Avances en Interacción Humano-Computadora, 2023, Año 8, No. 1, pp. 24-29
http://doi.org/10.47756/aihc.y8i1.133

RESEARCH PAPER

Towards the design of personal data protection-aware artificial intelligence applications in ubiquitous smart environments

Elba A. Morales-Vanegas, Beatriz Alexa Álvarez Magallán, Laura S. Gaytán-Lugo and Pedro C. Santana-Mancilla *

Published: 30 November 2023

Abstract
Protecting personal data in ubiquitous smart environments is crucial to ensure user privacy and trust in artificial intelligence (AI) applications. This paper explores approaches and techniques for designing privacy-aware and respectful AI applications where the balance between technological innovation and data protection is essential to ensure these technologies' ethical and sustainable adoption.

Keywords
Personal data protection; Privacy; Personal data protection-awareness; Artificial intelligence; Ubiquitous smart environments.

1 Introduction
In the present digital era, smart environments are no longer just a futuristic idea but a reality. These surroundings, ranging from automated homes to intelligent transportation systems, have the potential to enhance our daily lives significantly [6, 7, 13, 25]. However, this technological advancement also poses significant challenges in ensuring privacy and protecting personal data.

Integrating AI into daily life can be seen in smart home devices. These devices learn the user's behavior patterns, leading to the optimization of functions such as energy efficiency [2]. Similarly, intelligent transportation systems utilize real-time data to improve urban mobility and adapt to individual needs and preferences [17]. However, the collection of personal data by these systems raises significant concerns. For instance, home voice assistants may record private conversations [9], and health tracking devices collect sensitive personal information about the user's physical and medical condition [29].

Morales-Vanegas, Elba A., Álvarez-Magallán, Beatriz Alexa, Santana-Mancilla, Pedro C.*
Universidad de Colima
Colima, Mexico
Email: [abigail_morales, balvarez3, psantana @ucol.mx]

Gaytán-Lugo, Laura S.
Universidad de Colima
Coquimatlán, Mexico
Email: [laura@ucol.mx]

The scenarios mentioned above illustrate the difficulties that exist about privacy and security. Data breaches on smart devices serve as a reminder of the associated risks that come with improper handling of sensitive personal information. In addition, users need to be better informed and give their consent on how their data is collected, stored, and used. Many users should be aware of their devices' privacy policies and understand the extent of the consent they are granting.

These challenges regarding the risks of AI extend beyond the surface level. These issues have deep ethical and social implications. Widespread technological surveillance has the potential to impact human behavior significantly, and insufficient privacy management can lead to a loss of trust in technology, affecting its adoption and overall perception.

Given this context, this paper delves into the proactive design of AI applications in smart environments to ensure personal data protection awareness. We aim to examine existing challenges and suggest practical solutions that strike a balance between AI technological advancements and users' privacy and security.

2 Privacy challenges in ubiquitous smart environments
Ubiquitous intelligent environments have intrinsic characteristics predisposing them to privacy and data protection issues. To fully comprehend the nature and magnitude of these challenges, it is essential to delve into their particularities. Next, we describe the primary challenges (see Figure 1) that such environments face.

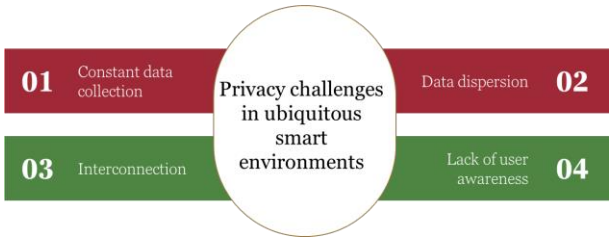

Figure 1. Smart environments privacy challenges.

2.1 Constant data collection
Smart environments are equipped with sensors and devices that collect data at a high level of detail [33]. For instance, a motion sensor in a smart home can detect an individual's presence and track specific movement patterns and daily routines. This ongoing data

collection can generate susceptible and personal information, such as audio recordings of conversations and precise biometric data [12].

The continual nature of this data collection can lead to the creation of comprehensive user profiles, potentially infringing upon their privacy by revealing intimate details of their daily lives.

2.2 Data dispersion

Nowadays, data is being collected from various devices, which leads to storing it in multiple and different locations. The locations can range from internal servers to external cloud infrastructures [3].

This fragmentation makes managing the data complex, increasing the risk of potential security breaches [30]. For instance, the synchronization of data across different platforms can result in difficulties in tracking and controlling data access, raising concerns about unauthorized use or exposure.

Furthermore, there are often different standards or protocols used due to the multiplicity of devices and operating systems in a ubiquitous context, thus creating possible gaps or overlaps in information protection.

2.3 Interconnection

Interconnectedness is a crucial characteristic of these environments, paradoxically expanding the possibility of attacks [10]. If intruders compromise a single device, they could gain access to the core system, compromising its integrity.

The constant data exchange between devices multiplies the opportunities for interceptions or manipulations of transmissions. The lack of standardized security protocols across diverse devices and systems creates additional vulnerabilities in the network [4].

Additionally, these systems rely on connectivity, which means that any interruption or weakness in the network could endanger the operation and the security and confidentiality of the information.

2.4 Lack of user awareness

Users typically have a passive attitude toward interacting with digital environments [22]. It means they often need to be constantly informed about the amount and nature of data being collected about them. The complexity and lack of clarity in privacy policies and terms of service contribute significantly to this unawareness [20].

Additionally, many devices are released to the market with default privacy settings that only sometimes prioritize maximum security and privacy. This reality, combined with a lack of awareness, can lead users to fail the need to customize these settings to protect their personal data adequately [31].

Table 1 provides a concise overview of the main challenges emerging in personal data protection within ubiquitous smart environments, describing their implications and proposing viable solutions.

Table 1. Main challenges in personal data protection.

Challenge	Description	Solutions
Constant data collection	Devices continuously gather data, potentially invading privacy by revealing personal details.	Implement strict data minimization principles and user consent mechanisms.
Data dispersion	Data is spread across various devices and locations, complicating management and increasing breach risks.	Develop unified data management systems with strong encryption and access controls.
Interconnection	Devices are interconnected, expanding attack surfaces and complicating data security.	Standardize security protocols across devices to prevent unauthorized access.
Lack of user awareness	Users are often unaware of the extent of data collection, leading to potential privacy risks.	Increase transparency and user control over data, and enhance privacy settings.

Ubiquitous smart environments undoubtedly have immense potential to enhance our quality of life and operational efficiency. However, they also pose significant data protection and privacy challenges. A comprehensive approach is necessary to overcome these challenges, including data protection-aware design, the implementation of rigorous standards, and user education focusing on security and privacy.

3 Data protection-aware design

In the contemporary era of ubiquitous intelligent environments, designing AI applications that primarily consider personal data privacy is imperative to safeguard the rights and dignity of users. In this context, it is crucial to outline various strategies to achieve a genuinely privacy-friendly design.

3.1 Data minimization

It is essential to selectively collect data, meaning you should only collect some of the data you can access [28]. For example, an application designed to control the lighting of a room does not need access to audio recordings. The concept of privacy by design [27] emphasizes the importance of collecting only the necessary data for a defined purpose. In addition, it is crucial to consider how long you retain the data. Keeping information beyond its usefulness can increase the risk of exposure. Therefore, implementing explicit retention policies and ensuring timely deletion of obsolete data is essential to minimize vulnerability.

3.2 Depersonalization (anonymity)

Data should be depersonalized by deleting or modifying personal identifiers to protect privacy [24]. It ensures that the collected information cannot be traced back to a specific individual. Aggregating the data enables general conclusions to be drawn, which dilutes specific details and safeguard individual identity.

3.3 Active consent

Being transparent about data collection is crucial. Users must be fully informed about what data is being collected, why it is being

collected, and how long it will be stored [19]. The communication about data collection should be transparent and accessible. An opt-in approach is the best way to collect data, where users can consent to collect specific information [5]. It is also important to periodically review and revalidate user consent, especially when the data's nature or purpose changes.

3.4 User control

It is of utmost importance to give users direct control over their data [11]. It can be achieved by providing them with tools to access, correct, and delete their personal information. The interface for these tools must be user-friendly and intuitive. Furthermore, it is essential to offer personalized configuration options, giving users the autonomy to determine the privacy parameters that best suit their preferences [23]. In addition, the service providers are responsible for keeping users informed about any events related to their data, such as potential data breaches or modifications to privacy policies.

Table 2 shows how each challenge can be solved using design techniques with data protection awareness.

Table 2. Design techniques solutions to challenges.

Challenge	Design techniques
Constant data collection	Data Minimization; Depersonalization (Anonymity).
Data dispersion	Data Minimization; Active Consent.
Interconnection	User Control; Active Consent.
Lack of user awareness	Depersonalization (Anonymity); User Control.

Privacy cannot be considered a mere addition when designing applications for ubiquitous smart environments. It must be at the core of the design process. This approach guarantees that users' data is protected and valued beyond the tangible benefits of technology. A strong emphasis on privacy is essential to build trust and ensure the durability of these groundbreaking technological advances.

4 AI techniques for personal data protection-awareness

AI poses a unique challenge regarding personal data protection [16]. Since AI algorithms require large datasets for training and inference, it becomes essential to reconsider traditional privacy practices [21]. However, several techniques have emerged as promising solutions to this issue. These techniques focus on balancing the data processing requirements of AI while ensuring that privacy concerns are addressed.

4.1 Differentially private learning

Differentially private learning involves adding controlled noise to data before processing it [8]. This technique ensures that the results of machine learning models or any derived conclusions do not reveal specific information about individual records, thus maintaining their privacy [37]. The advantage of this method is that it allows entities to create AI models without directly accessing the original data, thus protecting individual privacy [35]. However, balancing the amount of noise introduced and the model's performance can be challenging. If too much noise is added, it could reduce the model's accuracy.

4.2 Federated learning

Federated learning proposes a decentralized approach to the training process [14]. Instead of centralizing data to a single point, this methodology allows models to be trained directly on the user's device. Only model updates, not the data, are sent to the central server. This approach ensures that personal data remains on the user's device, thus minimizing the risks associated with transmitting or storing information on central servers [26]. However, this process requires more advanced algorithms and can face efficiency challenges, particularly when synchronizing models between different devices [18].

Regarding data processing and privacy, there are significant differences between federated and centralized learning. Federated learning processes data directly on the user's device, while centralized learning relies on consolidating data at a central server. With federated learning, data remains on the user's device, resulting in higher privacy. In contrast, centralized learning poses a greater risk to data privacy due to data centralization. However, while centralized learning is often more efficient due to the use of powerful centralized servers, federated learning may be less efficient due to the limitations of individual devices. For a more comprehensive comparison between the two approaches, please refer to Table 3.

Federated learning offers higher data security as it reduces the need for data transmission instead of centralized learning, which increases the risk associated with transmitting large amounts of data. Additionally, federated learning algorithms tend to be more complex, requiring synchronization across multiple devices, while centralized learning is less complex because of its centralized control. The table below illustrates the trade-offs between these approaches regarding data handling, privacy, efficiency, security, and algorithmic complexity.

Table 3. Comparison federated vs centralized learning.

Aspect	Federated learning	Centralized learning
Data location	User’s device	Central server
Privacy	Higher (data remains on device)	Lower (data centralized)
Efficiency	Can be lower due to device limitations	Typically, higher (powerful centralized servers)
Data security	Higher (reduced data transmission)	Lower (increased data transmission)
Algorithm complexity	More complex (requires synchronization)	Less complex (centralized control)

4.3 Homomorphic encryption

Homomorphic encryption [36] is a cutting-edge technique that enables operations to be carried out on encrypted data without requiring it to be decrypted first. This approach has great potential in AI, as it could allow models to analyze and make predictions on encrypted data without compromising its privacy [1]. This methodology reduces the chances of data breaches and ensures higher security by eliminating the need to decrypt data during processing. However, due to its complex nature, homomorphic encryption comes with a high computational cost and tends to be slower than operations on unencrypted data [15]. Researchers are

currently exploring ways to optimize the efficiency of these algorithms to make them more practical for real-world applications.

4.4 Zero-knowledge proofs

Zero-knowledge proofs are a cryptographic technique that allows one entity to prove the truth of a claim to another entity without revealing any additional information beyond the certainty of the claim itself [34]. This mechanism can verify the accuracy of calculations or the possession of specific data without disclosing the underlying information [32]. Although this technique is promising, its practical implementation is still in progress and requires significant computational capacity [38].

AI applications require a vast amount of data to function efficiently. However, the techniques presented here offer promising solutions to process this data while respecting privacy parameters. With advancements in technology and regulations, we can expect the emergence of new strategies and techniques that strike a balance between the demands of AI and the responsibilities associated with personal data protection.

5 Discussion

The paper analyzes the challenges, techniques, and algorithmic solutions for protecting personal data in ubiquitous smart environments, particularly AI-driven applications. The constant collection, dispersion, and interconnection of data and a lack of user awareness pose significant privacy risks. However, they also provide opportunities for innovative solutions. Data minimization, depersonalization, active consent, and user control are not just solutions but also fundamental principles that should guide the development of AI applications in these environments. Their practical implementation requires a careful balance between usability and privacy, highlighting the need for personal data protection-aware designs.

AI techniques such as differentially private learning, federated learning, homomorphic encryption, and zero-knowledge proofs are being evaluated to address privacy concerns. Each technique has its unique approach to handling data and ensuring privacy, highlighting the potential of AI to operate within strict data protection norms. However, these techniques pose challenges, such as computational efficiency, algorithm complexity, and balancing data utility and privacy. These challenges indicate areas of ongoing research and development.

Finding a balance between the impact of regulations and policies on emerging technologies is crucial. Although current data protection laws such as the General Data Protection Regulation (GDPR) or the Mexican data protection norms (Ley Federal de Protección de Datos Personales en Posesión de los Particulares and Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados) lay a foundation, regulatory frameworks need to evolve as AI technologies advance. Therefore, policymaking should be proactive in predicting future developments and creating guidelines that protect individual privacy while promoting technological innovation.

Discussions about proposed solutions to technical and implementation challenges are often complicated by real-world issues such as scalability, computational demands, and integration complexities. While these solutions may be theoretically sound, addressing these challenges requires collaboration across multiple disciplines, including computer science, law, ethics, and design.

The future of personal data protection in smart environments is likely to be influenced by various emerging trends. These include the growing use of AI in everyday devices, advancements in encryption technologies, and an increasing public awareness of privacy issues. Continuous research will be essential to stay ahead in this dynamic field. Ethical and legal considerations will also play a crucial role in shaping the future of personal data protection in smart environments.

This paper serves as a call to action for the research community to foster further exploration and development of AI technologies that respect and protect personal data privacy. The balancing act between technological innovation and data protection is a complex but necessary endeavor, essential for the responsible advancement of AI in our increasingly connected world.

6 Conclusion

Smart environments are everywhere, from homes to cities, and they have the potential to improve our lives and make everyday tasks more efficient. However, these environments rely on data, which risks our privacy and personal information. It is important to prioritize user privacy by implementing data protection-awareness designs to address this issue. Data minimization, depersonalization, active consent, and data management tools can help protect user rights in smart environments. In artificial intelligence, adopting techniques such as differentially private learning, federated learning, homomorphic encryption, and zero-knowledge proofs can further ensure that data is processed without compromising privacy. As a research community, it is essential to proactively address these challenges to ensure that the promises of smart environments are realized in an ethical, sustainable, and respectful manner that defends the human right to privacy.

7 Acknowledgments

We want to express our gratitude to the Consejo Nacional de Humanidades, Ciencias y Tecnología (CONAHCYT) for the financial support through the Beatriz Alexa Álvarez Magallán (CVU 1242722) scholarship.

8 References

[1] Acar, A., Aksu, H., Uluagac, A.S. and Conti, M. 2019. A Survey on Homomorphic Encryption Schemes: Theory and Implementation. *ACM Computing Surveys*. 51, 4 (Jul. 2019), 1–35. DOI:https://doi.org/10.1145/3214303.

[2] Asem Alzoubi 2022. MACHINE LEARNING FOR INTELLIGENT ENERGY CONSUMPTION IN SMART HOMES. *International Journal of Computations, Information and Manufacturing (IJCIM)*. 2, 1 (May 2022). DOI:https://doi.org/10.54489/ijcim.v2i1.75.

[3] Balcan, M.-F., Dick, T. and Vitercik, E. 2018. Dispersion for Data-Driven Algorithm Design, Online Learning, and Private Optimization. arXiv.

[4] Catuogno, L. and Turchi, S. 2015. The Dark Side of the Interconnection: Security and Privacy in the Web of Things. *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (Santa Cantarina, Brazil, Jul. 2015), 205–212.

[5] Clemens, N.A. 2012. Privacy, Consent, and the Electronic Mental Health Record: The Person vs. the System. *Journal of Psychiatric Practice*. 18, 1 (Jan. 2012), 46–50. DOI:https://doi.org/10.1097/01.pra.0000410987.38723.47.

[6] Da Rosa Tavares, J.E. and Victória Barbosa, J.L. 2020. Ubiquitous healthcare on smart environments: A systematic mapping study. *Journal of Ambient Intelligence and Smart Environments*. 12, 6 (Nov. 2020), 513–529. DOI:https://doi.org/10.3233/AIS-200581.

[7] Fantin Irudaya Raj, E. and Appadurai, M. 2022. Internet of Things-Based Smart Transportation System for Smart Cities. *Intelligent Systems for Social Good*. S. Mukherjee, N.B. Muppalaneni, S. Bhattacharya, and A.K. Pradhan, eds. Springer Nature Singapore. 39–50.

[8] Gong, M., Xie, Y., Pan, K., Feng, K. and Qin, A.K. 2020. A Survey on Differentially Private Machine Learning [Review Article]. *IEEE Computational Intelligence Magazine*. 15, 2 (May 2020), 49–64. DOI:https://doi.org/10.1109/MCI.2020.2976185.

[9] Hernández Acosta, L. and Reinhardt, D. 2022. A survey on privacy issues and solutions for Voice-controlled Digital Assistants. *Pervasive and Mobile Computing*. 80, (Feb. 2022), 101523. DOI:https://doi.org/10.1016/j.pmcj.2021.101523.

[10] Katewa, V., Anguluri, R. and Pasqualetti, F. 2021. On a security vs privacy trade-off in interconnected dynamical systems. *Automatica*. 125, (Mar. 2021), 109426. DOI:https://doi.org/10.1016/j.automatica.2020.109426.

[11] Kreuter, F., Haas, G.-C., Keusch, F., Bähr, S. and Trappmann, M. 2020. Collecting Survey and Smartphone Sensor Data With an App: Opportunities and Challenges Around Privacy and Informed Consent. *Social Science Computer Review*. 38, 5 (Oct. 2020), 533–549. DOI:https://doi.org/10.1177/0894439318816389.

[12] Kröger, J.L., Gellrich, L., Pape, S., Brause, S.R. and Ullrich, S. 2022. Personal information inference from voice recordings: User awareness and privacy concerns. *Proceedings on Privacy Enhancing Technologies*. 2022, 1 (Jan. 2022), 6–27. DOI:https://doi.org/10.2478/popets-2022-0002.

[13] Li, J., He, Z., Cui, Y., Wang, C., Chen, C., Yu, C., Zhang, M., Liu, Y. and Ma, S. 2022. Towards Ubiquitous Personalized Music Recommendation with Smart Bracelets. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 6, 3 (Sep. 2022), 1–34. DOI:https://doi.org/10.1145/3550333.

[14] Li, L., Fan, Y., Tse, M. and Lin, K.-Y. 2020. A review of applications in federated learning. *Computers & Industrial Engineering*. 149, (Nov. 2020), 106854. DOI:https://doi.org/10.1016/j.cie.2020.106854.

[15] Martins, P., Sousa, L. and Mariano, A. 2018. A Survey on Fully Homomorphic Encryption: An Engineering Perspective. *ACM Computing Surveys*. 50, 6 (Nov. 2018), 1–33. DOI:https://doi.org/10.1145/3124441.

[16] Meurisch, C. and Mühlhäuser, M. 2022. Data Protection in AI Services: A Survey. *ACM Computing Surveys*. 54, 2 (Mar. 2022), 1–38. DOI:https://doi.org/10.1145/3440754.

[17] Miao, Y., Yang, Y., Li, X., Choo, K.-K.R., Meng, X. and Deng, R.H. 2023. Comprehensive Survey on Privacy-Preserving Spatial Data Query in Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*. (2023), 1–14. DOI:https://doi.org/10.1109/TITS.2023.3295798.

[18] Nilsson, A., Smith, S., Ulm, G., Gustavsson, E. and Jirstrand, M. 2018. A Performance Evaluation of Federated Learning Algorithms. *Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning* (Rennes France, Dec. 2018), 1–8.

[19] Noain-Sánchez, A. 2016. "Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy. *Journal of Information, Communication and Ethics in Society*. 14, 2 (May 2016), 124–138. DOI:https://doi.org/10.1108/JICES-10-2014-0040.

[20] Nyoni, P. and Velempini, M. 2018. Privacy and user awareness on Facebook. *South African Journal of Science*. 114, 5/6 (May 2018), 5. DOI:https://doi.org/10.17159/sajs.2018/20170103.

[21] Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z. and Vasilakos, A. 2021. Security and Privacy for Artificial Intelligence: Opportunities and Challenges. arXiv.

[22] Pötzsch, S. 2009. Privacy Awareness: A Means to Solve the Privacy Paradox? *The Future of Identity in the Information Society*. V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda, eds. Springer Berlin Heidelberg. 226–236.

[23] Price, B.A., Adam, K. and Nuseibeh, B. 2005. Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *International Journal of Human-Computer Studies*. 63, 1–2 (Jul. 2005), 228–253. DOI:https://doi.org/10.1016/j.ijhcs.2005.04.008.

[24] Primenko, D.V., Spevakov, A.G. and Spevakova, S.V. 2020. Depersonalization of Personal Data in Information Systems. *Advances in Automation*. A.A. Radionov and A.S. Karandaev, eds. Springer International Publishing. 763–770.

[25] Rao, G.K.L. and Mokhtar, N. 2023. Dental Education in the Information Age: Teaching Dentistry to Generation Z Learners Using an Autonomous Smart Learning Environment. *Advances in Medical Education, Research, and Ethics*. M.B. Garcia, M.V. Lopez Cabrera, and R.P.P. De Almeida, eds. IGI Global. 243–264.

[26] Rieke, N. et al. 2020. The future of digital health with federated learning. *npj Digital Medicine*. 3, 1 (Sep. 2020), 119. DOI:https://doi.org/10.1038/s41746-020-00323-1.

[27] Schaar, P. 2010. Privacy by Design. *Identity in the Information Society*. 3, 2 (Aug. 2010), 267–274. DOI:https://doi.org/10.1007/s12394-010-0055-x.

[28] Senarath, A. and Arachchilage, N.A.G. 2019. A data minimization model for embedding privacy into software systems. *Computers & Security*. 87, (Nov. 2019), 101605. DOI:https://doi.org/10.1016/j.cose.2019.101605.

[29] Singh, S., Rathore, S., Alfarraj, O., Tolba, A. and Yoon, B. 2022. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*. 129, (Apr. 2022), 380–388. DOI:https://doi.org/10.1016/j.future.2021.11.028.

[30] Song, H., Li, J. and Li, H. 2021. A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption. *IEEE Access*. 9, (2021), 63745–63751. DOI:https://doi.org/10.1109/ACCESS.2021.3075340.

[31] Soumelidou, A. and Tsohou, A. 2021. Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness. *Telematics and Informatics*. 61, (Aug. 2021), 101592. DOI:https://doi.org/10.1016/j.tele.2021.101592.

[32] Sun, X., Yu, F.R., Zhang, P., Sun, Z., Xie, W. and Peng, X. 2021. A Survey on Zero-Knowledge Proof in Blockchain. *IEEE Network*. 35, 4 (Jul. 2021), 198–205. DOI:https://doi.org/10.1109/MNET.011.2000473.

[33] Thompson, S.A. and Warzel, C. 2022. Twelve Million Phones, One Dataset, Zero Privacy. *Ethics of Data and Analytics*. Auerbach Publications. 161–169.

[34] Tomaz, A.E.B., Nascimento, J.C.D., Hafid, A.S. and De Souza, J.N. 2020. Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof and Blockchain. *IEEE Access*. 8, (2020), 204441–204458. DOI:https://doi.org/10.1109/ACCESS.2020.3036811.

[35] Wang, J. and Zhou, Z.-H. 2020. Differentially Private Learning with Small Public Data. *Proceedings of the AAAI Conference on Artificial Intelligence*. 34, 04 (Apr. 2020), 6219–6226. DOI:https://doi.org/10.1609/aaai.v34i04.6088.

[36] Yi, X., Paulet, R. and Bertino, E. 2014. Homomorphic Encryption. *Homomorphic Encryption and Applications*. Springer International Publishing. 27–46.

[37] Yu, L., Liu, L., Pu, C., Gursoy, M.E. and Truex, S. 2019. Differentially Private Model Publishing for Deep Learning. *2019 IEEE Symposium on Security and Privacy (SP)* (San Francisco, CA, USA, May 2019), 332–349.

[38] Zhang, J., Xie, T., Zhang, Y. and Song, D. 2020. Transparent Polynomial Delegation and Its Applications to Zero Knowledge Proof. *2020 IEEE Symposium on Security and Privacy (SP)* (San Francisco, CA, USA, May 2020), 859–876.