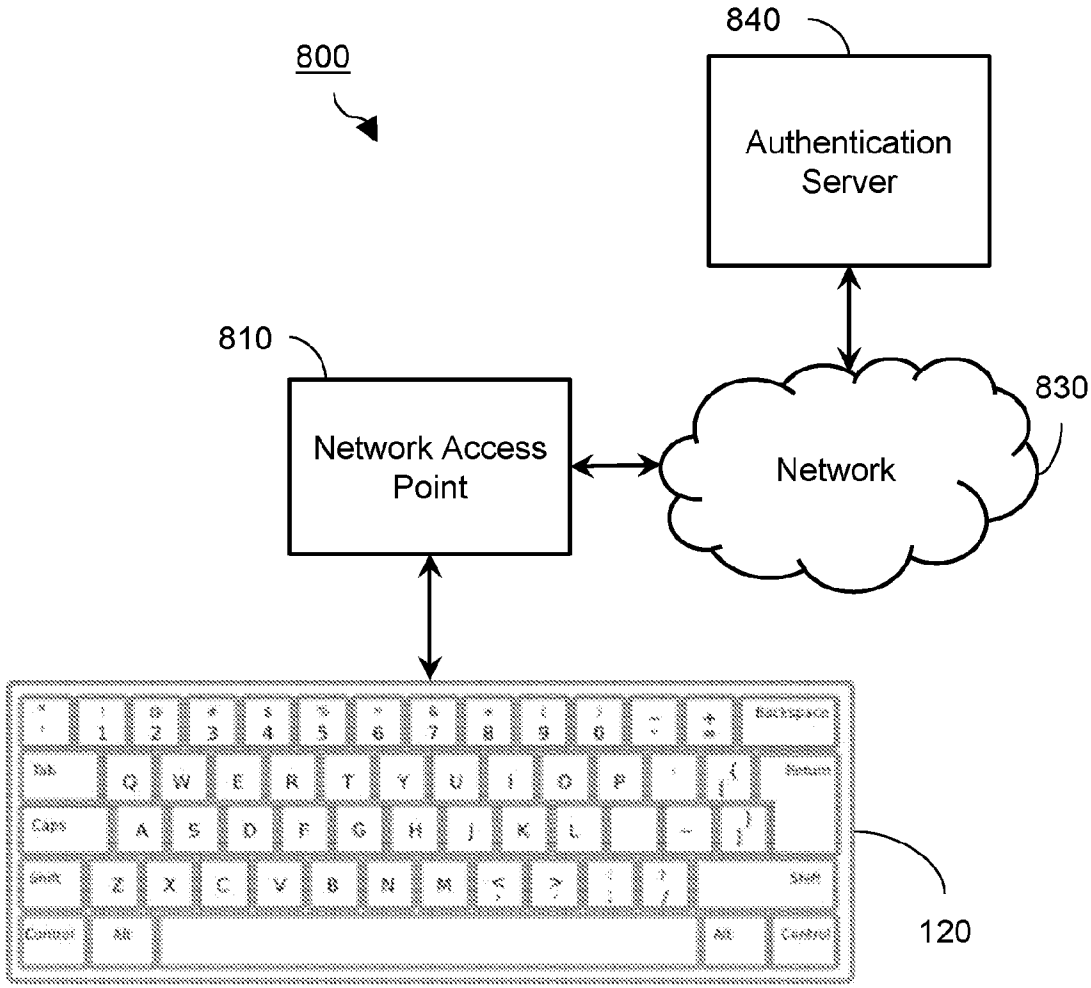
800
840
Authentication Server
810
Network Access Point
830
Network
120

FIG. 8

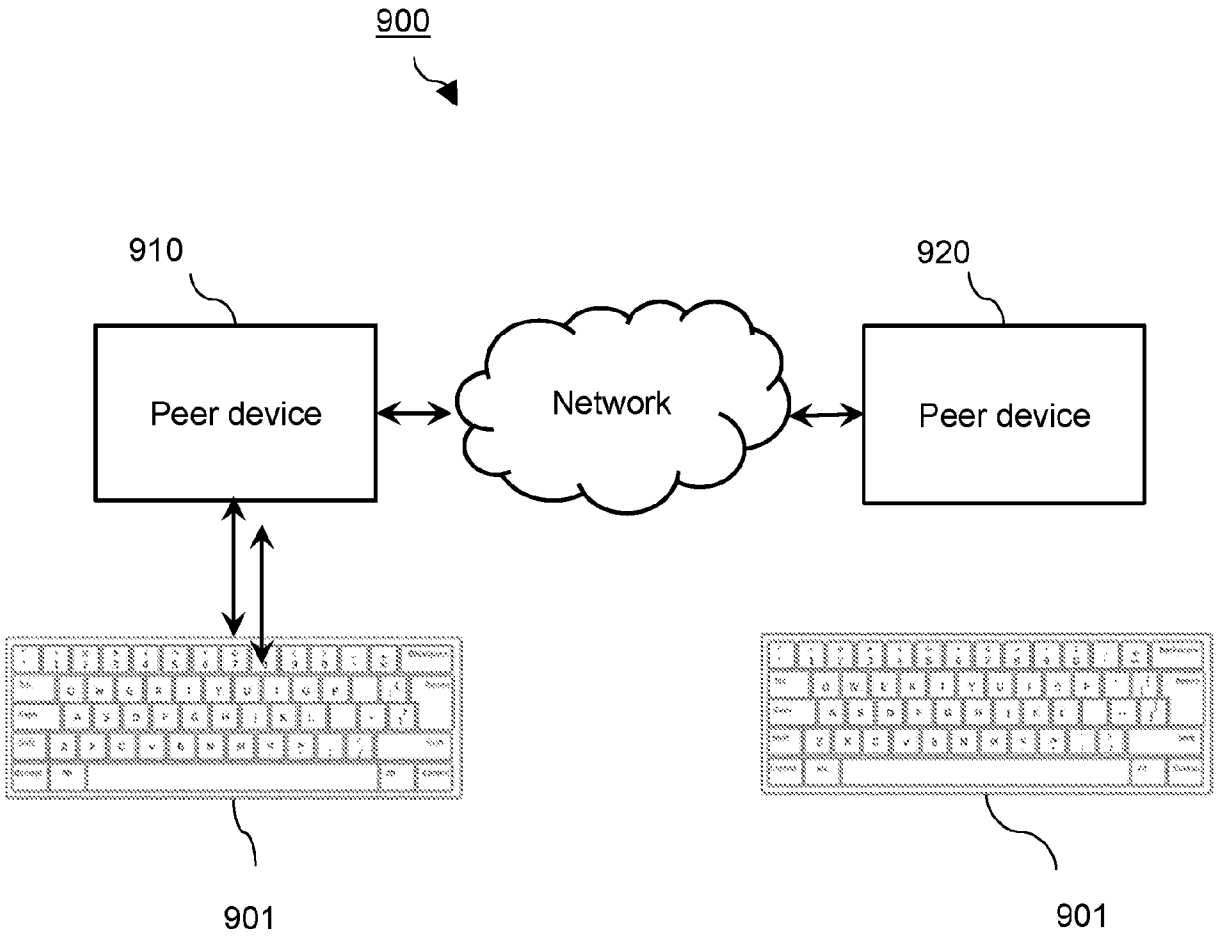

FIG. 9

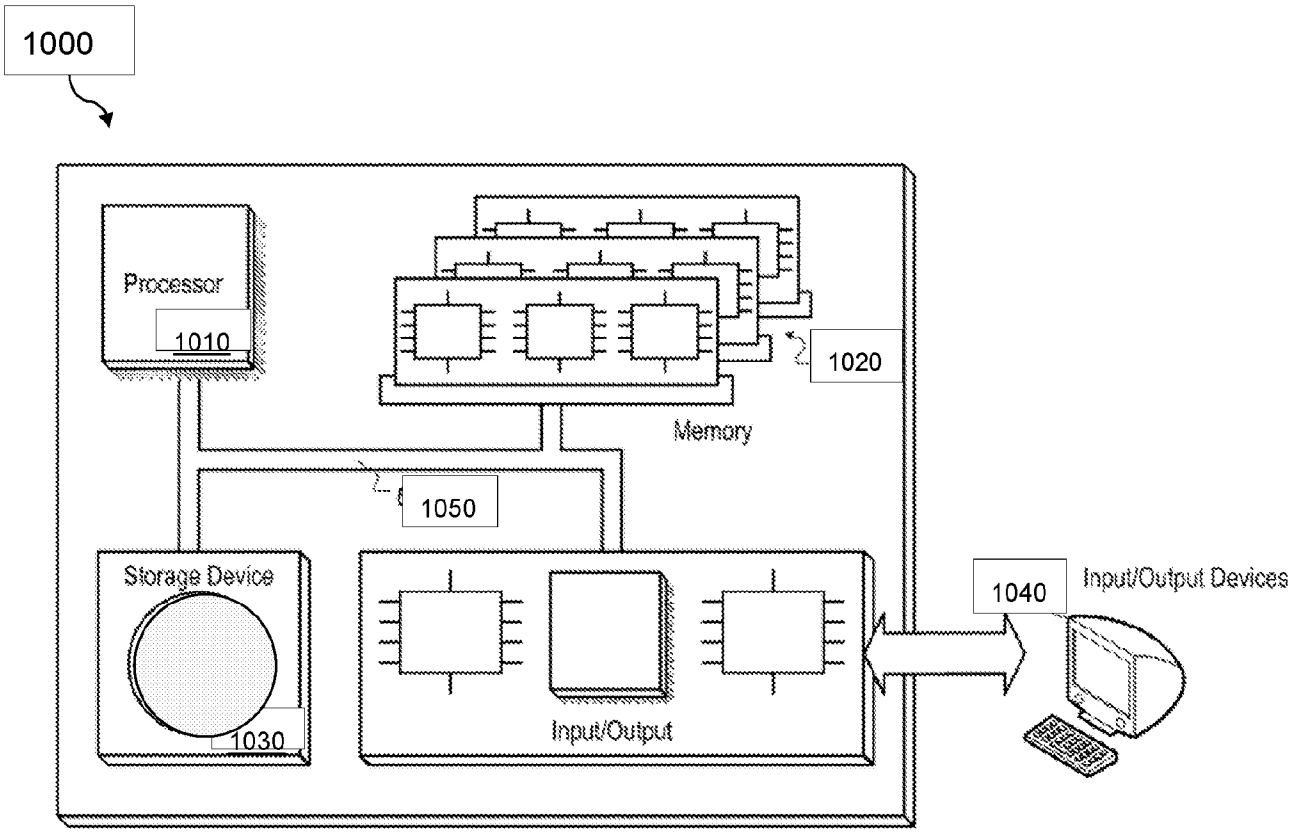
1000
Processor
1010
1020
Memory
1050
Storage Device
1030
Input/Output
1040
Input/Output Devices

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/035386

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)i, G06F 3/048(2006.01)i, G06F 3/041(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/32; G06F 21/20; G06F 21/45; G06F 21/83; G06T 7/00; H04Q 1/00; H04W 88/02; G06F 3/048; G06F 3/041

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: input interface, key, biometric sensor, different

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2008-197995 A (YAHOO JAPAN CORP.) 28 August 2008 See paragraphs [0011], [0027]-[0042]; claims 1-7; and figures 2-5.	1-3,5,26,28
Y		4
A		6-25,27
X	US 2015-0213245 A1 (QUALCOMM INCORPORATED) 30 July 2015 See paragraphs [0031]-[0042], [0050]-[0071], [0080]-[0101]; and figures 2, 5, 7-8.	6-25,27
Y		4
A	US 2015-0213244 A1 (MICROSOFT CORPORATION) 30 July 2015 See paragraphs [0025]-[0083]; and figures 8-18.	1-28
A	US 2012-0083311 A1 (TIMOTHY RYAN SALTER et al.) 05 April 2012 See claims 1-13.	1-28
A	US 2004-0075590 A1 (ESTHER MAE PEARSON) 22 April 2004 See paragraphs [0019]-[0020]; and figures 5-6.	1-28

☐ 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	Date of mailing of the international search report
18 October 2018 (18.10.2018)	**22 October 2018 (22.10.2018)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
CHIN, Sang Bum
Telephone No. +82-42-481-8398

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2018/035386

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2008-197995 A	28/08/2008	JP 4644689 B2	02/03/2011
US 2015-0213245 A1	30/07/2015	CN 106415570 A	15/02/2017
		EP 3100194 A1	07/12/2016
		JP 2017-511912 A	27/04/2017
		KR 10-1839860 B1	20/03/2018
		KR 10-2016-0114108 A	04/10/2016
		US 9747428 B2	29/08/2017
		WO 2015-116403 A1	06/08/2015
US 2015-0213244 A1	30/07/2015	CN 105980973 A	28/09/2016
		EP 3100152 A1	07/12/2016
		KR 10-2016-0114608 A	05/10/2016
		US 2016-0078210 A1	17/03/2016
		US 2017-0270289 A1	21/09/2017
		US 9223955 B2	29/12/2015
		US 9710632 B2	18/07/2017
		WO 2015-116477 A1	06/08/2015
US 2012-0083311 A1	05/04/2012	US 2014-0137233 A1	15/05/2014
		US 2017-0147804 A1	25/05/2017
		US 8667297 B2	04/03/2014
		US 9563759 B2	07/02/2017
US 2004-0075590 A1	22/04/2004	None	