Open Universiteit

Privacy-Preserving in Smart Home Environments

White Paper, MAI-HOME Project WP4

Clara Maathuis

OU, 30.06.2024

1. Introduction

The efficient and sustainable use of energy has become a critical aspect for both the well-being of the planet as well as to modern and future societies. Herein, the advancements in the AI (Artificial Intelligence) and smart technologies domains present a unique opportunity to transform the way that energy is managed, used, and conserved. In this sense, AI solutions have the potential to optimize energy systems and enhance the efficiency of use while ultimately mitigating the environmental impact. In the context of smart homes, energy management is a crucial consideration. These residences are equipped with various sensors that can significantly influence the energy consumption patterns and the overall lifestyle of people. As such systems are increasingly reliant on data and AI technologies, they can also have a supportive role for the residents in order to make informed decisions in relation to their energy use, ways to reduce energy waste, and decrease corresponding energy costs.

Nevertheless, both the data used and the intelligent solutions developed for smart homes need to consider a secure and ethical handling by safeguarding the safety, security, and privacy of the residents and their data. This includes examining the sensors and systems employed in smart homes, the data communication protocols used, and the AI techniques considered for energy consumption modelling and prediction. Additionally, the evaluation of energy-saving strategies, behavioural change mechanisms, and their effectiveness in real-world settings becomes a key area of investigation. Hence, the solutions and systems developed for energy consumption analysis, prediction, and optimization should be robust,

accounting for diverse usage patterns and behaviours. Then the challenge lies in reaching an equilibrium between technological innovation and responsible energy management, ensuring that the systems and solutions developed go hand in hand with sustainability and the preservation of relevant energy resources.

As this white paper aims to discuss the meaning and implications of privacy in the context of smart home environments together with presenting a series of privacy preserving technologies that could be of use, its outline is structured as follows. The second section discusses important characteristics and considerations that need to be accounted when building solutions for smart home environments. The third section presents a series of general aspects that characterize privacy preserving technologies. The fourth section stresses the importance of privacy preserving technologies in the context of smart home environments when dealing with energy-related systems. And the concluding section discusses current and future perspectives that need to be accounted in both technical and social terms when building innovative intelligent solutions in the energy domain.

2. Smart Home Environments

Smart home environments are characterized by the integration of advanced (digital) technologies in residential living to enhance the convenience, safety, and overall quality of life of their residents. These intelligent living spaces employ specialized systems and solutions that are based on advanced digital technologies, such as AI, IoT (Internet of Things), cloud computing, and advanced sensor networks, to automate and streamline various aspects of daily living. At the core of a smart home environment often lies a complex network of interconnected systems that includes sensors and smart appliances. These systems continuously gather data about the environment and the residents' activities. This data is further processed by AI-based systems to make informed decisions and provide tailored services to the users. Through remote control and monitoring capabilities facilitated by cloud computing and secure communication protocols, smart home environments offer unparalleled convenience by allowing residents to manage various aspects of their living space like temperature, lighting, and home safety measures (Chakraborty et al., 2023).

One of the key characteristics of smart homes is their ability to automate various tasks and processes without manual intervention for various home technological or human systems or activities. Through the integration of smart sensors and corresponding intelligent applications, these homes can automatically adjust lighting, thermostats, and security systems based on occupancy, preferences, and environmental conditions, providing valuable support in relation to the use of energy and further, for energy conservation. Moreover, smart homes offer remote monitoring and control capabilities, enabling users to check and manage their home appliances and systems from anywhere using the Internet based on their own behaviours and needs. This feature not only enhances convenience but also promotes enhanced security, as residents can monitor their homes and respond to potential threats or emergencies in real-time. The core of smart homes is represented by the data collection and processing system. For this, sensors, cameras, and smart applications continuously gather information about the environment, occupancy, and user behaviour. This data is then processed, analysed, and used based on deploying various data analytics and AI solutions in order to generate intelligent outcomes and deliver tailored services based on the collected information.

Smart homes leverage the power of the IoT by connecting various devices and systems through the Internet, enabling centralized control and management. This interconnectivity allows for seamless integration and coordination of various home systems, such as lighting, climate control, entertainment, and security, providing a cohesive and efficient living experience. Personalization is another key aspect of smart homes, as they can learn user preferences and adjust settings accordingly, providing a customized experience tailored to the unique needs and preferences of residents. This adaptive nature ensures that the services provided by smart homes continuously evolve and improve, offering a truly personalized living experience. Furthermore, smart homes promote increased efficiency by optimizing energy consumption and home systems, leading to significant energy conservation and cost-effectiveness . This not only benefits the environment, however it also translates into tangible cost savings for the residents (Chakraborty et al., 2023; Pandiyan et al., 2023).

Additionally, smart homes promote an improved lifestyle and living environment by optimizing daily routines and automating various tasks, these systems foster a more favourable living pattern, reducing stress and freeing up time for more meaningful pursuits. Furthermore,

smart home technologies can monitor air quality and integrate devices like air purifiers, creating a healthier and more pleasant living environment for occupants, while also playing a crucial role in facilitating family care and communication (Basarir-Ozel et al., 2023: Rock et al., 2024).

This further facilitates and empowers the awareness of the residents to identify areas of inefficiency, gain insights into their consumption habits, and understand the environmental impact of their actions. Crucially, this awareness serves as a catalyst for behaviour change, motivating the residents to actively participate in energy management and conservation efforts by adopting energy-saving practices like adjusting thermostat settings, optimizing lighting usage, or unplugging systems in 'idle' status. Hence, the visibility provided by smart home systems fosters a sense of accountability and personal responsibility among residents, enabling them to take proactive steps towards reducing their environmental footprint and aligning their actions with sustainable values.

By catalysing behaviour change at the individual level, these systems can collectively contribute to significant reductions in energy consumption, translating into cost savings, reducing energy poverty, and mitigating the environmental impact of residential energy usage. As the demand for sustainable living solutions grows, smart home technology's role in fostering behaviour change through energy awareness becomes increasingly crucial, and further contributes to building more environmentally conscious and responsible energy consumption practices (Fakhar et al., 2023; Whitmarsh et al., 2021; do Canto et al., 2023).

3. Privacy Preserving Technologies

When developing, deploying, and using AI-based solutions for energy management and optimization in smart homes, it is crucial to prioritize privacy considerations to ensure the ethical and responsible development of these technologies. This is due to the fact that vast amounts of personal data collected by smart home devices must be handled with utmost care to protect individual privacy and prevent potential misuse or breaches. By prioritizing privacy protection, smart home technologies and systems can foster trust and confidence among users, enabling them to fully embrace the benefits of intelligent living spaces while safeguarding their personal information and activities (Panwar et al., 2019).

As UN stresses, privacy protection is a fundamental right that serves numerous critical purposes in safeguarding individuals and promoting societal well-being. By preventing the exposure of personal information, privacy protection reduces the risks of financial loss, social harm, and even physical danger that can arise from unauthorized access or misuse of sensitive data. This control over one's own information is essential for maintaining autonomy and ensuring that data is not exploited in ways that violate individual preferences or identities. Moreover, privacy preservation plays a crucial role in preventing discrimination and promoting fairness by making it harder for others to target individuals based on factors such as behaviour, health status, or social preferences. These are important considerations in the energy domain. Accordingly, privacy measures also serve as an wall against unauthorized access to sensitive information, mitigating the risks of data breaches and misuse by cyber criminals. In this way, privacy protection respects personal boundaries and fosters trust, encouraging individuals to engage in activities that require sharing data while promoting a sense of security. At the same time, privacy is closely linked to emotional well-being and mental health, as the knowledge that one's information is secure can reduce feelings of anxiety and promote a sense of safety. This underscores the multifaceted importance of privacy protection in maintaining the overall individual and societal well-being, making it a crucial consideration in the design and implementation of AI systems that handle personal data in the context of smart home environments (Archer et al., 2023).

An important instrument developed to regulate the development, deployment, and use of AI systems that process personal data is the GDPR (General Data Protection Regulation). The GDPR requires stakeholders like organizations and AI developers to ensure there are justifiable grounds for processing personal data, such as obtaining explicit consent or demonstrating legitimate interest while balancing individual rights. In this sense, the AI systems need to be transparent about how they use personal data and provide meaningful information to individuals about the logic involved in automated decision-making. Furthermore, the GDPR grants important rights to individuals, including access to their data, portability, explanation of automated decisions, and the ability to contest detrimental outcomes. The organizations deploying AI-based solutions are accountable for their impact and must conduct data protection impact assessments for high-risk AI applications. Integrating data protection measures into AI development from the start, thus since its design

phase is crucial. This process includes security reviews, comprehensive audits of the software development lifecycle, and establishing clear data governance standards. By prioritizing data protection, transparency, and accountability, organizations can benefit of using intelligent systems while respecting fundamental rights. This calls in a specific context for dialogue between involved stakeholders, policymakers, and regulators for providing guidance and ensuring consistent application of GDPR principles in a specific context (EU Parliament, 2020).

In this context, the GDPR requires smart home developers to ensure justifiable grounds for data processing, obtain explicit consent, and implement robust privacy protection measures. Smart home technologies must be transparent about data usage, provide meaningful information to users about automated decision-making, and respect individual rights like data access and portability. Organizations deploying smart home systems are accountable for their impacts and must conduct data protection impact assessments for high-risk applications. By prioritizing data protection, transparency, and accountability, developers can harness the benefits of smart homes while respecting fundamental privacy rights. Ongoing collaboration between stakeholders, policymakers, and regulators is essential to provide guidance and ensure consistent application of GDPR principles to smart home technologies (Piasecki & Chen, 2022; Jhuang et al., 2023).

These principles are designed to ensure that personal data is handled in a lawful, fair, and transparent manner, and that individuals have control over their data. The principle of lawfulness, fairness, and transparency requires stakeholders to have a valid legal basis for processing personal data and be transparent about how they collect, use, and share data. Purpose limitation mandates that personal data be collected for specific, explicit, and legitimate purposes, and not further processed in an incompatible manner. Data minimization ensures that organizations only collect and process personal data that is adequate, relevant, and limited to what is necessary for the specified purposes. Accuracy obliges organizations to keep personal data up to date and take reasonable steps to erase or rectify inaccurate data without delay. Storage limitation requires that personal data be kept for no longer than necessary, with organizations establishing time limits for erasure or periodic review. The principle of integrity and confidentiality necessitates that personal data be processed securely, with appropriate measures to protect against unauthorized access or use. Finally, the accountability principle holds organizations responsible for demonstrating compliance

with the GDPR principles. This includes implementing appropriate technical and organizational measures and being able to prove compliance to regulatory authorities. By adhering to these principles, organizations can ensure that personal data is handled in a responsible and ethical manner, respecting the rights and freedoms of individuals while harnessing the benefits of data processing (European Union, 2016).

Key privacy preserving strategies include implementing edge computing to minimize data sharing, employing advanced encryption techniques like homomorphic encryption to process data without decryption and differential privacy, adopting a preventive stance in respect to the use of data and design of AI solutions, and adhering to the principles of privacy by design to strike a balance between the benefits of AI-powered energy optimization and the protection of personal privacy. Transparency, user control, robust security protocols, regular audits for bias and discrimination, and the development of ethical guidelines for AI deployment are necessary to ensure that the potential benefits of these technologies are realized while respecting individual privacy rights.

4. Privacy Preserving Technologies in Smart Home Environments

Smart home environments pose a unique challenge in balancing the preservation of user privacy with the functionality and convenience offered in this environment. While smart homes collect vast amounts of personal data to provide enhanced comfort, security, and efficiency, they must also implement robust privacy protection measures to address the susceptibility of this sensitive information to passive monitoring, inference attacks, and unauthorized access. Ensuring that personal information and activities remain confidential, with users maintaining control over their data, is crucial to prevent potential harm and promote emotional well-being and mental health. To strike the right balance, developers must prioritize privacy in the design and implementation of smart home technologies through a multidisciplinary approach, including edge computing, advanced encryption techniques, and customizable privacy settings. By fostering trust and confidence among users through robust privacy measures, developers can enable individuals to fully embrace the benefits of intelligent living spaces while safeguarding their personal information and respecting their privacy rights, ultimately ensuring the widespread adoption and acceptance of smart home technologies that

enhance the quality of life for individuals while maintaining the sanctity of their personal spaces (Kua et al, 2023).

Hussain & Qi (2018) propose a framework that employs asymmetric encryption when transmitting data from the Home Area Network (HAN) to external networks, ensuring secure communication and access only by authorized parties. Asymmetric encryption uses a private key to encrypt and decrypt messages, adding an extra layer of security to the exchange between devices and external actors like users or Smart Home Operators (SHOs). To further enhance security, the framework combines hashing functions to generate unique tokens with both symmetric and asymmetric encryption methods, establishing a multi-layered approach that aims to fortify the system against potential intruders and unauthorized access. In this way, the proposed framework demonstrates a comprehensive approach to preserving privacy in smart home environments, helping mitigate risks associated with data breaches and unauthorized access while enabling secure interactions between smart home components and external entities.

Du et al., (2023) stress that a combination of privacy-preserving techniques should be implemented in the context of smart home environments. To this end, strict access controls allow users to manage who can access their data by setting permissions and restrictions, while strong user authentication methods such as passwords, biometrics, or two-factor authentication prevent unauthorized access to sensitive information. Moreover, regular software updates and security patches for smart home devices address vulnerabilities that could be exploited to compromise data privacy. In this sense, conducting privacy impact assessments such as DPIA (Data Protection Impact Assessment) helps identify potential risks associated with smart home applications, enabling proactive mitigation measures to safeguard user privacy. Further, transparency and explicit consent are also essential as smart home applications clearly communicating the data they collect and obtaining user approval before gathering personal information.

Yang et al., (2024) present a comparative overview of different methods for privacy preservation in human activity sensing, including signal, algorithm, and system-level approaches. The study highlights the importance of maintaining privacy while ensuring effective sensing and recognition, and compares the advantages and disadvantages of each method in the context of human activity sensing. This comparative analysis provides valuable

insights into the trade-offs between privacy protection and sensing accuracy, helping researchers and practitioners make informed decisions when selecting appropriate privacy-preserving techniques. These methods can be summarized as follows:

- Signal-level privacy-preserving techniques aim to change or filter the sensed signals to remove private information, preventing eavesdropping and unauthorized recording. These methods work by modifying the signals to obscure sensitive data, such as using ultrasonic devices to stop speech from being recorded secretly. However, it is important to balance privacy protection with the accuracy of activity sensing, as altering the signals can potentially affect the quality of the data.
- Algorithm-level privacy-preserving methods focus on modifying the algorithms used in human activity sensing to protect sensitive data and ensure that the sensed information is kept private and not shared with external parties. These techniques are crucial in scenarios where individual human activity data should not be exposed, such as in healthcare or personal settings. By incorporating privacy-preserving algorithms, the risk of sensitive data leakage can be mitigated.
- System-level privacy-preserving techniques are designed to safeguard private information shared during collaborative human sensing. The primary goal is to prevent any leakage of sensitive data while collaborating on obtaining recognition models. These methods help maintain the privacy of user data in scenarios where collaborative sensing is required for improved performance, such as in smart home environments. By implementing system-level privacy preservation, the benefits of collaborative sensing can be realized while ensuring the protection of individual privacy.

From another perspective, Rivadeneira et al., (2023) proposes user-centric mechanisms for preserving privacy in IoT environments in order to empower individuals to control and protect their data. In this environment, intermediary systems or privacy mediators serve as transparent mechanisms and platforms, enabling users to regain control over their personal information. Then the user-centric solutions recognize that effective privacy preservation requires not only technical safeguards, but also user agency and informed decision-making. Overcoming the Privacy Paradox, where users express concerns about privacy but engage in risky behaviours, necessitates a holistic approach. In addition to

implementing robust technical solutions, educating users about privacy risks and data recipient intentions is crucial. Informed decision-making by users requires understanding both the benefits of sharing data and the potential privacy hazards. By fostering user awareness and providing transparent control mechanisms, user-centric privacy preservation approaches in IoT environments can help bridge the gap between user concerns and actual behaviours. Ultimately, user-centric privacy preservation is essential for building trust in IoT technologies and ensuring that individuals feel empowered to reap the benefits of connected devices while maintaining control over their personal information. Intermediary systems and educational initiatives that prioritize user agency and informed consent represent a promising direction for addressing privacy challenges in the rapidly evolving smart home landscape.

5. Conclusions

The integration of AI and smart technologies in smart home environments offers immense potential for optimizing energy systems and enhancing efficiency, ultimately mitigating environmental impact. Nevertheless, the reliance on data and AI solutions also raises significant privacy concerns, pointing to the need for secure and ethical handling of resident data. The sensors employed in smart homes, the data communication protocols, and the AI systems used for energy consumption modelling and prediction must be carefully examined to ensure the safety, security, and privacy of residents and their data. Moreover, the evaluation of energy-saving strategies and behavioural change mechanisms in real-world settings is crucial. To strike a balance between technological innovation and responsible energy management, solutions must be robust, secure, and responsible, accounting for diverse usage patterns and behaviours. Hence, preserving privacy in smart home environments is essential, and this can be achieved through the development and deployment of privacy preserving solutions that safeguard resident data while enabling informed decision-making about energy use and conservation. By prioritizing privacy, the benefits of AI and smart technologies in energy management are realized while respecting the fundamental rights of individuals.

Hence, future perspectives could consider the development, deployment, and use of intelligent systems that can learn from resident data while minimizing the risk of privacy breaches, considering design user-centric privacy controls and transparency

mechanisms to build trust and empower individuals to manage their data sharing preferences, and evaluating the long-term impact of smart home energy management on privacy and behaviour through longitudinal studies to inform the design of more effective and privacy-preserving smart home technologies that promote sustainable energy practices while harnessing the power of AI to support and facilitate energy informed decision-making processes and mitigate environmental impact.

References

Archer, D. W., Pigem, B. D. B., Bogdanov, D., Craddock, M., Gascon, A., Jansen, R., ... & Wardley, S. (2023). UN Handbook on Privacy-Preserving Computation Techniques. *arXiv preprint arXiv:2301.06167*.

Basarir-Ozel, B., Nasir, V. A., & Turker, H. B. (2023). Determinants of smart home adoption and differences across technology readiness segments. *Technological Forecasting and Social Change*, *197*, 122924.

Chakraborty, A., Islam, M., Shahriyar, F., Islam, S., Zaman, H. U., & Hasan, M. (2023). Smart home system: a comprehensive review. *Journal of Electrical and Computer Engineering*, *2023*(1), 7616683.

do Canto, N. R., Grunert, K. G., & Dutra de Barcellos, M. (2023). Goal-framing theory in environmental behaviours: review, future research agenda and possible applications in behavioural change. *Journal of Social Marketing*, *13*(1), 20-40.

Du, H., Han, Q., Yang, D., de Vries, B., & van Houten, T. (2023). Data privacy and smart home energy appliances: A stated choice experiment. *Heliyon*, *9*(11).

EU Parliament (2020). The impact of GDPR on Artificial Intelligence.

European Union (2016). General Data Protection Regulation.

Fakhar, M. Z., Yalcin, E., & Bilge, A. (2023). A survey of smart home energy conservation techniques. *Expert Systems with Applications*, *213*, 118974.

Hussain, F., & Qi, M. (2018). Integrated privacy preserving framework for smart home. In *2018 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)* (pp. 1246-1253). IEEE.

Jhuang, Y. Y., Yan, Y. H., & Horng, G. J. (2023). GDPR Personal Privacy Security Mechanism for Smart Home System. *Electronics*, *12*(4), 831.

Kua, J., Hossain, M. B., Natgunanathan, I., & Xiang, Y. (2023). Privacy Preservation in Smart Meters: Current Status, Challenges and Future Directions. *Sensors*, *23*(7), 3697.

Panwar, N., Sharma, S., Mehrotra, S., Krzywiecki, Ł., & Venkatasubramanian, N. (2019). Smart home survey on security and privacy. *arXiv preprint arXiv:1904.05476*.

Pandiyan, P., Saravanan, S., Usha, K., Kannadasan, R., Alsharif, M. H., & Kim, M. K. (2023). Technological advancements toward smart energy management in smart cities. *Energy Reports*, *10*, 648-677.

Piasecki, S., & Chen, J. (2022). Complying with the GDPR when vulnerable people use smart devices. *International Data Privacy Law*, *12*(2), 113-131.

Rivadeneira, J. E., Silva, J. S., Colomo-Palacios, R., Rodrigues, A., & Boavida, F. (2023). User-centric privacy preserving models for a new era of the Internet of Things. *Journal of Network and Computer Applications*, 103695.

Rock, L. Y., Tajudeen, F. P., & Chung, Y. W. (2024). Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective. *Universal access in the information society*, *23*(1), 345-364.

Whitmarsh, L., Poortinga, W., & Capstick, S. (2021). Behaviour change to address climate change. *Current Opinion in Psychology*, *42*, 76-81.

Yang, Y., Hu, P., Shen, J., Cheng, H., An, Z., & Liu, X. (2024). Privacy-preserving human activity sensing: A survey. *High-Confidence Computing*, 100204.