SYSTEMS AND METHODS FOR USING EYE SIGNALS WITH SECURE MOBILE COMMUNICATIONS

Apparatus, systems, and methods are provided for secure mobile communications (SMC) by an individual using biometric signals and identification in real time. The apparatus includes a wearable computing device where identification of the user is based on iris recognition, and/or other physiological and anatomical measures. Biometric identity measures can be combined with other security-based information such as passwords, date/time stamps, and device identification. Identity verification can be embedded within information that is transmitted from the device and/or to determine appropriate security measures. SMC addresses security issues associated with the transmission of eye-signal control and biometric identification data using secure interfaces with network devices within a system of systems (SoS) software architecture.
FIG. 8
FIG. 9
FIG. 10

1. BIOMETRIC SCAN 1600
2. FEATURE EXTRACTION 1610
3. VECTOR GENERATION 1620
4. REED-SOLOMON ENCODER 1645
5. PRIVATE KEY ENCRYPTION 1640
6. PUBLIC KEY GENERATION 1660
7. SECURE PRIVATE KEY 1655
8. PUBLIC KEY CERTIFICATE 1665
FIG. 11

COGNITIVE LOAD MANAGER
1160

SITUATIONAL CONTEXT
1700

ENVIRONMENTAL CONTEXT
1710

PHYSIOLOGICAL CONTEXT
1720

ENVIRONMENTAL DATA
ACQUISITION
1715

PHYSIOLOGICAL DATA
ACQUISITION
1725

1810

1815
FIG. 18
FIG. 24

IRIS 800

155

700

155

600

155

HOME CONTROL 905

COZY HOME

975

XFINITY

970

NEST

965
2900 identify item to purchase based on eye gaze

2910 proper eye signal to "go" icon? no

2920 proper eye signal to confirm purchase? no

2930 determine device wearer ID based on iris image

2940 data base of authorized purchasers

2950 is device wearer authorized? no

2960 perform purchasing transaction

FIG. 29
SYSTEMS AND METHODS FOR USING EYE SIGNALS WITH SECURE MOBILE COMMUNICATIONS

RELATED APPLICATION DATA


COPYRIGHT NOTICE

[0002] Contained herein is material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the United States Patent and Trademark Office patent file or records, but otherwise reserves all rights to the copyright whatsoever. The following notice applies to the software, screenshots and data as described below and in the drawings hereto and All Rights Reserved.

TECHNICAL FIELD OF THE INVENTION

[0003] The present invention relates to portable or wearable biometric base user identification and authentication for secure distributed and interactive systems and services.

BACKGROUND

[0004] The widespread use of the internet and computing/ communications devices has led to an explosive growth in the electronic dissemination of information. However, verifiable control over the recipient(s) of secure information remains an important issue in the field of cyber security. Moreover, recipients of information can also become sources of sensitive information where real time knowledge of the identity of such a source can be an important security issue. An example of this situation is knowledge of the identity of an individual entering credit card (or other account) information during the process of making an online purchase. Present-day techniques commonly used to remotely identify the recipients or sources of secure information are readily susceptible to deception. In the United States, identity theft affects approximately fifteen million individuals each year with an estimated financial impact of $50 billion.

[0005] To solve these problems, there is a need today to re-think system architectures and roles with a specific view on data security and non-repudiation of a user’s electronic signature (e.g. password), where the authenticity of the signature is being challenged. In a general sense, nonrepudiation involves associating actions or changes to a unique individual. For a secure area, for example, it may be desirable to implement a key card access system. Non-repudiation would be violated if it were not also a strictly enforced policy to prohibit sharing of the key cards and to immediately report lost or stolen cards. Otherwise determining who performed the action of opening the door cannot be trivially determined.

[0006] Similarly, for computer accounts, the individual owner of the account must not allow others to use that account, especially, for instance, by giving away their account’s password, and a policy should be implemented to enforce this. This prevents the owner of the account from denying actions performed by the account.

[0007] The ecosystem is dynamic and rapidly changing, where wireless capability is growing exponentially. Cloud based architectures are becoming more appealing and attainable at manageable costs. The place to start re-thinking is with transitional and end architectures in mind and the placement of what is called a “data abstraction layer”, this abstraction layer is distinguished by data movement defined as data on the move and data at rest; and includes considerations for data generation, data storage, data processing, and the role of the server and browser in the cloud.

[0008] A first transitional step on the way to the Internet of Things (IoT) is the emergence of fog computing or fog networking. This is an architecture that uses one smart device, a collaborative multitude of smart devices or near-user edge devices to carry out a substantial amount of processing and storage (rather than stored primarily in cloud data centers), communication (rather than routed over the internet backbone), and control, configuration, measurement, and management rather than controlled primarily by network gateways such as those in the Long Term Evolution (LTE) such as 4G LTE.

[0009] Fog Networking consists of a control plane and a data plane. For example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives, resulting in superior user-experience and redundancy in case of failure. Fog Networking supports the IoT, in which most of the devices that are used on a daily basis will be connected to each other. Examples include phones, wearable health monitoring devices, connected vehicle, and augmented reality using devices such as the Google Glass. The ultimate goal of the IoT is to realize connections between objects, objects and persons, all things, and networks for the secure identification, management, and control of data.

[0010] With the above in mind, wearable display devices will challenge traditional computer human machine interaction. Today, computer mice, joysticks, and other manual tracking devices are ubiquitous tools for specifying positional information during human-machine interactions (HMIs). With the advent of wearable computing, such bulky and obtrusive devices that, for example, generally require stationary surfaces for proper operation are incompatible with the portable nature of apparatuses that are designed to be worn on the body.

[0011] Wearable display devices include virtual reality ("VR") displays such as those manufactured by Sony, Samsung, Oculus, Carl Zeiss; head mounted displays ("HMDs") such as those produced by Google (e.g., Glass®) and Vuzix; augmented reality ("AR") displays such as those manufactured by Microsoft, Vuzix, and DigiLens; and similar devices. Eye tracking can be used to view such displays and to specify positional information. However, the eyes are also used extensively during normal human activities.

[0012] In a further discussion of an embodiment with respect to security, data collected from the face, eye(s), or voice constitute unique biometric data of the user or user groups, if desired. These collected data can be used to generate a unique private key in a system of public key and private key cryptography. Cryptographic systems have been widely
used for information protection, authentication, and access control for many years and as such are well known in the art of information security.

[0013] An additional component for the continuous exchange of secure information with a biometrically identified individual is the encryption of all transmitted (i.e., sent or received) data. Data encryption has a long history that predates the electronic computer. A number of well-established methods have been developed to protect the confidentiality, integrity, and authenticity of data. Most encryption techniques make use of one or more secret keys or security codes that can be used to encrypt and/or decipher data streams. Keys used to encode or decipher data streams can originate from a number of sources including previously transmitted data sequences, identification codes embedded during the manufacture of a device, and usage counts.

[0014] Encryption and deciphering methods that make use of transposition, substitution, repositioning, masking, translation tables, and/or pre-defined numeric sequences are well-known in the art. More sophisticated techniques utilize multiple methods applied to larger blocks (i.e., more than a single character or byte) of information. In addition, encryption and deciphering methods that include a processing step within a protected hardware component are generally more protected from attempts at decoding compared to those implemented using software stored on some form of memory device.

[0015] Field-programmable gate arrays (FPGAs) and application specific integrated circuits (ASICs) are particularly useful as encrypting and deciphering components. In fact, Streicher et al. (U.S. Pat. No. 8,363,833) and others describe processes whereby even the bit stream used to program an FPGA that can be used for encryption, is itself encrypted. Concealing both security keys and methods to decipher secure information greatly reduces the risk of anyone other than the intended recipient gaining meaningful access to an encrypted data stream.

[0016] As further background, Bluetooth had its origins in 1998 with the release of the 1.0 specification, with a subsequent release in 2000 of what was called 1.0b. These early releases were designed to remove wires from the desktop of a user; these included considerations for serial, headset, cordless phone, and LAN connections. However, these early versions had many problems and manufacturers had difficulty making their products interoperable. Subsequent releases of Bluetooth 1.1, 1.2, and 2.0 included expanded bandwidth, profile capability, and finally, in release 2.1, new levels of security, including what is now called Secure Simple Pairing (SSP).

[0017] SSP allows two devices to establish a link key based on a Diffie-Hellman key agreement and supports four methods to authenticate the key agreement. One of these methods, called the Passkey Entry method, uses a PIN (i.e., personal identification number) entered on one or both devices. However, the Passkey Entry method has been shown to leak this PIN to any attacker eavesdropping on the first part of the pairing process. If the attacker can prevent the pairing process to successfully complete and the user uses the same PIN twice (or a fixed PIN is used), the attacker can mount a man-in-the-middle attack on a new run of the pairing process.

[0018] Today there are numerous papers on the security risks even the most sophisticated protocols are challenged with. New systems and methods are needed to ensure what is termed nonrepudiation; "nonrepudiation" generally means an assurance that someone cannot deny something. In this case, the denial of the ability to ensure the use of a device or communications from a device cannot deny the authenticity of their signature on any use, communications, or messages that a qualified user originates.

SUMMARY

[0019] Although the best understanding of the present invention will be had from a thorough reading of the specification and claims presented below, this summary is provided in order to acquaint the reader with some of the new and useful features of the present invention. Of course, this summary is not intended to be a complete litigation of all of the features of the present invention, nor is it intended in any way to limit the breadth of the claims, which are presented at the end of the detailed description of this application.

[0020] In this disclosure, voluntary eye movements that are intended to interact with a computing device are referred to as “eye signals.” Eye signal controls are described in Systems and Methods for Biomechanically-based Eye Signals for Interacting with Real and Virtual Objects [Attorney Docket No. EYE-023], application Ser. No. 14/____, filed May 8, 2015, the entire disclosure of which is expressly incorporated by reference herein.

[0021] Processes for identification of a device user are described in Systems and Methods for Discerning Eye Signals and Continuous Biometric Identification [Attorney Docket No. EYE-024], application Ser. No. 14/____, filed May 8, 2015, the entire disclosure of which is expressly incorporated by reference herein.

[0022] In accordance with one embodiment, apparatus, systems, and methods are provided for a head-mounted device (HMD) that includes at least one processor connected to at least one imager, where at least one of the imagers is oriented toward the eye(s) of a user. The processor is configured to at least one of substantially continuously, simultaneously, and/or periodically determine eye signal estimation, where the eye signal estimation is determined by the processor using the imager to detect at least one gliot from the surface of the eye that has been generated from a light source attached to the HMD or where the imager detects one or more distinctive features of the eye; and determine biometric data of a user including facial features, voice, or iris data of a user, where the biometric data is used for the identification and authentication of the user for access and control of at least one of the HMD, a connected device, a wireless device, and a remote server.

[0023] In accordance with another embodiment, apparatus, systems, and methods are provided that may substantially continuously, periodically, and/or on demand perform iris recognition utilizing a head-mounted device. Biometric identification during the formation of eye-signal controls may be used in a wide range of applications in which user identification and/or authentication are required in real time.

[0024] In another embodiment, systems and methods are disclosed in which eye-signal control sequences are used for authentication of a user for at least one of withdrawing money from an automated teller machine (ATM) and making online purchases.

[0025] Another embodiment discloses systems and methods to authenticate a user for online activities including at least one of private, group, or other testing, complying with performance requirements coupled with identity for various forms of employment such as professional driving, piloting, or other transportation, logging hours, confirming acknowledg-
[0026] Another embodiment discloses systems and methods for combining identifying characteristics with other security tokens including at least one of information tokens (passwords), physical tokens (keys), produced tokens (speech, gestures, writing), and other biometric tokens such as fingerprint and voiceprint.

[0027] Another embodiment discloses systems and methods that describe a plurality of system configurations, including:

[0028] Storing multiple user codes where searching and matching is performed entirely on an HMD.

[0029] Sending user code(s) to a specific processor for identification and matching.

[0030] Sending user code(s) to the cloud.

[0031] Augmenting or replacing common password-based access to computing devices.

[0032] Substantially continuously re-verify the identity of the device wearer.

[0033] Another embodiment discloses systems and methods for capturing an image of the iris, or a locally generated irisCode (e.g., as described in Systems and Methods for Discerning Eye Signals and Continuous Biometric Identification, filed May 8, 2015) from the iris image, and transmit the iris information to the cloud for authentication of any HMD.

[0034] Another embodiment discloses systems and methods that replace or augment common password-based access to computing devices.

[0035] Another embodiment discloses systems and methods to use a specific implementation of the continuous biometric identification (CBID) approach (e.g., as described in Systems and Methods for Discerning Eye Signals and Continuous Biometric Identification, filed May 8, 2015) to “buy at the aisle” by using eye-signal methods or processes referred to as “look to buy.”

[0036] Another embodiment discloses systems and methods for displaying (on an HMD or remote display device) information, including cost, the item.

[0037] Another embodiment discloses systems and methods for object recognition used to identify items for purchase that are simply viewed within the environment of the user.

[0038] Another embodiment discloses systems and methods that establish a true identity of a user wearing the HMD.

[0039] Another embodiment discloses systems and methods that prevent user identity fraud and identity theft.

[0040] Another embodiment discloses systems and methods that use the HMD to authenticate users for at least one of educational or legal purposes.

[0041] Another embodiment discloses systems and methods that use the HMD for the purpose of authenticating a purchase, where the authenticated purchase is for online purchase security and offline purchase security, where offline includes at a retail establishment.

[0042] Another embodiment discloses systems and methods that use the HMD that includes a second imager connected to the processor oriented outward from the HMD, where the second imager detects a code that can be decoded by the processor, where the code is one of a bar code and a QR (i.e., quick response) code and where the processor decoded data represents information about a product.

[0043] Another embodiment discloses systems and methods that use the information related to a product to allow an authenticated user to securely purchase the product.

[0044] Another embodiment discloses systems and methods that allow an entity to initiate a secure communication channel with another entity by mutual gaze where the security of the communication channel may be established prior to communication and may be revalidated continuously or at intervals during communication.

[0045] Another embodiment discloses systems and methods that enable a secure protocol for coordination among parties to cause an action to occur whereupon each party performs some action during which their identities are substantially continuously verified with CBID.

[0046] Another embodiment discloses systems and methods that increase security when using a HMD device by limiting access to functional blocks in a silicon chip that supports eye-tracking for the HMD device.

[0047] Another embodiment discloses systems and methods that manage, coordinate, filter, and/or sequence the stimulus provided by one or more wearable devices associated with the identity of a user.

[0048] In another embodiment, systems and methods are provided that include a dynamically evolving cognitive architecture for a system based on interpreting the gaze-based intent of a user. Natural eye movement is interpreted by the system, and used for real-time image services. An illumination device comprising a processor and a camera is worn by the user, with the camera aimed toward an eye of the user. The system includes memory with stored instructions. When the instructions are executed the system receives eye measurement data from the camera aimed at the user’s eye. The data is used to determine a first state of the eye, and compare it to data captured from a second state of the eye. When the system determines that the first and second states of the eye are the same, further instructions are sent to at least one processor in the system.

[0049] So as to reduce the complexity and length of the Detailed Specification, and to fully establish the state of the art in certain areas of technology, Applicant(s) herein expressly incorporate(s) by reference all of the following materials identified in each numbered paragraph below. The incorporated materials are not necessarily “prior art” and Applicant(s) expressly reserve(s) the right to swear behind any of the incorporated materials.

[0050] Applicant(s) believe(s) that the material incorporated by reference herein is “non-essential” in accordance with 37 CFR 1.57, because it is referred to for purposes of indicating the background of the systems and methods herein. However, if the Examiner believes that any of the above-incorporated material constitutes “essential material” within the meaning of 37 CFR 1.57(c)(1)-(3), applicant(s) will amend the specification to expressly recite the essential material that is incorporated by reference as allowed by the applicable rules.

[0051] The inventors are also aware of the normal precepts of English grammar. Thus, if a noun, term, or phrase is intended to be further characterized, specified, or narrowed in some way, then such noun, term, or phrase will expressly include additional adjectives, descriptive terms, or other modifiers in accordance with the normal precepts of English grammar. Absent the use of such adjectives, descriptive terms, or modifiers, it is the intent that such nouns, terms,
phrases be given their plain, and ordinary English meaning to those skilled in the applicable arts as set forth above.

[0052] Further, the inventors are fully informed of the standards and application of the special provisions of 35 U.S.C. §112, ¶6. Thus, the use of the words “function,” “means” or “step” in the Detailed Description or Description of the Drawings or claims is not intended to somehow indicate a desire to invoke the special provisions of 35 U.S.C. §112, ¶6, to define terms or features herein. To the contrary, if the provisions of 35 U.S.C. §112, ¶6 are sought to be invoked to define features of the claims, the claims will specifically and expressly state the exact phrases “means for” or “step for”, and will also recite the word “function” (i.e., will state “means for performing the function of [insert function]”), without also reciting in such phrases any structure, material or act in support of the function. Thus, even when the claims recite a “means for performing the function of . . .” or “step for performing the function of . . .”, if the claims also recite any structure, material or acts in support of that means or step, or that perform the recited function, then it is the clear intention of the inventors not to invoke the provisions of 35 U.S.C. §112, ¶6. Moreover, even if the provisions of 35 U.S.C. §112, ¶6 are invoked to define the claimed features, it is intended that the features not be limited only to the specific structure, material, or acts that are described in the embodiments, but in addition, include any and all structures, materials or acts that perform the claimed function as described in alternative embodiments or forms, or that are well known present or later-developed, equivalent structures, material or acts for performing the claimed function.

BRIEF DESCRIPTION OF THE DRAWINGS

[0053] A more complete understanding of the present invention may be derived by referring to the detailed description when considered in connection with the following illustrative figures. In the figures, like-reference numbers refer to like-elements or acts throughout the figures. The presently embodiments are illustrated in the accompanying drawings, in which:

[0054] FIG. 1 is a front view of a human eye.
[0055] FIG. 2 is a section view of a human eye from the side.
[0056] FIG. 3A depicts a top down view of an eye showing the regions of vision.
[0057] FIG. 3B shows an example approximation of the sizes of the regions of vision.
[0058] FIG. 4 depicts overall system architecture.
[0059] FIG. 5 depicts architecture of the eye signal object.
[0060] FIG. 6 depicts abstracted hardware.
[0061] FIG. 7 depicts typical Bluetooth architecture.
[0062] FIG. 8 depicts hardware interface and hardware components.
[0063] FIG. 9 depicts imaging architecture.
[0064] FIG. 10 depicts biometric data generation.
[0065] FIG. 11 depicts a breakdown of a cognitive load manager.
[0066] FIG. 12 depicts system components of the cognitive load manager.
[0067] FIG. 13 depicts a HMD (head mounted device) connecting to a mobile device.
[0068] FIG. 14 depicts a HMD connecting to the cloud.
[0069] FIG. 15 depicts a HMD connecting to home and vehicle controls.

[0070] FIG. 16 depicts communication between a HMD and a NEST™ thermostat system.
[0071] FIG. 17 shows system architecture on a HMD communicating with the cloud.
[0072] FIG. 18 depicts a breakdown of the data manager.
[0073] FIG. 19 shows the system architecture of a HMD with the processing capabilities moved to the cloud.
[0074] FIG. 20 shows further evolution of a HMD towards the Internet of Things.
[0075] FIG. 21 depicts the system architecture from a HMD moved to a remote server.
[0076] FIG. 22 depicts a HMD with all processing pulled off to the cloud.
[0077] FIG. 23 depicts a HMD and the remote server communicating.
[0078] FIG. 24 depicts a HMD communicating with home control systems.
[0079] FIG. 25 depicts a HMD communicating with social media.
[0080] FIG. 26 depicts a HMD communicating with home entertainment systems.
[0081] FIG. 27 depicts a HMD communicating with vehicle entertainment systems.
[0082] FIG. 28 depicts a HMD communicating with vehicle control systems.
[0083] FIG. 29 is a flow chart of steps taken to perform an online, secure purchase.

DETAILED DESCRIPTION

[0084] In the following description, and for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the various aspects of the embodiments. It will be understood, however, by those skilled in the relevant arts, that the apparatus, systems, and methods herein may be practiced without these specific details. It is to be understood that other embodiments may be utilized and structural and functional changes may be made without departing from the scope of the apparatus, systems, and methods herein. In other instances, known structures and devices are shown or discussed more generally in order to avoid obscuring the embodiments. In many cases, a description of the operation is sufficient to enable one to implement the various forms, particularly when the operation is to be implemented in software. It should be noted that there are many different and alternative configurations, devices, and technologies to which the disclosed embodiments may be applied. The full scope of the embodiments is not limited to the examples that are described below.

[0085] The anatomy of the eye is well known in the art. For the purposes of this disclosure, relevant anatomy is depicted and described. FIGS. 1 and 2 generally depict the anatomy of the human eye 100. FIG. 1 is a front view of the eye 100 showing the pupil 145, iris 115, sclera 150, limbus 245, pupil/iris boundary 250, upper eyelid 105, lower eyelid 110, and eyelashes 235. FIG. 2 is section view of the eye 100 showing the pupil 145, iris 115, retina 52, sclera 150, fovea 160, lens 165, and cornea 170. The pupil 145 is the approximately round dark portion at the center of the eye that expands and contracts to regulate the light the retina 52 receives. The iris 115 is the colored portion of the eye 100 that surrounds and controls the expansion and contraction of the pupil 145. The sclera 150 is the white region of the eye 100 that surrounds the iris 115. The sclera 150 contains blood vessels and other identifiable markers. The limbus 245 is the outer edge of the
The pupil/iris boundary is where the pupil and the iris meet. The eyelids and the eyelashes surround the eye and partially cover or obscure portions of the eye during blinks, eye closures, or different angles of viewing. The retina is the sensory membrane that lines the eye and receives images from the lens and converts them into signals for the brain. The fovea is a small, circular area in the retina that contains only cones (no rods) and provides particularly acute vision. The lens is the nearly spherical body of the eye behind the cornea, which focuses light onto the retina. The cornea is the clear part of the eye covering the iris, pupil, lens, and sclera.

Wearable computing systems may implement without an operating system and robust support. A power management scheme and ACPI elements discussed above will need to be pulled up to an application control level, giving the application and user dynamic control of the power scheme. As discussed below, in highly abstracted embodiments, the ACPI might implement in a split or distributed fashion. This current standard does not fully anticipate the challenges of wearable computing devices like an HMD disclosed in this specification; therefore additional considerations for operating HMD systems in multiple modes is disclosed.

An HMD may include a low-power mode of operation that may be deployed during times when no eyes are detected. This typically occurs when the user removes the headwear or when the headwear has shifted out of place on a user’s head. This functionality could be implemented in silicon as a system on a chip (SOC).

At any time, the device can be re-mounted by the original user or worn by a new user. For purposes of device calibration (e.g., to account for anatomical variations among individuals) and/or user authentication, it is desirable for the device to be capable of determining the identity of registered users when re-mounted or re-deployed. This can include loading a new set of configuration/calibration parameters and differentiating identities between the previous and new user; including halting, pausing and/or concealing the outputs of any ongoing programs launched by the previous user.

Typically under the old standard, once the Operating System Power Management (OSPM) activates ACPI, it takes over exclusive control of all aspects of power management and device configuration. The OSPM implementation also exposes an ACPI-compatible environment to hardware drivers, which in turn impacts the system, device, and processor states; and these are managed globally as Power States and these include Global States, Device States, Processor States, and Performance States.

Power consumption is an omnipresent concern, particularly if the device is not worn for an extended period. A commonly deployed solution to this issue is an “off” switch that completely powers down an electronic device. However, the time and inconvenience of “powering up” a headset device is restrictive particularly, for example, if the device has only been removed from the head momentarily.

Low-power HMD and eye-signal control anticipates these issues by using at least one technique comprising:

- modifying the Processor States by reducing clock rates to processor(s);
- modifying Performance States by confining processing to a low power processor or portion of a processor;
- modifying Device States by imaging at a reduced frame rate;
- modifying Global States by turning the camera off or into a low-power mode between images;
- reducing illumination;
- collecting and/or processing images with reduced spatial resolution;
- limiting algorithms (particularly those associated with searching for iris boundaries) to low-spatial resolution modes.
relaxing stringency measures during irisCode comparisons, and

fabricating specific dedicated hardware (a chip or SOC) that operates in a low-power mode that does not "power-up" the full device until a low-level authentication has occurred. Further, such a chip or SOC could prohibit access to other embedded functionality or connected or wirelessly connected devices until authentication, possibly following power up and the determination of a user’s eye viewing a display or other target object is performed.

This specific dedicated hardware can utilize modern methods of “hybrid” chip manufacturing that can segment a portion of circuitry to operate in an extremely low power mode. This hybrid circuitry effectively builds a “firewall,” preventing an unauthorized user from fully powering up or utilizing a device.

Another application of low-power HMD modes is when a low-battery state is sensed. Instead of running a device until all global functions cease, a “graceful degradation” model is implemented as part of the new class of Power State for HMDs. “Graceful degradation” can include algorithmic approaches by limiting the use of more power-hungry (i.e., generally more sophisticated) image processing and other routines, as well as any number of the hybrid and hardware approaches to reduce power while maintaining at least partial functionality, discussed above. Low-power modes for the processor and critical operations continue until the battery finally runs out of power, the unit is plugged into a central power source, or the device is placed sufficiently close to an inductive charging station.

Another power management concern for all forms of wearable computing is that more sophisticated algorithmic eye tracking and user interface techniques can draw upon faster or parallel central processing units (CPUs), but generally these approaches require more power. Greater power consumption results in larger and/or heavier batteries, and/or shorter device use times between recharging or replacing batteries.

An alternative or adjunct to the deployment of more/faster CPUs is the use of embedded or distributed processing approaches. These can be implemented within a variety of hardware components including field-programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), complex programmable logic devices (CPLDs) and hybrid devices that can include system-on-chip (SOC) configurations.

Embedded or distributed processing can facilitate existing, CPU-based approaches by off-loading computationally intensive routines. Hardware dedicated to performing these routines can be faster (often requiring only one, or just a few, clock cycles) and utilize less power (often by greater than an order of magnitude). Distributed processing can also facilitate new algorithmic approaches that are generally not feasible (within time and power-consumption constraints) using CPUs. Distributed processing is particularly valuable within algorithms that require repeated and/or simultaneous application of calculations to be performed on large data sets such as video images. These are further discussed below in the sub-section Distributed Processing.

Another embodiment utilizes low-power distributed processing to detect whether the device has been removed from the head. In order to implement an “instant on” capability, the device must “sense” whether it is mounted on the wearer’s head or has been removed. A method to perform this function (without adding additional hardware) is to determine if an eye can be viewed within eye-tracking camera images. As described elsewhere, power consumption can be reduced when the device is not in use (i.e. removed from the head) by a reduced frame rate, low resolution imaging, lower CPU clock rate, etc.

For low-power eye-presence measurements, illumination can be eliminated or reduced by reducing the power of illuminating LEDs, reducing the number of LEDs turned on and/or only turning on illuminator(s) when actually sampling camera images (at reduced frame rates). A substantial reduction in power can also be attained by embedding relatively simple eye geometry detection routines in distributed processing hardware. An example of this is one form of convolution filter to determine if an image (i.e. of an eye) is present is a focus filter. Such a filter would be classified as a high-pass spatial filter that detects the presence of high spatial contrast edges. The absence of such edges indicates that the device has been removed from the head when a defocused image is generally present (i.e. absent a high-contrast object located at the approximately 25 mm focal distance of the camera). Another approach is to detect a dark (i.e. pupil) region adjacent to a white (i.e. sclera) region. When an in-focus eye is detected, the device “powers up” (recognizing that it was not completely powered off) for higher resolution eye tracking.

In another embodiment, the device may include a micro electro-mechanical system (MEMS) such as an accelerometer or rate sensor for determining motion. When the device is not being worn it may operate at an ultra-low power mode in which it is not intermittently searching for the presence of an eye. In the ultra-low power mode, the device may only search for the presence of an eye when movement of the device is detected, for instance when a user picks up the device. When movement is detected, the device may initiate a scan in search of an eye or eyes at predetermined intervals (for instance every two seconds) or substantially continuously for a period of time (for instance one minute) as set by user preferences. If the device fails to detect an eye in the pre-set time interval it may resume ultra-low power mode or it may cycle through a low power mode prior to resuming ultra-low power mode. Should an eye or eyes be detected, the device will switch into full power mode or into a power settings scheme as set by the preferences of the detected user. The primary device owner (administrator) may set the overall system power schemes that will govern the power mode settings for the device when it is not in use. Additionally, the device owner may lock down changes to the power schemes such that other users are unable to edit them.

FIG. 5 depicts a further breakdown of the IRIS Object 1000, including eye tracking 1100, a module for tracking the eye gaze of a user; eye data 1105 for user identification using biometric data of the user such as facial, speech and iris identification; eye control 1100 for relating the user’s eye gaze to a display, iUI® interface (an interface comprising eye-signal controls) 1116. Eye signals 1115 gleaned from eye movements are used to interact with a user interface iUI 1116 and display screen(s) and images on the display.

Included in the IRIS object 1000 are a number of software modules operative as managers of certain functions. As an example, but not limiting to:
Device Manager 1120 that allows a user to control hardware attached to the system, whether it be the imager in the HMD, a cell phone attached, or a vehicle infotainment system.

Data Manager/Personal Data Management 1125 enables the secure storage and access to user data such as e-mail, messages etc. The Data Manager 1125 also may include one or more of password management software, web browser favorites, and cryptographic software. Advance data management can include, as an example, setting and establishing a Virtual Private Network (VPN), terminal services with an external processor, whether local or accessible through the internet.

Communications Manager 1130 is designed to pass information from one system to another and provides remote access to systems and transmits files in a multitude of formats between computers. The Communications Manager 1130 also may include link management and data routing.

Security Manager 1135 refers to software steps or measures used to protect the HMD and user from threats, viruses, worms, malware, or remote hacker intrusions; to include preventive-control techniques, which safeguard the system and its data from being stolen or compromised.

Power Manager 1140 manages device power schemes to optimize and maximize a user’s experience and device battery life.

Display Manager 1145 has two basic functions: how the eye is trained to objects on the screen in the mode of the UI 1116; and what is displayed to the user in the HMD. The Display Manager 1145 also has the ability to transfer all or portions of the screen in the HMD to an external display, such as a computer screen, the dashboard of a vehicle, or a home entertainment monitor such as a TV.

With now a further discussion on the Security Manager 1135, a number of additional controls may be included, for example audio/video (A/V) control 1150; speech control 1155; or something more complex, e.g., cognitive load control 1160 (FIGS. 11 and 12).

The HAL 1030 (FIG. 6) includes the “hosted” aspects of external hardware systems; this generally includes software specific to the IRIS platform developed specifically for integration. The hardware anticipated, but not limited to, is a Bluetooth interface 1170 (discussed separately below as one embodiment), a TCP/IP interface 1175 to any form or any type of TCP communications to include 802.2 (wireless interface) 802.11, 802.15 (WPAN—Wireless Personal Area Networks other than Bluetooth), and 802.20 Wi-Max; this includes stacks that support the network and transport software 1195 and the physical links to wired or wireless systems. In addition, there are considerations for other systems through the Hardware IF 1180, which interfaces with external software and/or hardware drivers through physical links 1235; these physical links can be F/C, USB, serial, or proprietary.

In a discussion of one embodiment, as an example, the Bluetooth system has been selected in a non-limiting example of an embodiment because it is so pervasive in the rapidly growing market of mobile devices. As an example, today almost all vehicles have what are called infotainment systems; these are a combination of entertainment such as music and videos as well as information, where the information could come from within the vehicle as data from a sensor, control of a system like a heater or lights, or information available through the internet. Most of these systems use wired and wireless technologies to connect to the vehicle and/or the internet. Today, the wireless connections to the vehicle are generally Bluetooth established through a set of standard interfaces; these are referred to as Profiles 1300 (FIG. 9) and are hosted in a processor above the Bluetooth radio, further shown in FIG. 5 as Hands Free Profile (HFP) 1187; Advanced Audio Distribution Profile (A2DP) 1193, Audio Video Remote Control Profile (AVRCP) 1190, etc.

To date, it has not been anticipated that a HMD 600 would be used in a vehicle to control vehicle operations 915; to include the Infotainment system 910; therefore incorporation of one of the newest Profiles is inevitable, this Profile is called Human Interface Device (HID) Profile; profiles 1210, 1215, 1220, and 1225 exchange information from the applications through the profiles across the hardware abstraction to the Bluetooth module and Bluetooth radio. FIG. 6 depicts a Bluetooth systems architecture, including connections to the profiles, network and transport 1230, and the data link 1250 and modem 1255.

FIG. 7 depicts a breakdown of the Bluetooth architecture 1205 broken down into their subcomponents. Underlying all of these protocols is a key piece of Bluetooth termed the Service Discovery Protocol (SDP) 1310, which includes what is called Simple Secure Pairing (SSP). SSP today is required by all Bluetooth standards above v2.1. Secure Simple Pairing uses a form of public key cryptography, which can help protect against what is called “man in the middle,” or MITM attacks. Generally, the Bluetooth HID 1185 specification requires a security mode 4 for pairing and bonding two devices together citing that it should not be possible to perform pairing or bonding to any Bluetooth HID Host or Device without physical access to both the Bluetooth HID Host and Bluetooth HID device. Bluetooth HID Hosts and Bluetooth HID devices that support bonding use some form of non-volatile memory to store the 128-bit link keys and the corresponding BD_ADDRs, as well as the type of each link-key (authenticated, unauthenticated, or combination). In the case of a HMD, complex access is limited as there is no mouse or keyboard in a conventional sense. However, there are other ways to establish a secure link that have not been anticipated by Bluetooth, even though Bluetooth acknowledges the precepts of Public key cryptography.

In another example, a Bluetooth HID Host that accepts sensitive information from Bluetooth HID devices may be implemented to only accept sensitive information from reports that are contained in a top-level application collection of “Generic Desktop Keyboard” or “Generic Desktop Keypad.” Furthermore, such a Bluetooth HID Host may require MTM protection when pairing with any Bluetooth HID device with a Bluetooth HID report descriptor that contains a top-level application collection of “Generic Desktop Keyboard” or “Generic Desktop Keypad,” which in turn contains any of the following sets of usage codes and their descriptions:

IC—irisCode: the result of applying pattern-recognition techniques to images of an eye to quantify the epigenetic patterns within an iris into comparable bit-patterns for the purpose of biometric identification.
I0128 IIC—Encrypted IC: an irisCode that has been encrypted so that it cannot be reverse engineered to an original image of the iris or any other iris-based, derived parameter.

I0129 TEIC—Target EIC: an identified EIC in which a match with an IC computed from an image of an eye indicates association and thus, a positive biometric identification.

I0130 CBID—Continuous Biometric Identification: the repeated process of biometric identification that can be performed either on a headset device or remotely by transmitting EICs, or images of one or both eyes to a remote processor. CBID can occur at a fixed rate (e.g. 30 times per second) or an asynchronous rate (e.g. each time the device is moved or re-mounted).

I0131 The following table refers to the transmission and comparison of EICs; however, it is algorithmically possible to convert images of eyes into ICs and subsequently into EICs. Thus, CBID can equivalently involve comparisons and/or the exchange of information involving images of irises, ICs, EICs or other derived parameters. Similarly, databases used for biometric comparisons could equivalently (for the purposes of identification) contain ICs, EICs, images of eyes, images of faces (including eyes), images of irises, so-called “unfolded” (i.e. expressed in polar coordinates) iris images, or other derived parameters. Therefore, references to exchanges or comparisons of EICs also refer to the exchange or comparison of any other derived data sets for the purpose of biometric identification.

I0132 In Table 1 below, where a set of programmable attributes can be assigned to a new Bluetooth profile, these attributes can be used:

<table>
<thead>
<tr>
<th>Attribute ID</th>
<th>Attribute Value</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtendedProtocolDescriptor list</td>
<td>0x36 0x0C</td>
<td>Data element sequence, 12 octets</td>
<td>Following the BT HID 1.1</td>
</tr>
<tr>
<td>0x20F (Next BT HID Revision) stand-alone, 1 of 1</td>
<td>0x36 0x01</td>
<td>Boolean8, single TEIC stored within headset with no off-headset communication required for CBID</td>
<td></td>
</tr>
</tbody>
</table>

I0133 Other examples of programmable attributes include:

I0134 recognize an individual member of a family, all of whom are permitted to use a device (e.g. dynamically loads calibration factors associated with each user)

I0135 pay-per-view rental of a public HMD

I0136 enabling multiple, general-use headsets available to employees within a business

I0137 online purchase from an online “store” in which a user has been registered with no restrictions on the device used to make a purchase.

I0138 online purchase from an online “store” in which both a user and specific headset have been registered

I0139 determine if user is on a “no-fly” list

I0140 confidential list of traditional passwords

I0141 taking an examination within a massively online course

I0142 medical records made available to primary care doctor, specialist, and patient

I0143 structured advertising based on the demographic of an identified viewer

I0144 a device license agreement sent to a user

I0145 confirmation that all components of a legal document have been viewed

I0146 confirmation that a notice of changes in terms and conditions has been sent to a user

I0147 confirmation of informed consent related to legal documents

I0148 pre-flight inspection by a pilot

I0149 identification of a vehicle driver and possibly identifying pre-accident driver distractions

I0150 retrieve e-mail based on user identification where another user would be offered separate e-mail access

I0151 outgoing text and e-mail can (optionally) be tagged to indicate the CBID user is the author

I0152 electronically “sign” legal documents

I0153 administration of an examination that must take place in the presence of both student and an instructor

I0154 exchange of personal information between/ among people who have just met

I0155 purchases made in a bricks-and-mortar store that requires no check stand

I0156 remote control of door opening for authorized personnel only

I0157 gaining or restricting access to a building based on user identification

I0158 tracking an individual under house arrest

I0159 tracking an individual restricted from entering a casino or interacting with another individual

I0160 ensure legal purchase of alcohol or other age-sensitive materials to an individual

I0161 automatic 911 call with user identification (that can be linked to medical history), “vitals” and geographic location

I0162 based on CBID, interact with an automated teller machine

I0163 gaining access to highly secure military sites

I0164 proving the historical activities of an individual under investigation

I0165 restricting access to the audio/video of a private conversation

I0166 restricting access to the audio/video of a conference to participants

I0167 restricting access of a data set of a private conversation to CBID participants

I0168 when/where is the last time I saw my car keys?

I0169 list hockey (versus basketball or some other sport) scores first

I0170 control household thermostat by an adult (not a child)

I0171 remotely turn on household entry lights

I0172 In a further discussion of the image process and use of the imager or video, in the embodiment described above, a system is anticipated where the HMD is implemented with a single conventional 2D imager system oriented either toward the eye and face and outward facing to the scene. However, in an alternate embodiment, consideration is anticipated for the
HMD to be implemented with multiple imagers oriented toward the face and eyes as well as the scene, where the multiple imagers generate a stereoscopic 3D video image. In addition to stereoscopic 3D images, consideration for other forms of 3D image generation has been anticipated by the applicant. Today, non-contact three-dimensional cameras, or digitizers, generally fall into four categories: stereoscopic digitizers (as mentioned above), silhouette digitizers, timing digitizers, and projected pattern digitizers. The underlying 3D surface imaging technologies can further be summarized in terms of four broad categories: Spatial Phase Imaging (SPI), Triangulation, Time of Flight (TOF) and Coherent approaches.

Spatial Phase Imaging generally relies on the polarization state of light as it emanates from surfaces to capture information about the shape of objects. Triangulation employs the location of two or more displaced features, detectors, and/or illuminants to compute object geometry. Two important triangulation subcategories are stereo correspondence (STC) and stereoscopic (STO). Stereo correspondence cameras determine the location of features in a scene by identifying corresponding features in two or more offset intensity images using 3D geometry to compute feature location. Stereo cameras rely on human biological systems (eyes, brain) to create a notion of a 3D scene from two images taken from different vantage points and projected into the eyes of a viewer. Finally, coherent methods rely on a high degree of spatial and/or temporal coherence in the electromagnetic energy illuminating and/or emanating from the surfaces in order to determine 3D surface geometry.

Figs. 8 and 9 depict imager object code 1415 for either a 2D or 3D implementation. Regardless of the technology employed, any system implemented must consider two key factors: human-fidelic visualization (completely realistic display) and visual intelligence (automated vision). Human-fidelic visualization can create a visual notion of a scene in the mind of a human that is as realistic or almost as realistic as viewing the scene directly; the visualization system is human-fidelic. An imaging system has to be 3D to be human-fidelic, since human sight is 3D. The second being visual intelligence, which means sensing and analyzing light to understand the state of the physical world. Automatic recognition of human emotions, gestures, and activities represent examples of visual intelligence. 2D video cameras struggle to provide a high level of visual intelligence because they throw away depth information when a video is captured. As a consequence of neglecting depth, 2D images of 3D scenes are inferior to 3D images. 3D images have better contrast (the ability to distinguish between different objects). Real video of real scenes typically contains dozens of instances where contrast and depth ambiguity make it difficult for automated systems to understand the state of the scene.

3D video cameras do everything that 2D cameras do, but add the benefits just discussed. It is inevitable that single lens native 3D video will eventually replace 2D video offered today by offering two interesting benefits: human-fidelic visualization and improved visual intelligence. It is reasonable to assume that global production of most cameras will shift to 3D as they become cost effective, simple to operate, compact and produce visual fidelity. With this in mind, the technology emerging today as the most likely to reach mass markets in terms of cost, complexity, and fidelity is Spatial Phase Imaging within the broad 3D imaging categories discussed. This technology relies on commercially available imagers implementing a micro-polarizing lens over four sub-pixels resulting in an ability to rapidly determine small changes in reflected light, computing a vector as a direction cosine for each pixel and generating a three-dimensional value in terms of X, Y and Z-depth; truly a single lens native 3D video.

In another embodiment, the accuracy of both CBID and eye-signal control processes can be improved via the use of more than a single camera to view an eye. Images substantially simultaneously or sequentially acquired from multiple cameras can be used to 1) create on-axis (i.e. perpendicular to the surface) views of different regions of the eye, 2) view surfaces with specular reflections (particularly glints) located at different positions within images of the eye, 3) allow for viewing of fine structures while maintaining the ability to view over a wide spatial range, 4) increase eye tracking accuracy by making multiple measurements based on multiple views of glints and eye structures, and 5) view "around" obscuring objects such as eye lids and lashes.

Another area where distributed/embedded processing is particularly valuable is in the "off-loading" of operations that are computationally intensive for a CPU. Examples of such a "hybrid" approach (i.e. mixing CPU and embedded processing) within eye tracking and iris identification algorithms include subroutines that perform Fast Fourier Transform (FFT), random sample consensus (RANSAC), so-called StarBurst feature extraction, and trigonometric functions.

Included within the system architecture are methods for managing cognitive load for safety, optimized performance, and general well-being for individuals and groups. Generally, the concept of cognitive load extends from tactical fighter programs and activities that generally relate to situation awareness. These in turn drive cognitive load control 1160 in programs like cockpit workload management; cognitive load control 1160 generally deals with the human mind interacting with some external stimulus.

The definition of cognitive load is slightly different in different fields; for example, in an academic sense cognitive load refers to the total amount of mental activity invested on working memory at any instance in time; while in the ergonomics literature it is described as the portion of operator information processing capacity, or resources that are required to meet cognitive task demands. Each field provides different methods to measure cognitive load.

Cognitive load is considered herein as the mental effort or demand required for a particular user to comprehend or learn some material or complete some task. Cognitive load is relative to both the user (i.e., their ability to process novel information) and the task being completed (i.e., complexity), at any single point in time. It is attributable to the limited capacity of a person’s working memory and their ability to process novel information.

Conventional methods for measuring cognitive load, include:

- subjective measures, such as self-rating scales;
- physiological techniques, such as pupil dilation, heart rate and galvanic skin responses;
- task or performance based measures, such as critical error rates and task completion times; and
- behavioral measures, such as speech pathology (e.g., impairment, self-talk, etc.)
There are a number of problems with these methods for measuring cognitive load, including:

1. Some of the methods are intrusive and disrupt the normal flow of performing the task;
2. Some of the methods are physically uncomfortable for the user;
3. Some methods cannot be conducted in real-time as they are too intensive;
4. The data quality is potentially unreliable outside laboratory conditions; and
5. The data quality can be affected by outside factors, such as a user’s stress level.

FIG. 12 depicts system components for a cognitive load manager that addresses many of these issues. In one embodiment, mobile, wearable, implantable, consumed, and other physiologically integrated computers employ increasingly sophisticated and varied sensors, data input methods, data access methods, and processing capabilities that capture, access, and interpret more and more data that can be used as sensory input to the brain and impact cognitive activity. The data comprises physiological data and environmental data. The data are used to better establish a user’s preferences for the integration, management, and delivery of information to the head mounted unit.

FIGS. 13-15 depict three different system architectures for connecting the HMD to another device or to the Internet. FIG. 13 depicts the HMD 600 connecting through a local link, such as Bluetooth, to a mobile device 710 carried by the user; the mobile device 710 is connected via link 155 to a packet switched network typically provided by a wireless carrier through 700 or what today is generally referred to as a packet network also known as the world wide web; with subsequent connection to either a web-based service, a database, or external application.

FIG. 14 depicts the HMD 600 including a wireless transmitter 750 that is either embedded or attached to the HMD for connection directly to the internet 700 and a service provider.

FIG. 15 depicts the HMD 600 including a wireless transceiver 750 connected via a link 725 directly to the Internet, where the local link is generally a packet link, but could be other proprietary wireless protocols. In this configuration, the HMD is independent from other smart devices; essentially the HMD is connected directly to the Internet all of the time. Today, if a user wants to connect a smart device, or now a HMD, to another system for the control and operation of that system, the user would simply implement a local connection through a Bluetooth profile. In the case of home audio the user would need to use Audio Video Transport Profile, Audio Video Resource Control profile, or Advanced Audio Distribution Profile. If a user wanted to connect to a vehicle, he or she would need to implement the Hands Free Profile. Simpler and less complex systems are needed along with methods to connect to these systems, especially if the user is beyond the range of a local connection to the system they want to control.

To solve this new challenge, FIG. 16 depicts another embodiment where an HMD is implemented in an “abstracted” real-time server-browser cloud based architecture; known today as the “Internet of Things” or IoT. The key to any abstracted layer is the ability to abstract away from some device or software operational or strategic complexity; these could include proprietary aspects, including trade secrets and intellectual property. The abstraction can support extended or new business models to a technology supplier. A good example of this architecture is the NEST™ Labs business model. This model could be loosely referred to as a “razor/razor blade” model; in this case the NEST™ thermostat is the razor, the NEST™ Services are the razor blades or simply stated the business model includes the sale of the thermostat and a monthly recurring service. In addition to the sale of hardware and services, this business model supports data harvesting of a user in his home. In this system, the thermostat serves data off to a centralized server for the purposes of “learning.”

Even though NEST™ products can be accessed via the Internet, they cannot be directly connected to by a smart device for the control and operation of a home heating system. FIG. 16 depicts an HMD 600 connected via a packet network 155 to the Internet 700. In order for the user to access his or her home thermostat, the user needs to access their page on the NEST™ Services server. However, the traditional role of web server and browser has been expanded under the new HTML 5 standard. There has been what looks like a role reversal of the server and browser, one where the web server is now the smart thermostat; this server is simply serving small amounts of data to a fixed URL in the cloud running a browser. This browser in the cloud can be accessed by a user using a smart device or computer from virtually anywhere to read or interact with their thermostat. Using the web server in this role is now a key and underlying concept of the IoT, one where complexity and cost are greatly reduced.

Now re-thinking FIG. 15, in view of the IoT; access to home entertainment, home security systems, or for that matter any home appliance (washers, dryers, refrigerators, etc.) for their monitoring, control, and operation will implement differently. Further, considering the IoT architecture, the head-mounted device 600 could be connected to any consumer, industrial, or commercial device located anywhere in the world on the cloud, a user could control that device via eye interaction with the included display via eye signals defined as a standardized command set mapping the eye signals to communication, diagnostics, control, and interaction with the device(s).

This new model abstracts away complexity and cost, as an example, a model where the HMD may not require Bluetooth or, for that matter, a distributed intelligence. It is inevitable two things will happen in the near future: first, the HMD may continue to grow exponentially with gigabit service on the horizon; and second, the IoT architecture will deploy as it continues to deploy today; very rapidly. What are needed are methods and systems disclosed on how a standalone head mounted system will strategically evolve within a rapidly evolving ecosystem. FIGS. 17-23 depict an abstraction transition model from a smart head mounted system, to a much simpler model as depicted in FIG. 23.

Starting with the end of the transition first, FIG. 23 depicts a cloud based implementation within an IoT architecture of an HMD 600 connected by a very high speed packet based link, a wireless link that would rival or potentially outperform the typical communication bus in a local processor. These processor busses operate as subsystems of the processor to facilitate transfer of data between computer components or between computers. Typical bus types include front-side bus (FSB), which carries data between the CPU and memory controller hub; direct media interface (DMI), which is a point-to-point interconnection between an integrated memory controller and an I/O controller hub in the processor; and Quick Path Interconnect (QPI), which is a
point-to-point interconnect between the CPU and the integrated memory controller. Other high speed busses have been used in the embedded computing industry to include SPI for inter-processor communication. What is not currently anticipated is that under cloud based architectures and distributed computing, much of the intelligence will reside outside of the connected devices. HTML 5 and JSON are good examples of markup languages optimized for distributed computing. To include audio, video, and scalable vector graphics, operating systems will evolve and operate to meet these new distributed architectures likely using much simpler “publish-subscribe” access.

With the above in view, and with respect now to the HMD operating on the cloud, the HMD is connected to a centralized server-browser 800 that operates the Visual Disambiguation Service (VDS) interface termed IRIS (Interface for Real-time Image Services); think of this operating much like SIRI (Speech Interpretation and Recognition Interface) does for audio. The IRIS service is for the complex disambiguation of eye movement for the real-time interpretation, determination, and prediction of a user’s intent. IRIS, like SIRI, operates in the cloud. 1126 and 1127 represent the IRIS abstraction layer discussed above. The HMD now operates with a minimum amount of software, a processor richer in features and configured with a limited or possibly no operating system using a publish/subscribe messaging scheme.

At the beginning of the transition, the embedded IRIS (e-IRIS) 1111 includes a number of tools or utilities operating in the FOG as a combined real-time service. These include a data manager 1125, device manager 1120, communication manager 1130, power manager 1140, and security manager 1135a. In the e-IRIS abstraction 1127, there are counterpart managers, with a slight exception in the security manager 1135b; this will be discussed below in more detail.

Fig. 23 also depicts the eye management tools centralized in a cloud-based version in support of a user. These include an eye tracker 1100, eye data 1105 in support of security, eye control 1110, eye signals 1115, and IUI 1116 for an eye user interface. In addition to these elements, other real-time services are available and associated to IRIS including an Audio-Video manager 1150, speech manager 1155, cognitive load manager 1160 and a context manager 1165. The combination of these services and architecture constitutes IRIS.

Back now to Fig. 17 and an initial embodiment. The HMD 600 is wirelessly connected to a smart device (such as a smart phone, a tablet, home or office PC) or simply to the Internet through an 802.11 link. All of the services operate in the HMD 600 processor or are stored in a memory associated with the HMD 600. This embodiment would operate as a stand-alone computer, with an operating system, and microprocessor(s) and/or other logic elements. In a first transition step of the first embodiment, some of the non-real-time applications are off loaded to applications run on the local smart phone 710, local PC, or other smart devices. However, this first transition embodiment would still be highly dependent on the locally available resources in the HMD 600 to operate as intended.

Fig. 18 depicts a second transition step wherein the data manager 1125 takes on a new role. In addition to managing data on and off the HMD 600, the data manager is configured to manage some of the data either on or off board the HMD 600 using a markup language, such as or JSON (Java Script Object Notation), HTML 4.01, or 5.0. The object of this transition step is to implement a web server-browser relationship in the HMD 600. In this case, some of the data acquired by the imagers, audio input, or any other sensors available to the HMD 600 are served to the cloud and directed by a fixed URL to a cloud based IRIS, where a user’s browser page resides and his/her data are aggregated. This second transition supports non real-time data applications, as an example the HMD 600 is used for the transmission of data that have been collected and stored by a user. As an example, the user may capture a photograph, an audio clip, a video clip, or other user physiological data related to the eye or a user’s health; these data are then transferred to IRIS for storage, aggregation, or possible subsequent dissemination (discussed in more detail below).

Figs. 19, 20, and 21 depict a third step in the transition, where the wireless bandwidth is now near real-time. A web server and browser relationship exists operationally in parallel with a now more mature e-IRIS 1111 in the HMD 600 and IRIS 800 in the cloud. They operate and interact with each other in near real-time across the abstraction layer 1126 and 1127. This new configuration now allows an evolution of the security manager with respect to security and implementation of the private key-public key. The security manager 1135 resident in the HMD 600 takes on the role of generating a private key and public key based on certain bio-metrics as disclosed in described in Systems and Methods for Discerning Eye Signals and Continuous Biometric Identification, filed May 8, 2015. Data collected from the face, eye, or voice constitute unique biometric data of the user or user groups if desired. These data collected can be used to generate a unique private key in a system of public key and private key cryptography.

As background, cryptographic systems have been widely used for information protection, authentication, and access control for many years. These cryptosystems are generally categorized as symmetric key cryptosystems and public key cryptosystems. Symmetric key cryptosystems use the same key for encrypting and decrypting secret information; however using the same key can be problematic: 1) if the key is compromised, security cannot be assured; and 2) if there are multiple users, multiple keys are needed, which may increase system costs and data security. Public key cryptosystems can overcome these limitations by using a pair of cryptographic keys (i.e., a private key and a public key). The private key used for decryption is kept secret, whereas the public key used for encryption may be distributed to multiple users. Therefore, secrecy of the private key is a major challenge when it comes to achieving high levels of security in practical crypto systems.

As one example, the irisCode of the user possibly combined with other biometric data are used to establish a unique key that subsequently generates the private key-public key. The public key generated from the user’s unique biometric aspects is sent to IRIS 800 for storage in the security manager portion of the user’s browser, Fig. 22 1135b. The private key is never stored, but is generated in the HMD 600 every time a user instantiates a session. When the user dows the HMD 600, the private key is generated, Fig. 21 1129, and authenticated in IRIS 800. This ensures levels of non-repudiation and security currently not available in web applications, especially in e-commerce.

Fig. 23 depicts the final step in the transition to a real-time HMD 600. The Internet is now prolific and operates at speeds in excess of processor busses. IRIS 800 is cloud-
based and real-time for all intents and purposes. Data are collected and aggregated in IRIS 800. IRIS 800 is now implementing advanced algorithms based on learning about the physiology of the human eye, as well as the user generally; disambiguation in IRIS 800 is enhanced to the point. IRIS 800 can now predict what and where a user wants to see or do. The user’s HMD 600 is commodity, low cost, low power and immediately replaceable.

[0210] The final step abstracts all of the intelligence for the device to the cloud 700. CBID, now cloud 700 based, is substantially continuous and real-time. Since the generation of the private key is unique to a user, this allows any user to pick up any HMD 600 and use it at any time; simply slip it on and they are looking at their browser page where all of their personal information now resides. If their HMD 600 is stolen, the information is secure. If a user loses their HMD 600, no worry, simply borrow one, or buy a new one. The CBID and cloud 700 aspects of IRIS 800, abstract the device at a new level; it abstracts the user like HMI and displays do today.

[0211] As discussed above in the NEST™ home thermostat model, the thermostat is only accessible through the NEST™ Services portal and page. In this implementation, the HMD 600 is securely connected to IRIS 800 and a user’s page. If the user wants to access their thermostat, IRIS connects them directly and securely to the NEST™ Services portal 965. This model will extend to XFINITY, if a user wanted access to his/her account to set a recording, or have access to an XFINITY service, IRIS will connect them directly to the XFINITY portal 970. Further, if the user wants access to their COZY-HOME application, again, the link is securely made to the appropriate server in this case 975.

[0212] As discussed above, IRIS 800 may be linked to a user’s social media account, giving the user a real-time access. FIG. 25 depicts how IRIS 800 would securely connect a user securely to their Google+ account to see postings or to post in near real-time information they want to share. Social Media 920 comprises social media services available to a user.

[0213] Shifting now to real-time cloud based IRIS 800 and its extended capabilities, eye signals will be substantially continually aggregated and analyzed for its users. This makes IRIS 800 a unique service and development platform for applications and services associated with contextualized eye data (CED). IRIS 800 includes a context manager 1165 in both e-IRIS 1111 in FIG. 17, as well as IRIS 800 FIG. 23 and its role to generated Contextualized Eye Data (CED). CED begins with eye data extracted from episodic and/or substantially continuous monitoring of one or both eyes. These eye data include eye movements such as: saccades, fixations, dwells, pursuits, drift, tremors, and micro-saccades. Eye data also include blinks and winks, squints, pupil dilation, blood vessel patterns, iris and pupil size, feature locations, internal eye-structure size, shape, and location. A key aspect for CED is to use this data to detect behavior changes over time.

[0214] CED is the correlation of eye-data with other classes of data over time to extract relationships for meaningful prediction, measurement, analysis, interpretation, and impact on the user. As an example, three classes of data IRIS 800 will have aggregated are raw data, semantic data, and evoked data.

[0215] Raw data comprises data captured by any sensor, whether in the HMD 600 or present on or in a person. Today, there are many new wearable sensors uses in sports or health where these new systems all have wireless capability. IRIS 800 can take this raw data from an individual and correlate it with eye data. Examples include, but are not limited to, sensors that capture: movement, GSR (galvanic skin response), temperature, heart rate and heart rate variability (HRV), EOG (Electro-oculogram), EEG (Electro-encephalogram), EKG (electro-cardiogram), temperature, facial muscle movement and skin movement, internal organ or biological systems status and performance, scent, audio, scene and images for a range of electromagnetic radiation (visible light, IR, UV, and other electromagnetic frequencies), location (GPS and other beacon sensors), time monitoring/tracking, and more.

[0216] Semantic data comprises the interpretation or meaning of "what, when, where, and how" a user is "doing" something, as well as with whom the user is doing something. "Doing" can be working, playing, eating, exercising, reading, and myriad other activities. These data are constructed by interpreting sensor data in the context of a user’s activities.

[0217] Evoked data are extracted from conscious or subconscious individual response to visual, tactile, olfactory, taste, audio, brain, or other sensory, organ, or biological responses to intentional stimuli.

[0218] To date, the capture of data associated with “eye-tracking” has been primarily enabled with expensive, stationary, “remote” eye-tracking devices, situated in front of displays oriented towards users eyes, for limited durations (measured in minutes) for specific tests; or expensive, dedicated purpose, wearable eye-tracking devices, sometimes packaged as glasses, placed on users for limited durations, or limited controlled environments, for specific tests.

[0219] Eye-tracking data have primarily been captured indoors due to the technology’s inability to function well in high-infrared (outdoor) environments without substantial filtering or shielding of ambient IR light, further reducing the practicality, breadth, and quantity of eye-data capture. As such, high quality, environmentally diverse, high-volume data across diverse “natural” use cases have been limited due to the expense, limited portability, constrained form-factor, high-power requirements, high-computing requirements, limited environmental robustness, and dedicated “data capture” utility of eye-tracking technology and devices. While early research on the data captured has shown promise for extraordinary insights into human health, cognition, and behavior, the general capture of such data has been highly constrained to specific tests and environments for short durations.

[0220] The first generation of IRIS integrated HMDs may be worn by millions of people in a broad range of life activities. In the disclosed transition plan, these data may be collected by IRIS first as historical data, then in both near real-time, and ultimately in real-time. Should this transition occur, it could increase by orders of magnitude the quantity, quality, and contextualization of eye data that is captured. IRIS could then use the ability to correlate data with a broad range of other personal and aggregated data such as individual and group health cognition and behavior. IRIS may then use the aggregated data to provide insights into eye data correlated with personal health, cognition, and behavior as a starting point regarding self-quantification, self-improvement, and self-actualization.

[0221] IRIS will support applications for extracting patterns from large datasets that will expose and predict future behavior such as that of our likelihood to adopt a new habit, our interest in acquiring a product, or our likelihood in voting for a new politician. As an example, below lists the types of
measurements and predictions that will be afforded by IRIS’ contextualized eye-data; these include but are not limited to:

**[0222] MEASUREMENTS**

- [0223] Measuring drowsiness and fatigue
- [0224] Measuring medical conditions and trends
- [0225] Measuring reaction to a drugs, food, or other comestibles
- [0226] Measuring short, medium, and long term health trends
- [0227] Measuring reading speed, focus, interest, fluency, vocabulary, areas of confusion
- [0228] Measuring knowledge, understanding, and skills
- [0229] Measuring emotional state and reactions to stimuli
- [0230] Measuring interest and emotional reaction to people, places, and things
- [0231] Measuring recognition and familiarity with people, places, and things
- [0232] Measuring focus and cognitive load
- [0233] Measuring improvement in performance of specific and general tasks
- [0234] Measuring effectiveness and satisfaction with IRIS

**[0235] PREDICTION**

- [0236] Predicting the onset of a medical condition or disease
- [0237] Predicting the incidence of a specific health event such as a seizure or panic attack
- [0238] Predicting weight gain or loss
- [0239] Predicting the general improvement of health
- [0240] Predicting the likelihood of adopting a new behavior or a bad habit
- [0241] Predicting the likelihood of succeeding at a task or endeavor
- [0242] Predicting an automobile accident
- [0243] Predicting the rate of improvement of an athletic skill
- [0244] Predicting the market success of a new product
- [0245] Predicting the rise or fall of a specific stock or the stock market
- [0246] Predicting a political outcome, political stability, and political unrest
- [0247] Impacting learning, work, play, understanding, socialization, creativity, energy, focus, attitude, motivation, and all things that make us human today, and that will drive the enhancement and evolution of humanity and our species.

**[0248]** The IRIS application and tools positively impact the user of the HMD by contextualizing the eye data that are aggregated. IRIS technology will advance the user’s performance in many dimensions and will enhance the human-to-human interactions as well as their human-machine interactions.

**[0249] The key common aspect to any of these is IRIS’ role as a real-time secure abstraction. Figs. 26-28 depict other portals for secure access to a user’s information where again, the common element is IRIS 800. Further, the private key stored in IRIS can be related to a password for the user that greatly simplifies the user’s interaction on the web, to include secure transactions.**

**[0250] In accordance with other embodiments; systems and methods are provided to enhance security and convenience during online shopping. Fig. 29 depicts a user operating a setup process that needs to occur only once where the user needs to link their public key with account information. For increased security, a bank or other financial institution that is responsible for the account might verify other forms of target (i.e., intended) user identity and offer the linkage process as a service. Once linked, online purchase selections and transactions can be performed by a user with their HMD in a seemingly instantaneous fashion.**

**[0251] In another embodiment of secure shopping, real time knowledge of a device-wearer’s identity allows financial particulars to be exchanged electronically with each item as selected and purchased. This eliminates the need to repeatedly enter passwords, security questions or account information for each transaction or group of transactions. As a consequence, such an instantaneous purchasing system eliminates processes involved with a so-called online shopping “cart” since there is no longer a need to cluster items for the purpose of entering account information. Solely for customer convenience, groups of items purchased during an online shopping session can be treated as a cluster or summarized for the purchaser.**

**[0252] In accordance with another embodiment, systems and methods are provided to enhance security and streamline shopping at so-called “bricks and mortar” retail outlets. In this case, a camera mounted on the headwear device that views the environment of the device wearer can be used to identify objects that may be of interest for purchase. Identification can be based on bar codes or quick-response (i.e., Q-R) codes that are commonly attached to purchasable items. Such object identification uses image processing methods that are well known in the art.**

**[0253] Information about the item including a proposed purchase price can be generated by a processing unit associated with the retail outlet. This information can then be displayed on nearby monitors or on a head-mounted display associated with the device wearer. If the customer wishes to purchase a given item, a CBID-based transaction can be initiated by the customer. Such transactions can occur repeatedly throughout a store. A match between transported items and the transaction record would then allow items to be verifiably removed from the store by the customer. CBID-based retail purchases eliminate the need for check stands or till. In many situations, the automated, real time display of information during the purchasing process reduces the need for store clerks to assist potential customers.**

**[0254] These devices are also integrating increasingly sophisticated and varied data output methods that stimulate visual, auditory, tactile, olfactory, gustatory (sense of taste), equilibrioception (sense of balance), direct neurological, indirect (wireless) neurological (neural and synaptic brainwave stimulation), chemical, biological activity, and multimodal input sensation.**

**[0255] The increased stimulation of the body and associated enhanced delivery of information to the brain can affect brain activity in subtle and profound ways. Cognitive stimulation resulting from more, varied, and faster delivery of multiple forms of input to the brain can positively impact human performance. However, cognitive overload or inappropriate stimulation, can negatively impact performance, damage health, create safety hazards, and even kill.**

**[0256] As mobile, wearable, implanted, consumed, and other physiologically integrated computers proliferate, a solution is needed to manage stimulation and flow of data to the body and brain. Individuals are already applying various...**
forms of cognitive management in technologically stimulated situations. Some methods are purely manual, while methods for intelligent, software-based management are beginning to emerge. For example, reducing audio stimulation during periods of increased, high-impact cognitive activity is commonplace. Consider a driver of an automobile turning down the radio when driving stress increases in challenging traffic or when a driver is lost and is trying to navigate. The attention directed to listening, consciously or subconsciously, provided by the audio stimulus of the radio, reduces input to other areas of the brain, such as visual processing. Simultaneous multi-modalities, such as talking on a cell phone, impact the visual task of driving.

[0257] Reducing physical exertion during periods of higher cognitive load is another form of self-management that is commonplace. Research on “walking while talking” (WWT) shows a correlation between gait pace and rate as walkers talk. In general, walkers that become engaged in conversations requiring higher cognition typically slow their walking pace.

[0258] A recent form of cognitive load management associated with electronic stimulation includes applications that temporarily disable email, text, and other online forms of interruption. These applications are very simple in form, however.

[0259] This approach allows user’s customization and prioritization to improve over time as historical context, performance, biometric, and other data are accumulated and analyzed forming generally a user profile of activities and preferences. These also provide a variety of methods and techniques for dynamically managing stimuli (deferral, termination, sequencing, reprioritization, pacing, and more), support stimuli aggregation and management across multiple individuals for risk-controlled or performance-enhanced group activity.

[0260] Another embodiment is context-aware computing as 1165. In a mobile computing paradigm it will be advantageous for applications to discover and take advantage of contextual information such as user location, time of day, neighboring users and devices, user activity to specifically support collecting and disseminating context and applications that adapt to changing context.

[0261] For the sake of convenience, the operations are described as various interconnected functional blocks or distinct software modules. This is not necessary, however, and there may be cases where these functional blocks or modules are equivalently aggregated into a single logic device, program or operation with unclear boundaries. In any event, the functional blocks and software modules or described features can be implemented by themselves, or in combination with other operations in either hardware or software.

[0262] Having described and illustrated the principles of the present invention in embodiments thereof, it should be apparent that the present invention may be modified in arrangement and detail without departing from such principles. Claim is made to all modifications and variation coming within the scope of the following claims.

We claim:

1. A system for a dynamically evolving cognitive architecture based on a natural intent eye movement interpreter for real-time image services, comprising:

   one or more processors; and

   at least one structured illumination source, operatively coupled to at least one of the processors and configured to be disposed towards at least a first eye of a user; and

   a first sensor operatively coupled to the one or more processors, wherein the sensor is configured to be disposed towards the at least first eye of the user; and

   a non-transitory computer readable memory having a plurality of executable instructions stored thereon, wherein the instructions, when executed by the one or more processors, cause the one or more processors to process eye signal operations comprising:

   configuring the one or more processors to operate in a first processing mode; and

   receiving from the first sensor a first eye measurement data set representative of a first state of the first eye; and

   processing the received first eye measurement data set, wherein the processing calculates a predicted second state of the first eye, wherein the second state is calculated to occur at one or more of a future date, future time, future interval, future position, future sequence, and future pattern; and

   receiving from the first sensor a second eye measurement data set, wherein processing the second eye measurement data set calculates a second state of the first eye; and

   responsive to calculating the predicted second state of the first eye, sending a first executable instruction to the one or more processors; and

2. The system of claim 1, wherein the eye measurement data comprises at least one of: eye lid data, eye lash data, pupil data, cornea data, retina data, iris data, eye movement data, eye shape data, point of regard data, dwell data, fixation data, saccade data, and illumination data.

3. The system of claim 1, wherein the eye signal operations performed by the processor are at least one of continuously, simultaneously, and periodically.

4. The system of claim 1, wherein the first state of the first eye is a first eye gaze position.

5. The system of claim 1, wherein the eye measurement data includes the detection of at least one glint from the surface of the first eye.

6. The system of claim 5, wherein the glint from the surface of the first eye has been generated from a light source attached to a head mounted device.

7. The system of claim 1, wherein the eye measurement data includes one or more distinctive features of the eye.

8. The system of claim 1, wherein the eye measurement data includes at least one of facial features and iris data.

9. The system of claim 8, wherein the iris data is used as biometric input data for the generation of a public key and a private key, wherein the keys provide identification, authentication, and authorization for a user to access and control at least one of a local device, a wirelessly connected device, and a networked server.
10. The system of claim 1, wherein the system includes a second sensor operatively coupled to one or more processors, wherein the second sensor is disposed in a direction the user is facing.

11. A method for providing for real-time image control using a dynamically evolving cognitive architecture based on a natural intent eye movement interpreter, comprising:

an electronic device comprising:

one or more processors; and

at least one structured illumination device, operatively coupled to at least one of the processors and disposed towards at least a first eye of a user; and

a first sensor operatively coupled to one or more processors, wherein the first sensor is disposed towards the at least first eye of the user; and

a non-transitory computer readable memory having a plurality of executable instructions stored thereon, the instructions, when executed by the one or more processors, cause the one or more processors to perform operations, comprising:

configuring the one or more processors to operate in a first processing mode; and

receiving from the first sensor a first eye measurement data set representative of a first state of the first eye;

and

processing the received first eye measurement data set, wherein the processing calculates a second state of the first eye, wherein the second state is calculated to occur at one or more of a future date, future time, future interval, future position, future sequence, and future pattern; and

responsive to calculating the second state of the first eye, sending a first executable instruction to the one or more processors;

receiving from the first sensor a second eye measurement data set, wherein processing the second eye measurement data set calculates a second state of the first eye; and

responsive to calculating the second state of the first eye, correlating the predicted second state of the first eye with the second state of the first eye; and

responsive to correlating the predicted second state of the first eye and the second state of the first eye, wherein the correlation result determines the first and second eye states are congruent, sending a second executable instruction to the one or more processors.

12. The method of claim 11, wherein the eye measurement data includes at least one of: eye lid data, eye lash data, pupil data, cornea data, retina data, iris data, eye movement data, eye shape data, point of regard data, dwell data, fixation data, saccade data, and illumination data.

13. The method of claim 11, wherein the eye signal operations performed by the processor are at least one of continuously, simultaneously, and periodically.

14. The method of claim 11, wherein the first state of the first eye is a first eye gaze.

15. The method of claim 11, wherein the eye measurement data includes the detection of at least one glint from the surface of the first eye.

16. The method of claim 15, wherein the glint from the surface of the first eye has been generated from a light source attached to a head mounted device.

17. The method of claim 11, wherein the eye measurement data includes one or more distinctive features of the eye.

18. The method of claim 11, wherein the eye measurement data includes at least one of facial features and iris data.

19. The method of claim 11, wherein the iris data is used as biometric data for the generation of a public key and a private key, wherein the keys are for the identification and authentication of the user for access and control of at least one of a local device, a connected device, a wireless device, and a remote server.

20. The method of claim 11, wherein the system includes a second sensor operatively coupled to the one or more processors, wherein the second sensor is disposed in a direction the user is facing.