Augmented Humanity: Data, Privacy and Security

Liam Naughton and Herbert Daly

Abstract Wearable devices have already changed the way in which humans communicate with the digital world. Advances in so called “in-body” devices may further revolutionize the way in which humans learn, play and work. However, new technology brings with it new risks and vulnerabilities. Augmented Human technologies have the potential to help human actors and organizations make better decisions. The data produced must be secured, collated and processed. Unless the integrity of the data is assured these decisions cannot be relied upon. There are also issues related to the privacy of data generated by augmented humans. Sharing and accessing data across multiple jurisdictions presents challenges around consistent application of regulatory frameworks especially regarding data ownership and security.

Keywords Augmented humanity · Privacy · Cyborg · Medical augmentations · Big data · ZigBee · Bluetooth · WIFI · Cyber security · Security

1 Introduction

The term *Augmented Humanity* (AH) is generally credited to former Google CEO Eric Schmidt who used the term in his keynote speech at the IFA (Internationle FunkAusstellung) conference in Berlin in 2010 [12]. Schmidt’s discussion on how recent technological developments were nearing the realm of science fiction inspired him to coin the term. There have been many developments since then and it is perhaps difficult to settle on a definition of what AH really is and where the boundaries lie between AH and augmented reality and virtual reality. Certainly the lines are beginning to become blurred and we are entering a time where augmented

L. Naughton (✉) · H. Daly
School of Mathematics & Computer Science, Wolverhampton Cyber Research Institute (WCRI), University of Wolverhampton, Wolverhampton, UK
e-mail: l.naughton@wlv.ac.uk; herbert.daly@wlv.ac.uk

H. Jahankhani et al. (eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-35746-7_5

reality and physical reality are indistinguishable. Others talk about "man and machine integrated systems" and the idea that AH can enhance human biological capabilities in order to survive and surpass cognitive and physical abilities to achieve the next evolutionary stage. In the business world, one might describe AH as the practise of using artificial intelligence (AI) to gain competitive advantage or indeed one may frame AH as the answer to how AI and human intelligence (HI) can add value to each other. Recently, Augmented Humanity has been defined as "what happens when humans work in harmony with technology and machine intelligence to expand and enrich life, helping us to experience more and in deeper ways, to make better decisions and to fulfill our potential as humans" [15].

For the twenty-first century AH involves augmenting humans with devices which can collect data from the individual and from the individuals environment and transmit this data to an external device or service. Depending on the device this data may be intensely private to the individual but it may also be data which the individual wishes to share with external actors such as medical professionals. The data may include aspects which are personal or private to other actors in the users environment e.g. photographs. In any case there are privacy and security issues which must be addressed around AH data.

2 Augmented Humanity: Cyborgs

At this point it is helpful to discuss the fundamental role of data in the study and creation of Augmented Humanity as distinct from earlier ideas such as the Cybernetic Organism or Cyborg. The field of Cybernetics was proposed by Weiner [37], succinctly describing it as "the scientific study of control and communication in the animal and the machine". This wide ranging movement gave birth to many significant concepts in the study of the relationship between people and technology and is documented by Principia Cybernetica Web [24]. A Cyborg may be described as "an organism which is part animal and part machine" or focusing on utility "an organism with a machine built into it with consequent modification of function" [24]. Automatic and adaptive behaviour is achieved through autopoiesis or feedback response mechanisms.

Clarke [8] describes in details some differing kinds of Cyborg construction or intervention and distinguishes between the Prosthetic and the Orthotic. The prosthetic "provides the human body with previously missing functionality or overcomes defective functionality" while the orthotic "supplements or extends a humans capabilities" [8]. These definitions cover a broad range of uses the of technology for example they include users of artificial limbs (Prosthetic) and users of binoculars (Orthotic) as Cyborgs. Helpfully Clarke [8] also classifies Endo, Exo and External in each case where these are within the body, joined to the extremities of the body, or unconnected to the body respectively.

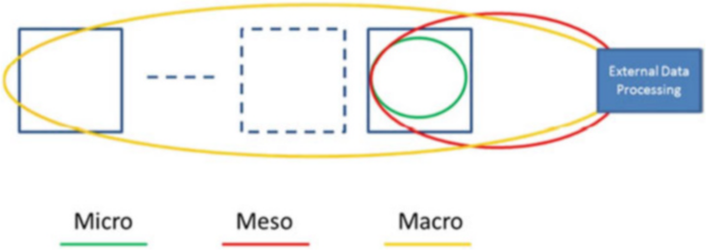


Fig. 1 Feedback response

Classification	Description
Endo-Prosthetic	Supporting capabilities integral to the body e.g. cardio pacemaker
Exo-Prosthetic	Supporting capabilities at the body extremities e.g. artificial limb
External- Prosthetic	Supporting capabilities external to the body e.g. walking stick
Endo-Orthotic	Extending capabilities integral to the body e.g. [36]
Exo-Orthotic	Extending capabilities at the body extremities e.g. smart contact lenses
External-Orthotic	Extension of capabilities external to the body e.g. Infrared goggles

A Cyborg then is, organic but at least in part a constructed artifact using technology to support or extend its natural capabilities through feedback response mechanisms (autopoiesis). In the simplest cases the mechanisms may be purely mechanical (springs responding to pressure) or purely organic (a decision made by the user based on observation). For our discussion in this chapter the Augmented Human is a distinctly data centric form of Cyborg with advanced capabilities for processing and sharing data.

An Augmented Human may display any of features classified above and various examples are discussed. Of the six classifications Endo-Orthotic examples are currently the hardest to find. Endo-Orthotic interventions challenge medical ethics, by using technology internally to enhance performance of an otherwise healthy person is considered questionable by many. Warwick [36] details an experimental intervention where an electrode array was interfaced surgically with the nervous systems of a consenting participant. The subject was then able to use the implant to collect data and operate devices remotely (Fig. 1).

External-Prosthetic and External-Orthotic are examples of using technology for help or support. For the Augmented Human however these devices may be used to communicate directly with Exo or Endo devices and so enhance their overall performance.

While some artifacts are wholly abstract, created from data, and others are wholly material; an Augmented Human has both an abstract and a material aspect. The “adaptive behaviour” which Wiener [37] focuses on is achieved through the “control and communication” of abstract data within the subject and in connection with its material being.

Moreover the Augmented Human (AH) is potentially capable of achieving autopoiesis at different levels including external layers of processing. The external processing may be Prosthetic or Orthotic depending on the analysis or services provided. For example external systems may be used to monitor and respond to long term health data collected about an individual. They may in turn integrate data about a group of users providing collective insights. They may also be used to provide services or extensions to existing capabilities e.g. remote payments. However we may view these as different levels of feedback response Micro, Meso and Macro enabling longer term more strategic behaviour, or service provision, with respect to the environment.

Feedback level	Description
Micro-Autopoiesis	Feedback response processed internally supporting reaction to localized data
Meso-Autopoiesis	Feedback response processed externally supporting complex processing of aggregate data for an individual
Macro-Autopoiesis	Feedback response processed externally supporting complex processing of longer term events aggregated across groups

Wu [38] describes a "Cyborg Intelligence" approach using sensory information fusion and machine learning techniques. Their hierarchical conceptual framework (See Fig. 2) describes an inequivalent three layer model for information processing and interaction in both machines and organisms.

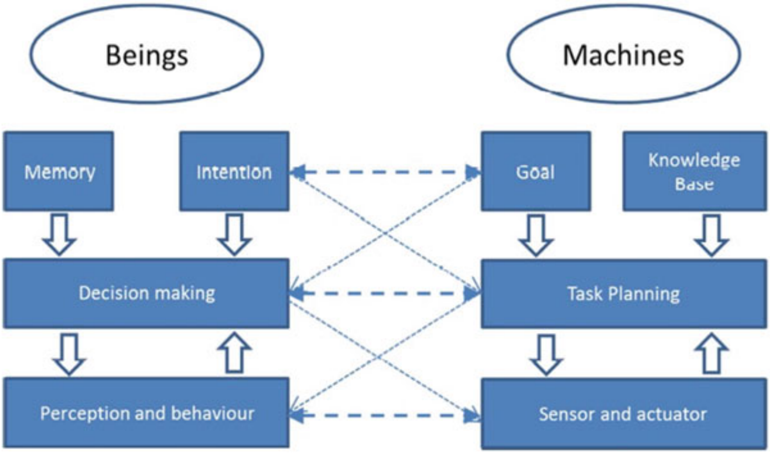


Fig. 2 Hierarchical conceptual framework [38]

3 Developments in Augmented Humanity

Many of the ideas around AH have their origins in the mid-twentieth century when scientists first started to think about the ways in which humans could be “enhanced”. In his seminal work on cybernetics William Ross Ashby [2] wrote about amplifying human intelligence. Ashby suggested that intellectual power may be equivalent to “power of appropriate selection” and he argued that since power of selection could be amplified using artificial means then so too could intellectual power.

At about the same time Licklider [18] envisaged a world where man and computers would be “coupled together very tightly” and he predicted that “the resulting partnership will think as no human brain has ever thought and process data in a way not approached by the information handling machines known today”. Licklider also recognized the role that the computer would play in what he referred to as “man-computer symbiosis”. Together with colleagues at the Defense Advanced Research Agency (DARPA) Licklider laid the foundations for a future where computers could work with humans rather than as tools merely for computation. Licklider’s colleague Douglas Englebert, [10], spoke about “taking a systematic approach to improving the intellectual effectiveness of the individual human being”. He produced a conceptual framework for augmenting human intellect and went on to found the Augmentation Research Center (ARC). ARC developed new tools for information processing and played a major role in the development of the personal computer. A visionary aspect of the work of both Licklider and Engelbert was to see computers as devices which could help humans process data more efficiently. Engelbert described “a way of life in an integrated domain where hunches, cut-and-try, intangibles, and the human feel for a situation usefully co-exist with powerful concepts, streamlined terminology and notation, sophisticated methods, and high-powered electronic aids”. Since the pioneering work of Licklider, Engelbart and others huge advances in human augmentation have been made.

3.1 Medical Augmentations

Much of the stimulus for developing augmentation solutions for humans has come about as a result of efforts to correct deficiencies or injuries. One of the most important devices developed is the cochlear implant. The modern cochlear implant was developed independently in the late seventies by two research teams based in Australia and Austria. The development of the cochlear implant marked the first time that a human sense had substantially been restored using a medical augmentation. A cochlear implant is a surgically implanted neuroprosthetic device which provides a sense of sound to individuals suffering hearing loss. The implant works by sending electric signals directly to the auditory nerve. The implant usually has an internal and an external component. The external component uses a microphone to pick up sound from the local environment. It then filters the sound to prioritize speech. The processed signal is then transmitted to the internal receiver which converts the received signal into impulses which stimulate the cochlear nerve causing it to send signals to the brain. In 2013 the developers of the cochlear implant were honored with the Lasker-DeBakey Clinical Medical research Award [17]. The cochlear implant is just one example of an augmentation which has been developed as a corrective approach to a condition. The technology behind the cochlear implant has stimulated research in other areas including eye prosthetics. One such example is the Retinal Implant project at MIT [39]. This innovation involves placing an array of electrodes behind the retina. The array receives images from a camera and then stimulates the retinal ganglion cells.

Another prominent area for medical human augmentations involves the development of prosthetic limbs. Physical augmentations for amputees now see bone-anchored prosthetics where a titanium prosthesis is directly grafted to the human skeleton eliminating the need for a socket interface [31]. Such biomechanical systems have revolutionized the treatment of amputees. Even more recently we have seen neural augmentations such as the NeuroLife system [4] which uses a brain implant and an electrode sleeve to give paralysis patients back control of their limbs. The general aim of such research has been to develop augmentations that can be controlled by the brain while also providing sensory feedback.

A prolific area of research into human augmentation since the early twentieth century involved the development of cardiac pacemakers. The first implantable pacemaker was developed in the 1950s and the decades since have seen a host of improvements and advances on this technology. The current state of the art for such technology includes the implantable cardioverter defibrillator (ICD), a device implanted in the body which can manipulate the heart rate and even perform emergency defibrillation. The ICD is a life changing augmentation for individuals at risk for sudden cardiac death.

3.2 Augmentation in the Twenty-First Century

Licklider and Engelbart recognized that human intelligence enhancement would enable humans to process information more efficiently. It is only in the very recent past that innovations have been developed which truly subscribe to this vision. We are now seeing a plethora of augmentations which involve on and in body devices which communicate with the individual as well as with outside controllers. For example, Spotify have recently developed a sensor which monitors the users heart rate and then uses an algorithm to choose music to suit the mood of the user. Meanwhile, Google Verily Lenses contain tiny integrated circuits, sensors and wireless communication capabilities for self contained wireless sensing on the surface of the eye. “The team has been working to engineer novel solutions to the technical challenges of significant miniaturization for autonomous sensing systems and dramatic reduction of power consumption to permit tiny batteries” [35]. Samsung have recently (July 2019) secured a patent to develop an augmented reality contact lens [22]. A key feature of this research is that the lens is designed to communicate with an external device e.g. a smartphone. The device “may include an antenna through which information may be transmitted to or from an external device, a capacitor configured to supply power to the display unit and a portion of the peripheral device, a control unit configured to control operations of the display unit and the peripheral device, a motion sensor configured to detect movement of the smart contact lens, and a thin-film camera” [22]. There are already a wide range of real-time in-ear translation systems readily available. Some models such as Google’s Pixelbuds communicate through a smart phone while others such as the WT2 Plus Earbuds work via a cloud based translation service. The WT2 Plus system involves a pair of buds where everything the first user speaks is communicated to the cloud by the users earbud. The translated language is then communicated from the cloud directly to the second user’s earbud using the chosen language of the second user.

Proteus, a digital medicine company, makes smart pills embedded with a sensor which can be tracked by a credit card sized patch worn on the patients stomach. “The sensor can either be stamped into a pill or included alongside a traditional medication and then encased in a translucent shell that breaks down when a patient swallows it. Then, patients attach a credit card-sized adhesive sensor anywhere on their stomach. The sensor tracks when the pill is ingested” [5]. The technology can also be used to see how active patients are by tracking their movements.

A defining characteristic of all of the twenty-first century AH devices described above is that they involve on or in body sensors transmitting data to external services. Whenever data is being transmitted, particularly personal data, there are a wide range of privacy and security considerations that must be taken into consideration.

4 Data from AH

All of the devices described in Sect. 3.2 produce data in one form or another. Some of the data is processed locally e.g. with a smartphone while more of the data is transmitted to the cloud for processing and subsequent analysis with feedback communicated back through the same channels in many cases. To date much of the data from AH devices has concentrated on lifestyle and health benefits. In 2016 it was reported that one in six consumers in the United States were currently using wearable technology, including smart-watches or fitness bands with the number of wearable fitness devices alone predicted to grow to over 100 million by 2019 [20]. Such devices have the potential to allow users direct access to personal analytics that can “contribute to their health, facilitate preventive care, and aid in the management of ongoing illness” [23]. The graphic in Fig. 3 is taken from [23] and it illustrates just some of the ways in which data is communicated via wearable consumer devices.

“Heart rate can be measured with an oximeter built into a ring, muscle activity with an electromyographic sensor embedded into clothing, stress with an electodermal sensor incorporated into a wristband, and physical activity or sleep patterns

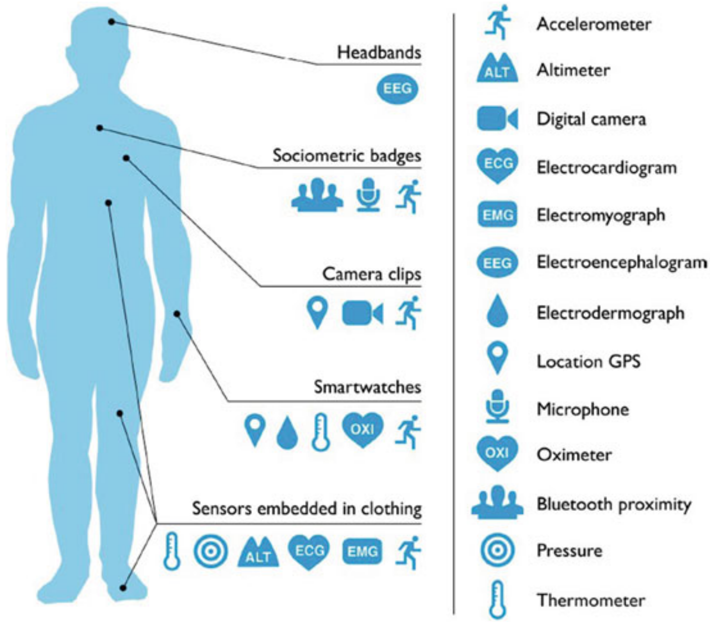


Fig. 3 Data from consumer wearables [23]

via an accelerometer in a watch. In addition, a female's most fertile period can be identified with detailed body temperature tracking, while levels of mental attention can be monitored with a small number of non-gelled electroencephalogram (EEG) electrodes. Levels of social interaction (also known to affect general well-being) can be monitored using proximity detections to others with Bluetooth or Wi-Fi-enabled devices. Consumer wearables can deliver personalized, immediate, and goal-oriented feedback based on specific tracking data obtained via sensors and provide long lasting functionality without requiring continual recharging. Their small form factor makes them easier to wear continuously." [23].

The data gathered from the various sensors and AH devices employed generally needs to be processed in a different ways. Some data processing may occur in the physical environment of the user e.g. via a smartphone or smart-watch, while further processing may take place after the data has been communicated to the cloud. A variety of options are then available for deep analysis and processing. This data will be useful for medical research, for customizing the behaviour of AH devices to match the users individual traits and characteristics e.g. Spotify choosing music based on the user's heart rate. the potential for such data is almost limitless.

"For the data transmission portion of the process, any variety of standard communication protocols may be used including Wi-Fi, Bluetooth, ANT, ZigBee, USB, and 2G, 3G, and 4G. An important recent innovation is Bluetooth low-energy (BTLE) which allows mobile devices to send data more efficiently with much greater battery efficiency than traditional Bluetooth, essentially enabling the regular ongoing if not continuous transmission of relevant data" [29].

The increasing ease of capturing, storing and manipulating data has given rise to a variety of technologies for sharing datasets and visualization tools. In the past, the cost and expertise required for working with large-scale datasets and visualizations generally limited access to institutional professionals, but cost decreases and tool improvements have made data collection and manipulation more available to the individual. One of the most interesting areas for individuals to measure is the self. An underlying assumption for many self-trackers is that data is an objective resource that can bring visibility, information and action to a situation quickly, and psychologically there may be an element of empowerment and control. Quantified self-tracking is being applied to a variety of life areas including time management, travel and social communications. Quantified self-tracking is the regular collection of any data that can be measured about the self such as biological, physical, behavioral or environmental information. Additional aspects may include the graphical display of the data and a feedback loop of introspection and self-experimentation. Health aspects that are not obviously quantitative such as mood can be recorded with qualitative words that can be stored as text or in a tag cloud, mapped to a quantitative scale, or ranked relative to other measures such as yesterdays' rating. Many health self-trackers are recording measurements daily or even more frequently (blood pressure for example) [28]. Furthermore, a number of scientific and popular publications describe methods and techniques for using consumer wearables as "self-hacking devices – to improve sleep, manage stress, or increase productivity [29]".

4.1 Data-Information-Knowledge

The field of Information Science and Knowledge Management has long debated the relationship between Data, Information, Knowledge and Wisdom. Of these wisdom is the most difficult to define and so is often excluded from the discussion. It is clear however that for Augmented Humanity applications to achieve their potential the management of data must support higher levels of insight and services.

Zins [40] explores expert views in the interrelationship between the concepts of Data, Information and Knowledge sometimes described as the "D-I-K model". In the context of the Augmented Human the distinction between the three relates directly to what may be achieved by collecting and transforming sensor data. It is sometimes suggested that the most significant relationship is in the ratio of the value between them as exemplified by Ackoff [1] "An ounce of information is worth a pound of data. An ounce of knowledge is worth a pound of information". The transformation between these categories is the effect of processing.

These maxims suggest essentially that a significant amount of data leads to information, and a significant amount of information leads to some knowledge. Though this view is somewhat superficial it may support the basic understanding of how data produced by Augmented Humans (AH) should be processed and managed. Firstly, key to the development of insight is multi-layered processing and refinement.

Although the terms are sometimes used interchangeably, even informally differences are apparent. A single data point, which some but not all of Zins [40] experts call a datum, allows for little or no inference; it is essentially a symbol. A data stream produced by a sensor can be analysed for its inherent properties, however without a contextual interpretation, such as whether it refers to heart rate, body temperature or blood pressure it is impossible to infer, or learn any useful information about the condition of the source. AH data requires appropriate interpretation frameworks to become information and appropriate analysis to become useful knowledge.

Schmarzo [25] describes the analytical approach for working with large data sets and strategies for identifying useful insights. Though there may be scope to apply such techniques for off-line reporting, the interactive nature for processing data produced by AH applications limits the scope of its effectiveness.

5 Security Issues with AH

The lessons of the recent past suggest that there are many security and privacy issues surrounding AH devices. One area which has gained much attention following the Facebook-Cambridge Analytica (see [6]) scandal is the ability of devices and their vendors to harvest vast quantities of personalized data without the consent of the user. In the Facebook-Cambridge Analytica case the data was used for political advertising purposes in an effort to manipulate the outcomes of elections. Users personal data was collected via their personalized Facebook accounts and became a target for external agencies. The legal gray areas around ownership of such data across jurisdictions also contributes to the problem. In the case of AH devices users are faced with the immediate problem of data ownership. After the data has been collected and communicated to the cloud it often becomes the property of the device manufacturer. While the user may own the device they may not have ownership of the data it records. Depending on the terms and conditions the user has agreed to, however unwittingly that may be, manufacturers may have permission to sell a users a data to third parties. This data may include highly personal data such as gender, weight, and GPS data.

On the other hand, it may be desirable for the user to share the data collected by one or more AH devices particularly if the devices form part of a personalized healthcare monitoring plan. There are many scenarios where it will be beneficial to the user for their data to be included in research studies and for this reason a security and privacy framework is necessary. It is not enough to simply anonymize user data since there are highly sophisticated algorithms available which are capable of identifying a user based on their digital behaviour. In fact the Facebook-Cambridge Analytica scandal described a scenario where a profile of each of two million users was created with "hundreds of data points per person" [14]. Combining similar algorithms with the data generated from AH devices will produce a digital fingerprint of each user which can be used to identify them. Perhaps even more alarmingly “Research on “digital traces” from other sources (e.g., social media) demonstrates that these can be alarmingly accurate when it comes to predicting personality and risk-taking behaviors, two very individual and personal traits” [23].

Another area of concern is the potential for direct attacks against individual AH devices. In 2008 modern implantable defibrillators were shown to be vulnerable to unauthorized communication, potentially harmful device reprogramming, and unauthorized data extraction [19]. The response from the Heart Rhythm Society (US) noted that the devices “were not designed to withstand a terrorist attack (see [13]). Advances in security for medical AH devices have been made since then however the threat of a cuber attack against an individual device cannot be discounted. There are a variety of reasons why a hacker might choose to attack an individual device besides the compromising of user data including damaging the reputation of the manufacturer or financial gain. It is also possible that device security may be compromised accidentally. Malware designed to attack a cloud based system may render an AH device useless either temporarily or permanently. As well as transmitting user data to an external service many AH devices may require occasional software updates. This is another vector which could be capitalized upon by an external hacker. AH devices may also be vulnerable to Denial of Service (Dos) attacks where the devices are flooded with so much communication that they are unable to receive essential communications. AH devices are by their nature low power and that renders them susceptible to attacks which seek to drain the batteries of such devices by repeatedly awakening them from ‘sleep mode’. Depending on the device this could have catastrophic consequences. An attack on a non-essential system such as the cochlear implant may be deemed low risk due to the nature of the augmentation it provides whereas devices including pacemakers which have the ability to sustain life require additional safeguards.

5.1 AH Data and the Regulatory Landscape

From the previous discussion then, clearly, effective storing and processing of data is key to reaping the wider benefits of Augmented Humanity applications. Though it is possible as early systems have demonstrated to process data locally to its collection point this inherently has limits. For example for applications which process visual data; captured images, video, alternative visualization (e.g. infra-red, radioactivity) localized storage and processing will always be a limitation in terms of capacity and cause of systems failure. In certain kinds of systems, upgrades and repairs may be trivial, however those with intrinsic features may only be upgraded rarely or perhaps not at all. Many of the advanced use cases for AH, particularly those related to leisure and commerce, require the exchange of value, or some form of tokenisation. Typically these must be processed, or at least recognized beyond a single unit in order to have validity. Where the aim of augmentation is to overcome environmental issues the data collected is typically of greatest value in understanding the problem as a whole, co-ordinating the collaboration of groups or possibly collecting evidence of a defined quality required for later action. There is also, of course the potential for AH projects to evolve beyond their original brief. Data, once collected has the potential to be used or enriched beyond original conception. As more data sources become publicly available, for example through open linked data initiatives, it may be possible to create services, or studies, based on multiple data sources enriched or combined. (pollution and health?) (Stress at work?) (Disaster and emergency?) Moreover the use of artificial intelligence and machine learning to integrate autonomous systems in these applications presents issues about how data is integrated practically into the decision making process. Additionally a particular feature of the AH data is the potential for issues around privacy. These concerns will shape not only how data could be used, but also how it must not be used or shared in the development of services.

5.2 General Data Protection Regulation

The General Data Protection Regulation [9] is a regulation in European Union (EU) law on data protection for all individual citizens of the (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. GDPR contains provisions and requirements relating to the processing of the personal data of individuals. Generally, if a user wants to use an AH device they have little choice but to agree to the manufacturers terms and conditions and this often gives consent for the manufacturer to collect and process the users personal data. The most relevant clause is GDPR Article 25, Data Protection by Design and by Default. Data protection by design (often ‘privacy by design’) is a concept which is generally attributed to Cavoukian [7]. The principle asserts that “we build privacy directly into the design and operation, not only of technology, but also of operational systems, work processes, management structures, physical spaces and networked infrastructure” [7]. Previously the adoption of data protection by design and default has been voluntary and a matter of good practice. GDPR makes it necessary for each data controller to consider “having regard to the state of the art and the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk”. The elements of GDPR and, particularly, data protection by design and default provides guidance on the amount of data that AH devices can collect and process. However, in such a rapidly changing technological area it is difficult see how the GDPR can be considered ‘future proof’. Nevertheless, it has raised consumer awareness to the extent that users of AH devices are likely to be more aware and cautious about the consequences of consenting to the terms, conditions and privacy policy of manufacturers.

5.3 U.S. Regulatory Frameworks

The regulatory framework in the U.S. is less clear-cut than in the EU. There are various federal acts which may be relevant including the Food, Drug and Cosmetic Act (FD&C) [33] which covers certain medical devices, the Health Insurance Portability and Accountability Act (HIPAA) [32] which gives users rights over some of their information, and the Federal Trade Commission Act (FTC) [34] which is perhaps the most important act with regard to AH devices. The Food and Drug Administration (FDA) does not classify wearable technology as a medical device within the FD&C act, rather it considers them to be low risk general wellness products which are not regulated by the FDA. Apart from specific clearly defined medical devices the FD&C act may not apply to AH devices in general. The HIPAA may provide some limited protection for data collected via AH devices but, as with the FD&C act, there must be a clear medical function to the design of the device or the collection and processing of the data it generates. The FTC act prohibits companies from engaging in deceptive or unfair acts or practices, including failing to comply with an organizations own privacy policy. The act is enforced by the FTC commission which can bring legal action against organizations that have violated consumer privacy rights and/or failed to maintain the security of sensitive data. Nevertheless, the liability, if any, of AH device manufacturers is far from clear under the above acts.

5.4 Cross Jurisdiction Privacy

Clarke [8] discusses at length the issues of Cyborg rights which are, by extension, rights of the augmented human. Privacy as a right however is not significantly explored and in the case of the augmented human this is a unique and significant vulnerability. Smallwood [27] discusses this issues and frameworks around information governance and more broadly Personally Identifiable Information (PII). This would apply in particular to operational data associated with the augmented human such as codes and identifiers related to the exchange of information and may at some points in the data transfer cycle be dealt with using encryption. The key issues presented by encryption are that it is typically a resource intensive process and software may require updating in the event of a security breech.

Ownership of data about oneself is the subject of discussion across jurisdictions. In the case of the AH although they may be protected by some legislation, the question of consent in the automatic generation of data is critical to establishing rights both of ownership and of privacy. For example, if an augmented human produces data that may be used to diagnose a medical condition, a number of questions emerge; Is their data anonymous or does it identify them uniquely? Do they have the right to access, copy or delete the data? Do they have the right to consent or opt out of different kinds of data analysis that may be applied?

As people travel globally and processing infrastructure may be needed locally to provide appropriate services to augmented humans, designers of these must consider the compliance issues for the legal requirements with respect to data privacy in different regions of the world. The table below illustrates only some of the legislation that may need to be taken into account (Table 1).

Table 1 Global legal frameworks relating to PII for AH data adapted from Smallwood [27]

Nation	Region	Privacy legislation
Morocco	Africa	Data Protection Act
South Africa	Africa	Economic Communications and Transactions Act 2002
Australia	Asia/Pacific	Privacy Act 1988
Hong Kong	Asia/Pacific	Personal Data Ordinance
Japan	Asia/Pacific	Personal Information Protection Act 1988
Philippines	Asia/Pacific	Data Privacy Act 2011
European Union	Europe	European Union Data Protection Directive of 1998 and EU Privacy Law 2002 (2002/58/EC)
France	Europe	Data Protection Act 1978 (Revised 2004)
Germany	Europe	Federal Data Protection Act 2001
Ireland	Europe	Data Protection Act 2003
United Kingdom	Europe	UK Data Protection Act 1998
Canada	North America/Central	Privacy Act 1983 and Personal Information Protection and Electronic Data Act (PIPEDA) 2000
Canada	North America/Central	Privacy Act 1983 and Personal Information Protection and Electronic Data Act (PIPEDA) 2000
Mexico	North America/Central	Federal Law for the Protection of Personal Data Possessed by Private Persons
United States of America	North America/Central	Privacy Protection Act 1980 and Video Privacy Protection Act 1988
Argentina	South America	Personal Data Protection Act 2000 (Habeas Data)
Brazil	South America	Article 5 of the 1988 Constitution
Chile	South America	Act on the Protection of Personal Data 1998
Colombia	South America	Law 1266 of 2008 and Law 1273 of 2009

6 Blockchain and Augmented Humanity

6.1 Blockchain Overview

Blockchain was invented in 2008 by a person (or several persons) using the name Satoshi Nakamoto [21] as the public transaction ledger of the cryptocurrency bitcoin. A blockchain is a constantly growing list of transactions which are collected into batches called blocks. Each block contains a cryptographic hash of the previous block. Blockchain is an immutable, distributed ledger that can record transactions between parties in an efficient and verifiable way. The immutable nature of blockchain means that a record cannot be altered retrospectively without altering all subsequent blocks. A transaction is added to the blockchain only after it has been validated via a consensus mechanism (e.g. mining). Blockchain technologies can be categorized into two main types: Public blockchains and Private blockchain. The differences between the two types will now be outlined.

6.1.1 Access & Permissions

Public blockchains are generally permissionless. Anyone can read or write data to the blockchain and their is no predetermined criteria to take part. All transactions are visible to all other participants. Examples of public blockchains include Bitcoin [3] and Ethereum [11]. Private blockchains only allow certain authorized entities to participate. They have the ability to grant specific rights and restrictions to participants on the network. They are considered to be more centralized than public blockchains since only a small group of participants control the network. An example of such a private blockchain is Hyperledger [30].

6.1.2 Consensus

Transaction on public and private blockchains are verified using a consensus based system but there are different ways in which consensus can be reached. With public blockchains consensus mechanisms are often based on an incentive scheme which rewards participants for making some contribution to the network. One of the most widely used consensus schemes, which is used with several cryptocurrencies, is ‘proof-of-work’. In such a scenario ‘miners’ contribute their computing power to solve cryptographic problems to verify transactions and they are rewarded in the form of a token. Proof-of-work is often computationally intensive and expensive in terms of time. This often leads to slow transaction speeds and high electricity costs. Other consensus schemes such as ‘proof-of-stake’, ‘proof-of-capacity’ and ‘proof-of-elapsed-time’ can also be used. In a private blockchain consensus is often reached via ‘selective endorsement’. In this framework only a defined group of entities can verify transactions. An example of such a consensus framework is ‘proof-of-authority’.

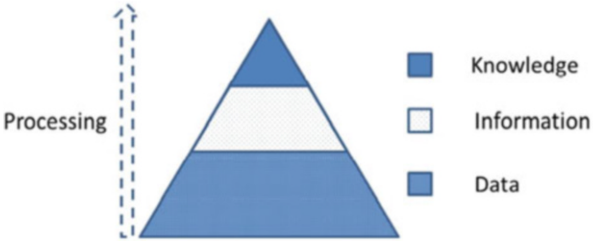
6.2 *Blockchain for AH Data Security and Privacy*

Blockchain technology can be used in any system which involves a database and as such it can provide tools to handle data issues around authentication, security and privatization. The immutable nature of the technology means that once a transaction has been made it cannot be altered or tampered with and this provides security. Modern blockchain technologies now come equipped with robust authentication and identification systems that permit different levels of access to the blockchain. For example, one type of access might allow users to write data to the ledger whereas another type of access might allow other users to act as monitors while still a third type of access might allow a user to administer the transfer of value (coins, tokens etc.) between users. An advantage to such a system is that it keeps different types of users and their access to the data compartmentalized. Such a system of access permissions could be produced for AH data which allowed e.g. users to write data to the blockchain via their AH devices while still allowing e.g. medical research professionals to access the data for research purposes. In the light of recent scandals, such as the Facebook-Cambridge Analytica scandal, consumers are becoming more conscious about the security of their personal data. Trust has disappeared from the process so users need a platform where data can be shared in a secure and tamper-proof way.

6.2.1 Validation

AH data stored in a blockchain is encrypted so that unauthorized data modification is a difficult task. The use of cryptographic signatures (hash functions) means that users can verify that a file has not been tampered with by merely inspecting the signature rather than analysing the entire file. Signatures can be cross checked with others across all of the blocks to verify their integrity. If an unwanted agent (e.g. hacker) changes a record then the signature will be invalid. In this way blockchain facilitates reliable data validation (Fig. 4).

Fig. 4 Processing



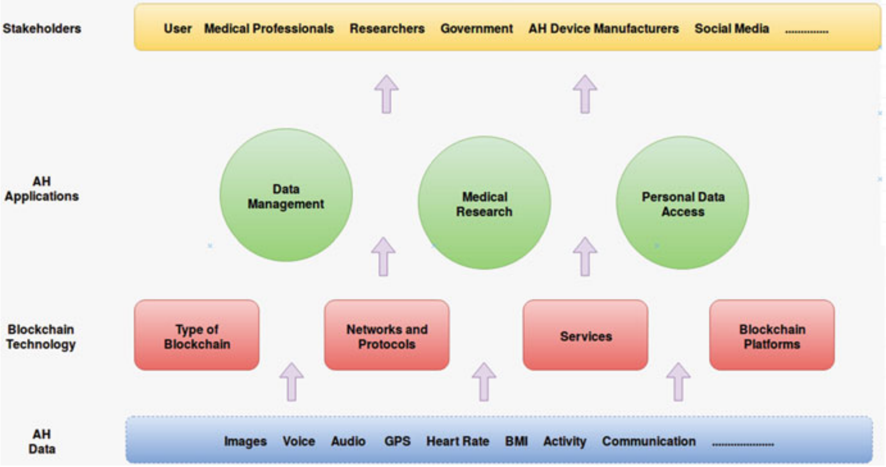


Fig. 5 Workflow of blockchain AH applications

6.2.2 Decentralized Verification

The decentralized nature of blockchain means that it does not rely on any single point of control. Every device on the network has access to a complete copy of the data. The lack of a single gatekeeper makes the system more secure. Consensus is reached across the network in a democratic way to validate transactions and record data. This ensures that the data stored is accurate and trustworthy. For example, the integrity of research carried out using AH data can be trusted since all nodes have access to the data, a difficulty with much current research in fields such as medicine.

6.3 Applications

Figure 5 illustrates a blockchain based workflow for AH applications. The first layer of the diagram consists of the AH data collected by the various AH devices. Given the diverse nature of the devices available this includes GPS data collected by trackers, voice recorded data captured by ear buds, audio data recorded from the user environment, medical data such as heart rate, level of activity as well as communication data transmitted to and from the users' various AH devices. Blockchain technology sits on top of the raw data. In this workflow this layer is divided into four components although there may be others. Each of the platforms has different characteristics and enables users to instigate and manage transactions. Once the chosen technology has been implemented the next step involves integrating this technology with the wider system. In Fig. 5 we have outlined three broad areas for blockchain applications in AH. The first category for AH applications is Data Management. This category involves data storage and organization. This could be the storage of particular type of data e.g. audio, voice, images. The second category is dedicated specifically to medical research. AH includes the Internet of medical things (IoMT) and there is already a well established application for blockchain technology in this area (see e.g. [26]). The legislation and concerns about medical data warrant treating this as a separate class of blockchain application. The third category considers applications which are concerned with allowing users to control access to their own data. At the top of the stack comes the stakeholder layer. This layer consist of all parties who will benefit from the blockchain applications in AH including users, business, researchers as well as government and regulatory bodies.

6.3.1 Internet of Me

In [16] the authors provide a comprehensive review of the use of blockchain technology in healthcare and also suggest directions for future research. One focus of the article (Sect. 5) is the Internet of Medical Things (IoMT). ‘With IoMT “healthcare equipment such as heart monitors, body scanners and wearable devices can gather, process and share data over the internet in real time. For example, with the advancement of AI, healthcare providers, using the IoMT paradigm, can capture an image, identify malignant parts or even suspicious cells, and share such knowledge with those who have the right to access the information” [16]. IoMT is certainly a subset of Internet of things (IoT), but some aspects of AH can also be considered as a subset of IoT. One can characterize these aspects of AH which are a subset of IoT as ‘Internet of Me” (IoMe). For example devices such as cochlear implant and implanted defibrillators can be considered as both situated within IoMT and IoMe. In similar fashion to [16] one can illustrate IoMe within blockchain via the diagram in Fig. 6.

The user is the source of all data in IoMe. The next level consists of the IoMe AH devices which are generally either attached to or implanted in the user. They typically generate a large volume of data. The devices may be directly connected to the Internet or they may be in e.g. bluetooth communication with a local device e.g. smartphone which is itself connected to the internet. The data from this stage is stored in e.g. cloud storage. At the next stage “AI will help blockchain to create intelligent virtual agents, which in turn can create new ledgers automatically. In case of sensitive medical data, where security is the first priority, decentralized AI system could help block chain to reach highest security” [16]. The final stage involves the end users and this can include health professionals, marketing analysts, employers or government organizations.

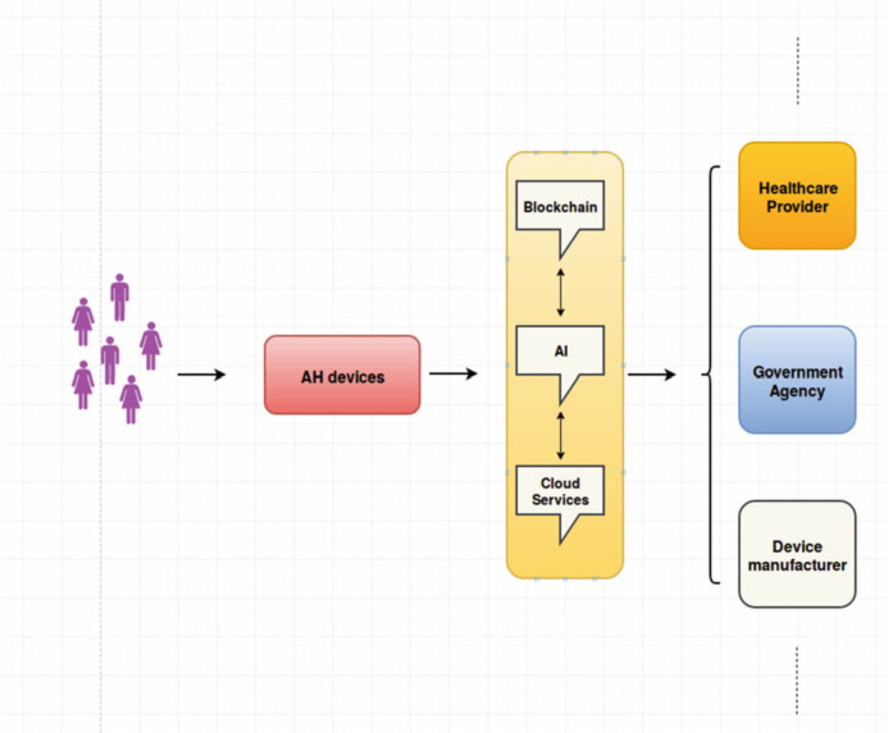


Fig. 6 Data flow in AH

7 Concluding Remarks

There are many concerns around the security and privacy of data generated by AH devices. The rapidly developing nature of the field of AH means that there is also a lack of a clear overarching framework for the regulation of the data landscape concerning AH. Questions around ownership and protection of data still require clear answers. How best to combine the various regulatory frameworks that are available in different jurisdictions is a question that still requires much consideration. Fortunately, there is a body of research beginning in the mid twentieth century with the work of Ashby [2] and others which laid the foundation for the next sixty years of development. The more recent work of Wu [38] and Clarke [8] on Cyborg rights and intelligence provide a starting point for considering how best to approach issues around acceptable treatment of AH data from the user point of view. There are also opportunities, particularly in terms of using AH data for research. Blockchain is one technology which can play a major role. Similar to its applications in IoT and IoMT the applications of blockchain in IoMe will be many. More evaluation of blockchain applications in IoT and IoMT is needed before the potential in IoMe can be fully realised. More work is needed in this area to fully understand the implications and applications of AH data.

References

1. Ackoff RL (1999) Ackoff's best: his classic writings on management. Wiley, New York
2. Ashby WR (1956) An introduction to cybernetics. Wiley, New York. https://www.biodiversitylibrary.org/bibliography/5851
3. bitcoin.org (2019) Bitcoin. https://bitcoin.org/en/. Accessed 18 Aug 2019
4. Bouton CE et al (2016) Restoring cortical control of functional movement in a human with quadriplegia. Nature. https://doi.org/10.1038/nature17435
5. Business Insider (2019) A silicon valley company just launched 'smart' cancer pills that track you with tiny sensors stamped into your medications
6. Cadwalladr C, Graham-Harrison E (2018) Revealed: 50 million Facebook profiles harvested for Cambridge analytica in major data breach. The Guardian
7. Cavoukian A (2010) Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. Identity in the Inf Soc 3(2):247–251
8. Clarke R (2010) Cyborg rights. Proc Int Symp Technol Soc 30:9–22
9. Council of European Union (2014) Council regulation (EU) no 269/2014. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1416170084502&uri=CELEX:32014R0269
10. Engelbart D (1962) Augmenting human intellect: a conceptual framework. AFOSR. Stanford Research Institute, Menlo Park
11. ethereum.org (2019) Ethereum. https://www.ethereum.org/. Accessed 15 Aug 2019
12. Gannes L (2010) Eric schmidt: Welcome to "age of augmented humanity"
13. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, Fu K, Kohno T, Maisel WH (2008) Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In: 2008 IEEE symposium on security and privacy (SP 2008), pp 129–142
14. Hern A (2018) Cambridge analytica: how did it turn clicks into votes? The Guardian
15. Isobar (2019) Augmented humanity, Isobar trends report
16. Khezr S, Moniruzzaman M, Yassine A, Benlamri R (2019) Blockchain technology in healthcare: a comprehensive review and directions for future research. Appl Sci 9:1736
17. Lasker Foundation (2013) 2013 lasker debakey clinical medical research award
18. Licklider JCR (1960) Man-computer symbiosis. IRE Trans Hum Factors Electron 1:4–11
19. Maisel WH, Kohno T (2010) Improving the security and privacy of implantable medical devices. New Engl J Med 362(13):1164–1166. PMID: 20357279
20. Moar J (2018) Juniper research smart wearable devices. Fitness, healthcare, entertainment and enterprise 2013–2018
21. Nakamoto S (2009) Bitcoin: a peer-to-peer electronic cash system. Cryptography Mailing list at https://metzdowd.com
22. Patently Mobile (2019) Samsung wins patent for augmented reality contact lenses
23. Piwek L, Ellis DA, Andrews S, Joinson A (2016) The rise of consumer health wearables: promises and barriers. PLOS Med 13(2):1–9
24. Principia Cybernetica Project (2019) Welcome to principia cybernetica web. http://pespmc1.vub.ac.be/. Accessed: 05 Sep 2019
25. Schmarzo B (2013) Big data: understanding how data powers big business. Wiley, Indianapolis
26. Seliem M, Elgazzar K (2019) BIoMT: blockchain for the internet of medical things
27. Smallwood R (2014) Information governance: concepts, strategies, and best practices. Wiley CIO. Wiley, Hoboken
28. Swan M (2009) Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and quantified self-tracking. Int J Environ Res Public Health 6(2):492–525
29. Swan M (2012) Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. J Sens Actuator Netw 1(3):217–253
30. The Linux Foundation (2019) Hyperledger. https://www.hyperledger.org/. Accessed: 02 Sep 2019

31. Thesleff, Alexander, Brånemark R, Håkansson B, Ortiz-Catalan M (2018) Biomechanical characterisation of bone-anchored implant systems for amputation limb prostheses: a systematic review. Ann Biomed Eng. https://distill.pub/2017/aia
32. United States (2004) The health insurance portability and accountability act (hipaa). Washington, D.C.: U.S. Department of Labor, Employee Benefits Security Administration
33. US Congress (1934) United states code: federal food, drug, and cosmetic act, 21 U.S.C. Retrieved from the Library of Congress,
[Periodical]. https://www.loc.gov/item/uscode1934-006021009/
34. U.S. Government (2018) Federal trade commission act
35. Verily (2019) Smart lens program
36. Warwick K, Gasson M, Hutt B, Goodhew I, Kyberd P, Schulzrinne H, Wu X (2004) Thought communication and control: a first step using radiotelegraphy. IEEE Proc Commun 151:185–189
37. Wiener N (1948) Cybernetics; or control and communication in the animal and the machine. Wiley, New York
38. Wu Z, Zhou Y, Shi Z, Zhang C, Li G, Zheng X, Zheng N, Pan G (2016) Cyborg intelligence: recent progress and future directions. IEEE Intell Syst 31(6):44–50
39. Wyatt Jr J (2011) The retinal implant project. Research Laboratory of Electronics, MIT. http://www.rle.mit.edu/media/pr151/19.pdf
40. Zins C (2007) Conceptual approaches for defining data, information, and knowledge. JASIST 58:479–493