As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 9(05): 912-919, 2023

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0905155
Available online at: http://www.ijmtst.com/vol9issue05.html

An Analysis of the risks of Ambient Intelligence in Modern Systems

Karan Chawla

Ashoka Unviersity

To Cite this Article
Karan Chawla. An Analysis of the risks of Ambient Intelligence in Modern Systems. International Journal for Modern Trends in Science and Technology 2023, 9(05), pp. 912-919. https://doi.org/10.46501/IJMTST0905155

Article Info
Received: 28 April 2023; Accepted: 24 May 2023; Published: 25 May 2023.

ABSTRACT

In sociology, conviviality often refers to a relationship between people and emphasisesvirtues like equality and a sense of belonging to a society. However, when powerchanges between people and groups, social interactions alter: Minority and majoritygroups emerge, outsiders are shut out, and others compel entry. According to Wright'sSafe-guards in a World of Ambient Intelligent project study, there hasn't yet been a sufficiently thorough analysis of AmI research projects in Europe, the United States,and Canada that has a focus on privacy, security, identification, and trust concerns.Nobody has thought about the variety of protections required for people. The negativerepercussions of conviviality highlight these mechanisms, highlight what should beavoided, and highlight the necessity of combining a number of safeguards in order toappropriately safeguard people, communities, and institutions. Ambient intelligence isincreasingly being used in healthcare settings, for example, by monitoring staffadherence to clinical best practices to maintain clinician and patient safety or byrelieving staff of taxing paperwork chores. In order to collect data efficiently andeffectively, ambient intelligence uses contactless sensors and wearables implanted inhealthcare environments, together with machine learning algorithms.This review paper assesses the risks associated with ambient intelligence in the fieldsof Health care as well as in the workplace and examines the risks with respect toconviviality as well.

KEYWORDS:Sociology,Conviviality, Ambient Intelligence, Machine Learning, Health-Care, Computing.

1. INTRODUCTION

In ambient intelligence applications, users annotate physical locations with virtual notes, which are then pushed to or accessed by other users when in the vicinity, as in the mass-scale annotation system GeoNotes. Thus, user groups are created according to area. It would appear that what happens next between these users is what matters. Users are encouraged to share information and work together by creating convivial relationships and places, while being dissuaded from abusing other users. AmI is not a single technology, but a collection of technologies. It brings together developments in computer vision, machine learning, processing, networks, hardware sensors, and natural language processing (NLP), to mention a few. For it to work, it must touch on every facet of computer science. We haven't really seen enough advancements in any one of these areas until the last ten years for AmI to be a viable idea. Zelkha first used the term "ambient intelligence" in 1998 while conducting research for Philips on how to conceptualise the future of computing and technology in the home and how it might be combined from a patchwork of disparate electronic devices into a single extensible and adaptable system. Parallel initiatives started, most notably from the European Commission's Information Society and Technology Advisory Group (ISTAG), which in 2001 published a paper by Ducatel et al. that elaborated on use cases and scenarios. Since Turing's seminal work, significant advancements have been made in computer vision research, such as feature extraction, edge detection, and facial recognition; in machine learning and speech recognition; in the miniaturisation of electronics; in ubiquitous computing; and in networks, particularly broadband and WiFi. That The magnitude of the challenge facing researchers before a coherent idea of AmI was ever formally established is illustrated by the fact that this list only touches the surface of the technological developments required to get us near to developing AmI systems. The term "AmI" describes a system that surrounds a person with intelligent, intuitive interfaces that are seamlessly, unobtrusively, and frequently invisible integrated into objects and the immediate environment and are capable of recognising and responding to the presence of various people. Even if it is questionable whether Amazon's Alexa1 and Google's Home2 gadgets are AmI, they both provide helpful insights into how people utilise this kind of technology and how we would desire to engage with technology that is integrated into our surroundings. The current standard for commercial realisations of this objective is these devices.

2. CONVIVIALITY

The term "ambient intelligence," which refers to a future in which people will be surrounded by intelligent and intuitive interfaces embedded in everyday objects around us and an environment recognising and responding to our presence in an invisible way, was first used by the Information Society Technologies Programme Advisory Group (ISTAG) of the European Union in 1999. Its goal is to make it possible for people to express themselves more clearly, concisely, and effectively by secretly documenting and recording their preferences. Therefore, concepts like privacy, identification, and conviviality must be taken into account by context-aware programmes. The three basic types of black holes are broken down and analysed in this review study, along with the methodology used to determine each black hole's gravitational wave recoil. It makes suggestions for further study and points out gaps, such as the knowledge gap regarding non-stationary black holes and the structure of the primordial globular cluster, where the existing research methodologies and procedures pertaining to gravitational recoil in various black holes would require study. In sociology, conviviality often refers to a relationship between people and places an emphasis on ideals like equality and community involvement. However, when people and organisations' levels of power vary, new minority and majority groups emerge, outsiders are shut out, and others try to get in. Collaborative Capture, another ambient intelligence tool, enables, for instance, "a group of people taking photos at an event to merge their captures and provide a complete collection." Of course, this presents privacy concerns because you might not want to share all of your photos. Traditional security, based on authorizations, is challenging to implement in the setting of impromptu contacts, necessitating the investigation of novel alternatives built on more dynamic ideas like conviviality. The sheer idea of ubiquitous capture might be unsettling since anybody, everywhere having the capacity to engage in capture activities could alter societal dynamics. Concentration must be placed on individuals and their social contexts in a computer environment as a whole. Conviviality may build barriers of protection for and amongst its peers by reinforcing shared ground among the group's members. A computer system that is placed in a particular environment and is able to take autonomous action in this environment in order to achieve its design goals is referred to as an agent in multi-agent systems. Agents are able to exhibit flexible (social, proactive, and reactive) conduct. Since it enables agents to work together, plan their activities together, and bargain with one another, this capacity is very important for ambient intelligence. Applications for ambient intelligence may gain a lot from conviviality's advantages, including knowledge and talent sharing, handling conflict, facilitating inclusivity, and promoting equality and trust among participants. However, before it can be effectively employed as a coordinating mechanism between people, organisations, and institutions and as a tool to strengthen social cohesion, conviviality must first be defined publicly and formalised. It is essential to incorporate the required safeguards against the possible drawbacks of conviviality, such as trickery, group disintegration, and reductionism, into the designs of ambient intelligence applications. For instance, intelligent interfaces enable immediate interactions and hence strongly necessitate coordination and regulatory techniques. To guarantee that people are protected from abuses like privacy invasions and identity theft, these demands must be met.

3. HEALTH-CARE

Ambient intelligence, or the capacity to continually and unobtrusively observe and interpret behaviours in physical settings, has been made possible by concomitant developments in multimodal sensor technology, machine learning, and computer vision. In healthcare settings, ambient intelligence is being used more and more. In order to collect data (such as images of physical spaces, audio, or body temperature), contactless sensors and contact-based wearable devices embedded in healthcare settings are used in ambient intelligence (figure). These devices are combined with machine learning algorithms that effectively and efficiently interpret the data. When used in healthcare settings, this technology may track a patient's health state and course as well as emphasise the standard and type of treatment provided by the whole medical staff. The term "AmI" refers to a system that surrounds a person with intuitive, intelligent interfaces that are integrated into items and the surrounding environment and are capable of recognising and responding to the presence of diverse persons in a seamless, unobtrusive, and frequently undetectable way. Although it is debatable whether Amazon's Alexa1 and Google's Home2 devices meet the criteria for being AmI, they offer both a useful insight into how people adopt this type of technology and how we might want to interact with technology embedded in our environments. These devices serve as the current benchmark for commercial realisations of this goal. Researchers utilise a distinct labelled validation dataset during the training stage to make sure learned models can generalise to unseen data. The validation dataset is used regularly to assess and fine-tune the algorithm during the training phase; it is analogous to online practice tests. The algorithm is assessed against the test dataset after achieving a good score on the validation dataset; this is analogous to the final exam when the algorithm is run on never-before-seen data and its final performance characteristics are provided. Successful training, validation, and testing in the majority of frequently used machine learning implementations (i.e., supervised machine learning) are only achievable with labelled data, and in huge quantities. Deployment in the intended healthcare environment is the next step in the procedure. The algorithm, which may be used to give direct interventions for quality improvement or to support physicians in making decisions, typically evaluates the sensory data only when it is implemented. Although machine learning algorithms that can receive feedback loops from the experts (i.e., physicians in health-care settings) can be created using active learning techniques, such algorithms are uncommon in the application of ambient intelligence to health-care environments. Research questions at this point can instead focus on whether or how the algorithm influences clinical treatment and, ideally, patient outcomes. Based on the use of the algorithm, research attention may also turn to quality enhancements. Domain shift is a phenomenon where algorithm performance might change while switching from training data to target data. For instance, if an algorithm encounters a strange room layout that it was never exposed to during training, it may fail. Unexpected outcomes like this need to be looked into, which frequently entails someone examining the photographs to comprehend the mechanism of failure and develop a fix. The output of the deployed algorithm must be linked to some clinical procedure or action in order for ambient intelligence to be useful, which is frequently not enough. Is there a human in the loop who is presented a notice and then must determine how to respond, in which case is it preferable to err on the side of notifying too much or too little? Does the algorithm's output automatically result in a decision or action? What are the operational or clinical indicators used to gauge success? These inquiries serve as the link between an algorithm that performs well theoretically and one that really helps patients or other stakeholders. How to test the algorithms in a clinical setting is a topic that is brought up during the deployment phase. If the sensors and algorithms are combined, they may be categorised as medical devices in the USA and be subject to oversight by the US Food and Drug Administration. The list of activities or behaviours that the research community is interested in might expand as our understanding of how to produce this technology advances. To identify an additional set of activities for labelling, previously annotated photos can be reannotated (or researchers may be interested in a finer gradation of previously tagged activities). Furthermore, the performance of algorithms may be enhanced over time by creating ever larger databases of tagged pictures. At every level of the research process, interaction with numerous ethical problems is also necessary for the creation of ambient intelligence. There are already general ethical frameworks for the use of machine learning and artificial intelligence. It will be crucial to develop tools and procedures for ambient intelligence usage that incorporate active and ongoing reflection and engagement with ethical issues in the design and development of these applications, going beyond lists of broader principles. For instance, it will be important to determine the stages of development at which to engage stakeholders' perspectives or incorporate ethical consultation. The table summarises the ethical concerns associated with ambient intelligence creation and application in healthcare settings, while the following sections go into more detail. A person is protected against unauthorised access to or interference with their private affairs by a range of obligations and rights that are included in the concept of privacy. The importance of informational privacy is frequently emphasised in artificial intelligence projects and healthcare settings. Informational privacy includes how and when personal information should be communicated or obtained and what uses of it will be made by others. It also encompasses the collection, storage, use, maintenance, dissemination/disclosure, and disposition of personal information. Ambient sensors may gather information on a range of individuals in healthcare environments, including patients, physicians, residents or postgraduate trainees, nurses, hospital personnel, patients' loved ones, and others. An ambient sensor can record a person's face, voice, heart rate, stride, and other physical characteristics, as well as data that can expose IP addresses, depending on the hardware's specifications. These kinds of data might be used to identify a person personally or to reveal sensitive information about their activities or health to the public. When several sorts of data (such voice, breathing, and body temperature) are gathered and evaluated together, they may be utilised to develop predictions about how a person will feel in the future. Participants might not be aware of the extra health inferences that could be made from their data or how their data can be evaluated for prediction reasons. There are other privacy concerns outside informational privacy that may be problematic. Ambient sensors could be installed at a patient's home or in a variety of healthcare facilities that patients, hospital personnel, carers, family members, and other people might typically assume to be free of monitoring equipment. Some individuals might wish to limit when a stranger can see specific portions of their body or keep an eye on them while they're in a vulnerable situation, such as when they're using the loo. A distinct component of privacy is decisional privacy, which is the right of a person to choose their own care and activities without undue intrusion by the government or unauthorised others. The types of consent that must be given, when they must be given, and who must grant them are all protected aspects of decisional privacy. Some of these privacy problems are pertinent to the stage of data collecting and algorithmic development. At various phases of a project's development, it could be important for stakeholders to know who has access to the data and whether an algorithm or a person is seeing it. With other values and project considerations, privacy is a value that requires trade-offs. The project type (such as research vs quality improvement) has an impact on the moral framework employed to evaluate these trade-offs. For instance, employing thermal imaging rather than complete video recording can mask participant identities, but this must be evaluated against other objectives, such as whether thermal imaging can sufficiently capture the features important to a project's scientific objectives. Individual privacy protection and the need to encourage data exchange for scientific objectives are often balanced by privacy measures in medical research. Researchers working with ambient intelligence who are gathering data from sensors must be able to clearly state the advantages of their work in order to facilitate weighing those advantages against privacy risks and developing appropriate privacy protection measures. There are other privacy concerns outside informational privacy that may be problematic. Ambient sensors could be installed at a patient's home or in a variety of healthcare facilities that patients, hospital personnel, carers, family members, and other people might typically assume to be free of monitoring equipment. Some individuals might wish to limit when a stranger can see specific portions of their body or keep an eye on them while they're in a vulnerable situation, such as when they're using the loo. A distinct component of privacy is decisional privacy, which is the right of a person to choose their own care and activities without undue intrusion by the government or unauthorised others. A project should determine whether state and municipal data privacy or biometric laws apply. For instance, the California Consumer Privacy Act gives customers the right to view, share, and delete their personal information that has been gathered by organisations. This right may apply to particular settings and data related to health care. In contrast to HIPAA, the EU Data Privacy Regulation (GDPR) is more comprehensive and defines personal data as data related to an identified or identifiable individual. Thus, data like IP addresses and video pictures may be subject to the GDPR. Additionally, if they treat patients from Europe, US healthcare institutions may be held accountable under the GDPR. To utilise protected health information for particular research projects, the HIPAA Privacy Rule requires informed consent, a waiver of authorization, or evidence of informed consent; however, there are no limits on the use or dissemination of de-identified information. Two methods for identifying patient data are outlined under HIPAA: safe harbour and expert decision. According to the safe harbour approach, all 18 specified personal identifiers must be removed. These include dates and names as well as voice and fingerprints as well as full-face photos and any pictures that are similar. Therefore, it might not be possible to de-identify visual sensor data in clinical contexts. Additional deidentification steps can be required by local institutional review boards or state regulations.The expert decision approach states that an expert must conclude that the risk is extremely low that the information may be used by an expected receiver to identify a person who is the subject of the information, either by itself or in conjunction with other reasonably accessible information. This criterion might be achieved by carefully controlling who has access to the data and by prohibiting the combination of data. Think of an annotator using a secure terminal, where it is forbidden to copy picture data and to combine data (such as image data with internet search data). The data might then be regarded as de-identified according to this criterion. Although it is more likely to cost more, the expert determination technique to deidentification is easier to customise to the project at hand and more consistent with giving precise assurances on the completeness of the de-identification on offer. Both approaches to de-identification may be appropriate for a particular ambient intelligence project. It is crucial to remember that there is always a chance that data might be reidentified. Large internet databases are increasingly including personal information, and current developments in data aggregation and analytics increase the likelihood that data may be reidentified. Numerous various forms of health data that were traditionally deidentified can be reidentified, according to studies. Approaches can be used to reduce the danger of re-identification, at best.

4. WORKPLACE

Important obstacles to the protection of privacy as we currently understand it exist in an AmI environment. The division between personal and professional life is a crucial issue. As seen by this hypothetical situation, the lines separating the two will blur as more individuals work from home and communicate about personal matters over distance in the workplace. All of this is strongly related to the interconnectedness and articulation of the many places that exist today. We may need to reinvent or reinterpret the concepts of home, communication, and private life under AmI. The expert decision approach states that an expert must conclude that the risk is extremely low that the information may be used by an expected receiver to identify a person who is a subject of the information, either alone or in conjunction with other reasonably accessible information. This criterion might be achieved by carefully controlling who has access to the data and by prohibiting the combination of data. Think of an annotator using a secure terminal, where it is forbidden to copy picture data and to combine data (such as image data with internet search data). The data might then be regarded as de-identified according to this criterion. It is crucial to maintain the safety of this information in a world where everything will be connected and information will travel between many locations. In order to be able to complete contracts across networks, we also need secure systems. Several legislative provisions impose significant security requirements on service providers. However, there are significant enforcement issues because there are no clear regulations governing the fulfilment of these security requirements. Who can be held accountable when harm results from poor security is the key question. When two or more service providers are involved, it might be challenging for the victim to pinpoint just who is to blame for a security breach. Similar issues might arise if the security of the home network used for business reasons is compromised. However, this shouldn't prohibit the victim from obtaining compensation. It is important to strengthen consumer protection against undesirable parts of e-commerce, remote contracts, and unsolicited marketing messaging. In an AmI future, service providers would work to gather as much data as possible in order to offer individualised services and communications. However, such handling of personal data also implies significant hazards. Data processors should exercise caution when handling inaccurate information since the data subject might suffer serious consequences. Additionally, profiling will be crucial in facilitating AmI services. As a result, the risks associated with inaccurate or lacking information are increased. Although the data subject is given protections under the law, it is essential to make sure that these protections are really used. Particularly important is the protection of data subjects against decisions made purely on the basis of automated data processing. These methods are included in EU Directives 95/46 and 2002/58, however they do not apply to police profiling or other "third pillar"-related operations. It could be necessary to rectify this gap. The practice of "data laundering," where (similar to "money laundering") a huge unregulated and untraceable (commercial) circulation of individual profiles and personal data might become one of the "escape routes," could pose a threat to the implementation of data protection laws. Here, some particular actions may be envisaged, such as the adoption of a requirement to notice significant acquisitions of personal data and specific incrimination. The Cybercrime Convention punishes unauthorised access to and unauthorised interception of computer systems or data (such as gaining access to the data on the RFID blouse). The scope of this harmonisation, however, is constrained both in terms of substance (countries may impose additional requirements before an act qualifies as a crime) and geography (only a small number of nations have joined the Convention)

5. ANALYSIS

For Conviviality, in order to prevent one side from being overpowered by another, best practises and standards for creating ambient intelligence systems must take into account factors including ensuring each party's point of view. The idea of conviviality is essential for ambient intelligence because it enables consideration of the social, cognitive, and ethical challenges brought up by the large-scale development of ambient intelligence systems and also highlights the drawbacks that must be overcome. For health-care, The discussion of privacy issues for the use of ambient intelligence should attempt to go beyond merely adhering to applicable regulations and examine the many values and trade-offs associated with privacy interests. Which ethical framework is utilised to assess these trade-offs and interests will depend on the specific usage of ambient intelligence. When creating an ambient intelligence application, it is important to keep in mind that many players in the healthcare industry are subject to various ethical and legal frameworks. Which legal standards involving privacy and informed permission will be applicable, for instance, depends on whether a study is carried out as research rather than quality enhancement. "The need to make systems capable of understanding and relating to people at a social level, timing, and cuing their interactions in a socially adept manner" is the challenge that awaits researchers in ambient intelligence.

6. CONCLUSION

For medical research, researchers have examined a few of the moral dilemmas the research community faced as ambient intelligence in healthcare settings developed. These problems will need to be anticipated and addressed by researchers who are pushing the boundaries of ambient intelligence applications in healthcare. For instance, although privacy is a major concern, additional privacy factors, such as data protection, must be weighed against other interests and values. Collaboration across disciplines will be helpful in detecting and resolving possible ethical problems. Participants' potential harms can be reduced by involving experts with relevant experience outside of research teams and the stakeholders themselves. At the workplace, research shows AmI vulnerabilities in a normal family's life in three different settings—at home, at work, and at a park (a public area). It implies that users and therefore AmI services are mobile inside and across various areas. However, the main emphasis is on dangers and vulnerabilities that may result in critical scenarios or so-called dark situations linked to inconvenience, control, crime, security, and profiling, among other things. Research also suggests a sense of some of the possible benefits of AmI services. This situation also brings up significant difficulties like security and human aspects, negative emotions, notably loss of control, exaggerated reactions based on unfounded assumptions, identity theft, and exclusion.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] J. Synnott, S. McComb, C. Nugent, and J. McLaughlin. 2015. NI-CHIC: A model for academic engagement with industry. In Ambient Intelligence for Health: First International Conference, AmIHEALTH 2015 Puerto Varas, Chile, December 1-4, 2015 Proceedings. J. Bravo, R. Hervas, and V. Villarreal (Eds.). Springer, 258–263. DOI:https://doi.org/ 10.1007/978-3-319-26508-7

[2] Michael M. Bronstein, Joan Bruna, Yann Lecun, Arthur Szlam, and Pierre Vandergheynst. 2017. Geometric deep learning: Going beyond Euclidean data. IEEE Signal Processing Magazine 34, 4 (2017), 18–42. DOI:https://doi.org/10. 1109/MSP.2017.2693418 arxiv:1611.08097

[3] Aylin Caliskan, Joanna J. Bryson, and Arvind Narayanan. 2017. Semantics derived automatically from language corpora necessarily contain human biases. Science 356, 6334 (2017), 183–186. DOI:https://doi.org/10.1126/science. aal4230

[4] Davide Calvaresi, Daniel Cesarini, Paolo Sernani, Mauro Marinoni, Aldo Franco Dragoni, and Arnon Sturm. 2017. Exploring the ambient assisted living domain: A systematic review. Journal of Ambient Intelligence and Humanized Computing 8 (2017), 239–257. DOI:https://doi.org/10.1007/s12652-016-0374-3

[5] John Canny. 1986. A computational approach to edge detection. IEEE Transactions on Pattern Analysis and Machine Intelligence PAMI-8, 6 (Nov. 1986), 679–698. DOI:https://doi.org/10.1109/TPAMI.1986.4767851

[6] Maurizio Caon, Stefano Carrino, Simon Ruffieux, Omar Abou Khaled, and Elena Mugellini. 2012. Augmenting interaction possibilities between people with mobility impairments and their surrounding environment. Communications in Computer and Information Science 322 (2012), 172–181. DOI:https://doi.org/10.1007/978-3-642-35326-0_18

[7] Roberto Casas, Rubén Blasco Marín, Alexia Robinet, Armando Roy Delgado, Armando Roy Yarza, John McGinn, Richard Picking, and Vic Grout. 2008. User modelling in ambient intelligence for elderly and disabled people. In Computers Helping People with Special Needs. Lecture Notes in Computer Science, Vol. 5105. Springer, 114–122. DOI:https://doi.org/10.1007/978-3-540-70540-6_15

[8] Haoyu Chen, Xin Liu, Xiaobai Li, Henglin Shi, and Guoying Zhao. 2019. Analyze spontaneous gestures for emotional stress state recognition: A micro-gesture dataset and analysis with deep learning. Proceedings of the 14th IEEE International Conference on Automatic Face and Gesture Recognition (FG'19). DOI:https://doi.org/10.1109/FG.2019. 8756513

[9] SaisakulChernbumroong, Ahmad Lotfi, and Caroline Langensiepen. 2015. Prediction of mobility entropy in an ambient intelligent environment. In Proceedings of the 2014 IEEE Symposium on Intelligent Agents (IA'15). 65–72. DOI:https://doi.org/10.1109/IA.2014.7009460

[10] Diane J. Cook, Juan C. Augusto, and Vikramaditya R. Jakkula. 2009. Ambient intelligence: Technologies, applications, and opportunities. Pervasive and Mobile Computing 5, 4 (2009), 277–298. DOI:https://doi.org/10.1016/j.pmcj.2009.04. 001

[11] CiprianCorneanu, Fatemeh Noroozi, Dorota Kaminska, Tomasz Sapinski, Sergio Escalera, and GholamrezaAnbarjafari. 2018. Survey on emotional body gesture recognition. IEEE Transactions on Affective Computing. Early access, October 16, 2018. DOI:https://doi.org/10.1109/TAFFC.2018.2874986

[12] 2.Unna N. Danner, Henk Aarts, and Nanne K. De Vries. 2008. Habit vs. intention in the prediction of future behaviour: The role of frequency, context stability and mental accessibility of past behaviour. British Journal of Social Psychology 47, 2 (2008), 245–265. DOI:https://doi.org/10.1348/014466607X230876

[13] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2019. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. Technical Report. Google AI Language. arxiv:1810.04805v2.

[14] Yegang Du, Yuto Lim, and Yasuo Tan. 2019. A novel human activity recognition and prediction in smart home based on interaction. Sensors (Switzerland) 19, 20 (2019), 4474. DOI:https://doi.org/10.3390/s19204474

[15] K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten, and J.-C. Burgelman. 2001. Scenarios for ambient intelligence in 2010. Society 2001 (2001), 58. ftp://ftp.cordis.europa.eu/pub/ist/docs/istagscenarios2010.pdf.

[16] Abubaker Elbayoudi, Ahmad Lotfi, Caroline Langensiepen, and Kofi Appiah. 2016. Determining behavioural trends in an ambient intelligence environment. In Proceedings of the 9th ACM International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'16). ACM, New York, NY, 1–8. DOI:https://doi.org/10.1145/2910674. 2935834

[17] Abubaker Elbayoudi, Ahmad Lotfi, Caroline Langensiepen, and Kofi Appiah. 2017. Trend analysis techniques in forecasting human behaviour evolution. In Proceedings of the 10th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA'17). 293–299. DOI:https://doi.org/10.1145/3056540.3076198

[18] .Pier Luigi Emiliani and Constantine Stephanidis. 2005. Universal access to ambient intelligence environments: Opportunities and challenges for people with disabilities. IBM Systems Journal 44, 3 (2005), 605–619. DOI:https: //doi.org/10.1147/sj.443.0605

[19] K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten, and J.-C. Burgelman. 2003. Scenarios for Ambient Intelligence in 2010. Technical Report. ISTAG.

[20] .Iram Fatima, Muhammad Fahim, Young-Koo Lee, and Sungyoung Lee. 2013. A unified framework for activity recognition-based behavior analysis and action prediction in smart homes. Sensors 13, 2 (2013), 2682–2699. DOI:https://doi.org/10.3390/s130202682

[21] Michael Friedewald, Elena Vildjiounaite, Yves Punie, and David Wright. 2007. Privacy, identity and security in ambient intelligence: A scenario analysis. Telematics and Informatics 24, 1 (2007), 15–29. DOI:https://doi.org/10.1016/j. tele.2005.12.005

[22] Nuno M. Garcia and Joel Jose P. C. Rodrigues. 2015. Ambient Assisted Living. CRC Press, Boca Raton, FL. DOI:https: //doi.org/10.1201/b18520

[23] .Yoav Goldberg. 2017. Neural network methods for natural language processing. Synthesis Lectures on Human Language Technologies 10, 1 (April 2017), 1–309. DOI:https://doi.org/10.2200/S00762ED1V01Y201703HLT037

[24] Karthik Gopalratnam and Diane J. Cook. 2004. Active Lezi: An incremental parsing algorithm for sequential prediction. International Journal on Artificial Intelligence Tools 13, 04 (2004), 917–929. DOI:https://doi.org/10.1142/ s0218213004001892

[25] David Griol, Zoraida Callejas, and Ramón López-Cózar. 2015. A framework to develop context-aware adaptive dialogue systems. In Proceedings of the Annual Conference of the International Speech Communication Association (INTERSPEECH'15). 2012–2016.

[26] KristrúnGunnarsdóttir and Michael Arribas-Ayllon. 2003. Ambient Intelligence: A Narrative in Search of Users. Discussion Paper. Lancaster University.

[27] P. Gupta and P. R. Kumar. 2000. The capacity of wireless networks. IEEE Transactions on Information Theory 46, 2 (March 2000), 388–404. DOI:https://doi.org/10.1109/18.825799

[28] Albert Haque, Arnold Milstein, and Li Fei-Fei. 2020. Illuminating the dark spaces of healthcare with ambient intelligence. Nature 585, 7824 (2020), 193–202. DOI:https://doi.org/10.1038/s41586-020-2669-y

[29] Weijia He, Juliette Hainline, Roshni Padhi, and Blase Ur. 2018. Clap on, clap off: Usability of authentication methods in the smart home. In Proceedings of the Interactive Workshop on the Human Aspect of Smarthome Security and Privacy (WSSP'18). 1–3. https://support.apple.com/en-us/HT208108,

[30] Dan Ionescu, Bogdan Ionescu, Cristian Gadea, and Shahidul Islam. 2011. An intelligent gesture interface for controlling TV sets and set-top boxes. In Proceedings of the 6th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI'11). 159–164. DOI:https://doi.org/10.1109/SACI.2011.5872992

[31] Mian Ahmad Jan, Wenjing Zhang, Muhammad Usman, Zhiyuan Tan, Fazlullah Khan, and Entao Luo. 2019. SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. Journal of Network and Computer Applications 137 (March 2019), 1–10. DOI:https://doi.org/10.1016/j.jnca.2019.02.023

[32] Jerry Kaplan. 2017. Artificial intelligence: Think again. Communications of the ACM 60, 1 (2017), 36–38. DOI:https: //doi.org/10.1145/2950039

[33] Irakli Kardava, Jemal Antidze, and Nana Gulua. 2016. Solving the problem of the accents for speech recognition systems. International Journal of Signal Processing Systems 4, 3 (2016), 235–238. DOI:https://doi.org/10.18178/ijsps.4. 3.235-238

[34] Aggelos K. Katsaggelos. 2002. IEEE Signal Processing Magazine: Farewell. IEEE Signal Processing Magazine 19, 6 (2002), 2–4

[35] R. W. Keyes. 2000. Miniaturization of electronics and its limits. IBM Journal of Research and Development 44, 1.2 (Jan. 2000), 84–88. DOI:https://doi.org/10.1147/rd.441.0084

[36] Yassin Kortli, Maher Jridi, Ayman Al Falou, and Mohamed Atri. 2020. Face recognition systems: A survey. Sensors (Switzerland) 20, 2 (2020), 342. DOI:https://doi.org/10.3390/s20020342

[37] Martin Legowiecki. 2016. Using artificial intelligence to create invisible UI. TechCrunch. Retrieved March 5, 2021 from https://techcrunch.com/2016/08/15/using-artificial-intelligence-to-create-invisi ble-ui/

[38] Wenbin Li and Matthieu Liewig. 2020. A survey of AI accelerators for edge environment. In Trends and Innovation in Information Systems and Technologies. Advances in Intelligent Systems and Computing, Vol. Springer, 35–44. DOI:https://doi.org/10.1007/978-3-030-45691-7_4

[39] Jaime Lien, Nicholas Gillian, M. Emre Karagozler, Patrick Amihood, Carsten Schwesig, Erik Olson, Hakim Raja, Ivan Poupyrev, and Google Atap. 2016. Soli: Ubiquitous gesture sensing with millimeter wave radar. ACM Transactions on Graphics 35, 10 (2016), Article 142. DOI:https://doi.org/10.1145/2897824.2925953

[40] Hua Liu, Guo Chen, and Yanting Huang. 2019. Smart hardware hybrid secure searchable encryption in cloud with IoT privacy management for smart home system. Cluster Computing 22, s1 (2019), 1125–1135. DOI:https://doi.org/ 10.1007/s10586-017-1143-6

[41] Ahmad Lotfi and Caroline Langensiepen. 2012. Smart homes for the elderly dementia sufferers: Identification and prediction of abnormal behaviour. Journal of Ambient Intelligence and Humanized Computing 3, 3 (2012), 205–218. DOI:https://doi.org/10.1007/s12652-010-0043-x