Farina. *J Smart Environ Green Comput* 2023;3:37-43
DOI: 10.20517/jsegc.2023.11

Journal of Smart Environments and Green Computing

Editorial

Open Access

Chat GPT in smart home systems: prospects, risks, and benefits

Mirko Farina

Faculty of Humanities and Social Sciences, Innopolis University, Innopolis 420500, Republic of Tatarstan, Russian Federation.

Correspondence to: Prof. Mirko Farina, Faculty of Humanities and Social Sciences, Innopolis University, Universitetskaya St, 1, Innopolis 420500, Republic of Tatarstan, Russian Federation. E-mail: m.farina@innopolis.ru

How to cite this article: Farina M. Chat GPT in smart home systems: prospects, risks, and benefits. *J Smart Environ Green Comput* 2023;3:37-43. https://dx.doi.org/10.20517/jsegc.2023.11

Received: 19 May 2023 **Accepted:** 14 Jun 2023 **Published:** 16 Jun 2023

Academic Editor: Zhaoyang Dong **Copy Editor:** Pei-Yun Wang **Production Editor:** Dong-Li Li

INTRODUCTION: INTERNET OF THINGS AD SMART HOME SYSTEMS

The expression Internet of Things (IoT, henceforth) denotes a network of interrelated computing devices (mechanical and digital machines) and objects, animals, and/or people that are provided with unique identifiers (UIDs) and the ability to transfer data over the said network in almost real time[1]. Examples of "things" in IoT networks include WiFi-controlled fridges, dishwashers and driers, remotely programmable thermostats, smart TVs and watches, surveillance cameras, alarm pads, people with heart monitor implants, farm animals with biochip transponders, fitness trackers (such as Fitbit Charge), self-driving cars or trucks, etc.

What is interesting about this technology is the fact that it provides all the nodes of any given network (whether they are machines, humans, or a combination of them) with complete, sound, and reliable (often efficient) information about what is going on around them[2]. This has been achieved because of (among other things): (a) significant advances in wireless networking technology[3]; (b) greater standardization in communication protocols[4]; (c) remarkable developments in sensor technology[5,6]; and (d) the constant and steady decrease in the cost of production for silicon chips[7]. By some estimates, there will be over 100 billion IoT devices worldwide by 2026[8]. It is, therefore, not surprising that numerous institutions and industries across the globe begun using IoT to operate more efficiently (e.g., reduce the costs of their businesses),

better understand their customers, improve their services, and enhance decision-making processes[9,10].

Thanks to the power of Artificial Intelligence (AI), IoT has also made a significant impact on home automation. Home automation, as its name suggests, is a process that allows homeowners to remotely control various systems in their houses from a centralized hub[11]. This technology is designed to allow machines to process data independently from humans and to draw certain conclusions autonomously. What makes IoT and home automation fascinating for many people is the sheer scale and variability of devices and platforms that they can -in principle- incorporate. For example, automated lighting systems can adjust light levels automatically according to ambient light conditions or pre-set programs tailored to match the personal preferences of users. Smart door locks powered by AI can recognize the faces of regular visitors and unlock the house without the need for the owners to always carry the keys. Voice-activated assistants (such as Alexa, Siri, and Alisa) can be used to surf the internet and ask all sorts of questions (concerning the weather or more sensitive ones -for instance- about politics, history, or science) while sending texts or emails, keeping track of trips, and even organizing data (such as healthcare information). In sum, it appears as if homeowners -due to rapid advances in AI technology- can now get better value out of their purchases and receive unprecedented convenience benefits.

However, as Ashton[12] brilliantly noticed, we can say that IoT (in the context of home automation but also beyond it) threatens to alter the balance of power in human-machine relations, switching the equation from human-based data input (where the human remains in control) to human- and machine-based data input (where the machines occasionally take precedence over the human). In this short contribution, building and expanding on this important observation, I will briefly comment on the future development of the technology underlying home automation and on its possible integration with Large Language Models (LLMs), such as Chat GPT, essentially models that can generate natural language texts from large amounts of data, via self-supervised learning[13]. While such marriage - I shall argue- may offer tremendous opportunities for their users (for example, in terms of greater functionality and convenience through ubiquitous networking), I will also point out various concerns revolving around personal security, privacy, and ethical issues, which demand significant attention and urgent actions. The goal, obviously, is not to impede the progress of this technology but rather to make decision-makers and users alike fully aware of the potential undesirable consequences that the uncritical (naïve) usage of such technology may trigger in the long term.

CHAT GPT AND SMART HOME SYSTEMS: PROMISES AND POTENTIAL BENEFITS

One of the most promising AI systems for the development of IoT is Chat GPT, a natural language processing chatbot that uses machine learning to generate quite sophisticated answers to given questions[14]. The chatbot works by analyzing a query, breaking it down into its components, and then finding the most relevant information to solve it[15]. Chat GPT has many potential applications in smart cities, ranging from automated customer service to city planning (e.g., spotting traffic congestion, hence suggesting amelioration for infrastructure) and even city management (by leveraging it, local governments can develop better services, resulting -for example- in economic growth). Thus, Chat GPT seems to be (in many senses) an ideal tool for smart city optimization. In this short commentary, however, I would like to focus - as noticed above- on the potential applications of Chat GPT in home environments (private places), specifically in the context of smart home systems. Some of the (negative) considerations I will make, though, potentially apply to smart cities (public places) as well.

As smart home automation becomes more and more popular, it becomes necessary to provide users with smooth, intuitive, and more natural ways to access their appliances[16]. The combination of Chat GPT and

smart home automation bears the promise of serving this purpose extremely well. For example, users could use the refined language capabilities of Chat GPT to automate several tasks (such as setting up alarms, scheduling reminders ahead of time, and organizing calendars) simply with their voice. The combination of Chat GPT with smart home automation could also be used to enhance the security of any home. The chatbot, thanks to AI, could -for instance- be used to detect suspicious (unordinary) activities in the house or to monitor conversations within the home with the goal of finding out potential security breaches (for instance, by analyzing voice patterns recorded live and matching them against those of the homeowners, which could be stored on the cloud).

Another benefit (although arguable) arising from the integration of Chat GPT with smart home systems would lie in its ability to provide personalized recommendations[17]. Naturally, the learning displayed could be limited -at the beginning- in terms of acquired knowledge; however, for the sake of argument, we can assume a situation in which the integration is reliable, constant, and perpetual, so to speak. In that case, by learning from previous interactions of the user with the chatbot, Chat GPT could offer (based on algorithmic predictions and statistical analysis) tailored suggestions for products and services that may be of interest to the homeowner (pretty much like social media already do, but in a much more powerful way). These suggestions could indeed be very useful to those seeking to buy new gadgets or appliances, say, for their homes. Suggestions could also be made by the chatbot for purchasing a specific movie, a piece of clothing, a certain song, or a car (based on the behavioral patterns, pre-set preferences, or recorded conversations of the user). The chatbot could also compile a list of several options available on the market and offer them for choice (in case he/she is uncertain about the specific item he/she is looking for). This could well lead to greater efficiency (time optimization), more convenience and comfort, and more intuitive interfaces for controlling home environments, which would not require the memorization of complex commands or the performance of tedious searches through various menus.

To be sure, this is not a work of science fiction. A proof-of-concept video gives us a glimpse of what the near future may look like (https://www.theverge.com/2023/1/19/23562063/gpt3-siri-apple-shortcuts-homekit-demo-voice-assistant-artificial-intelligence). Here, a developer is asking his voice assistant (Josh) -integrated with Chat GPT- "to open the shades, to turn off the music in his flat, and to let him know what the weather is". Remarkably, the voice assistant handles the three requests given at the same time rather smoothly. The developer then goes on to tell "Josh" that he is "filming a video" and that "it's kind of dark in here", to which the voice assistant quickly responds by turning up the lights in the room (thereby making a rather impressive inference) (https://www.youtube.com/watch?web=1&wdLOR=c784E8594-F16D-4CE8-81E4-F39E6F2BC1DB&v=FL_LP8u4E4g&feature=youtu.be&ab_channel=JoshAI). Today, standard voice assistants (not integrated with Chat GPT) are not very accurate, require precise language input, are sensitive to different accents, and occasionally confuse basic requests or even mishear them, often providing useless responses. Josh, on the contrary, being integrated with an LLM, seems to be very effective in carrying out the given tasks (this is due to the superior conversional abilities of Chat GPT). As of today, to the best of my knowledge, there are no measures of performance of this possible integration reported in the relevant literature; however, as several researchers start looking at this issue[18-20], we can expect decisive progress on the field. Therefore, the point I am trying to make for the economy of this commentary is the following: the combination of home automatization with the conversational capabilities of LLMs (such as Chat GPT) could open the door to important behavioral changes in our domestic environs, thereby revolutionizing the way in which we relate to our homes and to each other within them.

THE POTENTIAL RISKS AND DANGERS OF INTEGRATING CHAT GPT-4 INTO SMART HOME SYSTEMS

A significant level of caution should nevertheless be exercised at this stage. Costs may constitute a major drawback in the implementation of this technology. Because the technology is very new, it would probably be extremely expensive to implement and maintain it; that is, it would likely require constant hardware updates to keep up with the latest information available. More importantly, perhaps, there seem to be two sets of concerns (involving security and ethical/privacy issues) surrounding the future development of smart home systems that demand immediate attention from decision-makers and may license many doubts - among potential users- about the desirability of this promised revolution. It is to such issues that I turn next.

Security issues for future smart homes

Malicious actors (including hackers or outright criminals) may use AI features in-built into the technology required for the integration of future smart homes to gain previously unavailable access to smart home activities, from an external location, with the goal of interfering or disrupting them. Criminals could, therefore, disable -at will- the functioning of cameras or alarm pads. They could likewise jam such systems and, in doing so, mislead the police with fake images or recordings. They could also send fake reports to non-present homeowners, which would be tricked into believing that their homes are safe when instead, they are being robbed. Manufacturers should therefore focus on developing (with maximum urgency) effective and personalized protocols for dealing (promptly and effectively) with cybersecurity incidents/threats[21]. This would be of paramount importance to guarantee a secure perimeter for smart homes. The procedure for the development of such protocols could include designing security strategies, which would require authentication checks against authorized (or unauthorized) third-party networks, increasingly personalized options for accessing the ecosystem, as well as maintaining constant secondary vigilance (man-powered) overprotected infrastructures. Another important issue potentially affecting future smart homes could involve data security[22]. Crooks could use Chat GPT when integrated with home automation to steal relevant data of customers (login credentials or information about bank accounts) from the cloud -for instance- via phishing emails. They could then sell such data to unscrupulous companies/ individuals or use them for non-legal activities [such as blackmailing (quid pro quo) or forgery].

Ethical and privacy issues for future smart homes

The full integration of Chat GPT with domestic automatized ecosystems (such as those described above) may prove to be extremely dangerous ethically as well. This is because unmonitored, generative AI could arbitrarily regurgitate discriminative content from the web with almost no filter. No company would want racist voice assistants spewing highly controversial content into people's homes through their hardware[23]. This is a risk that should be carefully considered before pushing ahead with the integration of these technologies. Another significant ethical concern related to the usage of this technology would be the loyalization of customers, which -in the long term and via repeated and uncritical usage- could lower psychological thresholds and lead to radical forms of consumerism, which would be detrimental to the unity and harmony of society.

Furthermore, the pervasive and large-scale integration of Chat GPT with smart home systems may also threaten personal privacy. Smart appliances would store data in some form on devices, and such data could be targeted by wrongdoers. Inconvenient recordings from any home could -for instance- be sold for profits or spread on the internet to cause reputational damage. Thus, comprehensive encryption practices should be embedded into development software. Possibly, very robust passwords should be installed upon initial configuration of smart appliances. Furthermore, mandatory software updates should be routinely carried out by tech companies, as those would ensure continued compatibility as well as protection against cyber-

attacks. However, where would all the sensitive information gathered in such a rich infosphere[24] be stored? And who would have access to it and under which circumstances? Strict and transparent guidelines should be implemented in this respect by both governments (possibly supranational institutions) and tech companies to safeguard users and pursue social and moral good[25]. Furthermore, it would be extremely important for users to understand how the collected data are being used by third parties and make sure that those adhere to privacy laws[26].

There is room for being skeptical about the feasibility of such a proposal, though. Since 2013, we have become increasingly aware that many tech companies spy on customers by actively profiling them through social media (the case of Cambridge Analytica is particularly instructive in this context). We also know that government agencies routinely carry out mass surveillance activity by accessing our inboxes, keeping track of material we share on messaging apps, scrutinizing the websites we open, or following the transactions we make online[27]. Thousands of laptops are found each year with hidden keyloggers. It is known that secret agencies have developed programs (such as the Brutal Kangaroo2) to infiltrate even air-gapped networks[28]. Thus, it is very probable to assume that the spread of this technology will attract the attention of governmental agencies, which would be presented with the unique possibility to wiretap citizens and constantly monitor them even at home. To be sure, forms of extensive monitoring already exist (as discussed above); however, the possibility to scale up such monitoring to unprecedented levels across the entire infosphere (and in extremely private places, such as homes) could be achieved with little possible limitations, once the technological infrastructure is sufficiently spread. This could lead to a significant diminishment of our basic freedoms, an Orwellian world, which in Foucauldian terms[29] we may well call "biopolitics"; a condition whereby a pervasive mode of power controls, influences, regulates, and even manages the entire life of its citizens. Consumers should be well aware of this possibility, which -alas- does not look so remote.

CONCLUSION

The integration of Chat GPT with smart home systems represents a great way to make home automation more intuitive and personalized. It can optimize our time, give us a feeling of "convenience", and even make us feel safer (e.g., less subject to crimes). However, decision-makers, tech companies, and users alike should carefully weigh in pros and cons of this potential full-scale integration before pushing ahead with it. As shown in this short commentary, the consequences might be dire, and the dangers significant, as important concerns arise with respect to data security, privacy (constant online monitoring), and ethical issues. All this may just be a too high price to pay for this feeling of smooth connectivity and convenience that we so much desire and strive for. There is an old adagio that says that knowledge is power. Technological literacy should urgently become a key focus of educational learning. The goal is to help future generations protect themselves against forms of technological/technocratic tyranny that may threaten our basic freedom and civil rights; those very freedoms and rights for which our forebears fought and (often) laid their lives.

DECLARATIONS

Acknowledgments

The author would like to express his gratitude to Prof. Witold Pedrycz for insightful discussions on this topic and for his precise and helpful feedback on earlier drafts of this manuscript.

Authors' contributions

The author contributed solely to the article.

Availability of data and material
Not applicable.

Financial support and sponsorship
None.

Ethics approval and consent to participate
Not applicable.

Conflicts of interest
All authors declared that there are no conflicts of interest.

Consent for publication
Not applicable.

REFERENCES
1. Greengard S. The internet of things. Cambridge, MA: MIT Press; 2021. DOI
2. Shackelford SJ. The internet of things: what everyone needs to know. Oxford, UK: Oxford University Press; 2020. DOI
3. Salau BA, Rawal A, Rawat DB. Recent advances in artificial intelligence for wireless internet of things and cyber-physical systems: a comprehensive survey. *IEEE Internet Things J* 2022;9:12916-30. DOI
4. Gawlik-kobylińska M. Current issues in combating chemical, biological, radiological, and nuclear threats to empower sustainability: a systematic review. *Appl Sci* 2022;12:8315. DOI
5. Howard J, Murashov V, Cauda E, Snawder J. Advanced sensor technologies and the future of work. *Am J Ind Med* 2022;65:3-11. DOI PubMed
6. Zhang Z, Wen F, Sun Z, Guo X, He T, Lee C. Artificial intelligence-enabled sensing technologies in the 5G/internet of things era: from virtual reality/augmented reality to the digital twin. *Adv Intell Syst* 2022;4:2100228. DOI
7. Mack C. The multiple lives of moore's law. *IEEE Spectr* 2015;52:31-31. DOI
8. Juniper Research Ltd. 5G monetisation: business models, strategic recommendations & market forecasts 2022-2027. Available from: https://www.juniperresearch.com/researchstore/operators-providers/5g-monetisation-research-report?utm_source=juniper_pr&utm_campaign=pr2_5gmonetisation_providers_operators_jan23&utm_medium=email. [Last accessed on 15 Jun 2023].
9. Lee I. The internet of things for enterprises: an ecosystem, architecture, and IoT service business model. *Internet of Things* 2019;7:100078. DOI
10. Lavazza A, Farina M. Infosphere, datafication, and decision-making processes in the AI era. Available from: https://link.springer.com/article/10.1007/s11245-023-09919-0. [Last accessed on 15 Jun 2023].
11. Nasir M, Muhammad K, Ullah A, Ahmad J, Wook Baik S, Sajjad M. Enabling automation and edge intelligence over resource constraint IoT devices for smart home. *Neurocomputing* 2022;491:494-506. DOI
12. Ashton K. That 'Internet of things' thing. *RFiD Journal* 2009;22:97-114. Available from: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=mtisukoAAAAJ&citation_for_view=mtisukoAAAAJ:IjCSPb-OGe4C. [Last accessed on 15 Jun 2023].
13. Social Europe. The promise and peril of generative AI. Available from: https://www.socialeurope.eu/the-promise-and-peril-of-generative-ai. [Last accessed on 15 Jun 2023].
14. Farina M, Lavazza A. ChatGPT in society: emerging issues. *Front Artif Intell* 2023;6:1130913. DOI
15. Gibney E. Open-source language AI challenges big tech's models. *Nature* 2022;606:850-1. DOI PubMed
16. Zaidan AA, Zaidan BB. A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. *Artif Intell Rev* 2020;53:141-65. DOI
17. Li J, Zhang W, Wang T, Xiong G, Lu A, Medioni G. GPT4Rec: a generative framework for personalized recommendation and user interests interpretation. arXiv: 2304.03879 [Preprint]. April 8, 2023. DOI
18. Shafeeg A, Shazhaev I, Mihaylov D, Tularov A, Shazhaev I. Voice assistant integrated with Chat GPT. *Indones J Electr Eng Comput Sci* 2023;12:1. DOI
19. Gill SS, Kaur R. ChatGPT: vision and challenges. *IoT and Cyber-Physical Systems* 2023;3:262-71. DOI

20. King E, Yu H, Lee S, Julien C. "Get ready for a party": exploring smarter smart spaces with help from large language models. arXiv: 2303.14143 [Preprint]. March 24, 2023. DOI
21. Bringhenti D, Valenza F, Basile C. Toward cybersecurity personalization in smart homes. *IEEE Secur Privacy* 2022;20:45-53. DOI
22. Moniruzzaman M, Khezr S, Yassine A, Benlamri R. Blockchain for smart homes: review of current trends and research challenges. *Comput Electr Eng* 2020;83:106585. DOI
23. Roberts T, Marchais G. Assessing the role of social media and digital technology in violence reporting. *Contemp Read Law Soc* 2018;10:9-42. DOI
24. Floridi L. The ethics of information. Oxford, UK: Oxford University Press; 2013. DOI
25. Farina M, Zhdanov P, Karimov A, Lavazza A. AI and society: a virtue ethics approach. *AI & Soc* 2022. DOI
26. Edu JS, Such JM, Suarez-tangil G. Smart home personal assistants: a security and privacy review. *ACM Comput Surv* 2021;53:1-36. DOI
27. Snowden E. Permanent record. NYC, NY: Metropolitan Books; 2019. Available from: https://en.wikipedia.org/wiki/Permanent_Record_(autobiography). [Last accessed on 15 Jun 2023].
28. Farina M, Lavazza A. The meaning of freedom after Covid-19. *Hist Philos Life Sci* 2021;43:3. DOI PubMed PMC
29. Foucault M. (1997). Society must be defended: lectures at the college de france, 1975-1976. Available from: http://s3.amazonaws.com/arena-attachments/2288168/a517f6153600c84ff334b416cf460745.pdf?1528579703. [Last accessed on 15 Jun 2023].