Internet of Things (IoT)

Giordano et al. (2022) surveyed the use of AI techniques that implement privacy in IoT systems. The authors pose several research questions that handle this issue and focus on algorithms, datasets, strategies, techniques and evaluation of AI in IoT privacy. For each of these aspects, the authors extracted relevant data from different research papers and organized this literature according to several dimensions that include privacy, ML algorithms, topics of interest programming language, training strategy, validation techniques, dataset, evaluation metrics, and limitations. Through the prospect of these assignments, once they had identified the final set of sources to consider, they extracted the information relevant to address the research questions. Elhoseny et al. (2021) suggested an IoT solution for AI-enabled privacy-preserving for big data transferring using blockchain. They developed a system for gathering and transmitting data that uses AI for efficient services in the healthcare system. In their research they utilized symmetric-based digital certificates for confidential transmission with communication resources using blockchain. Credibility was enhanced by means of a cloud platform. In addition, they ensured integrity by incorporating blockchain technology in distribution development. They tested and analyzed the results by simulations and showed that the AI algorithm outperforms existing solutions with consistent and sustainable communication. Their proposed algorithm was explored with existing solutions via multiple simulations and the results demonstrate improvement in terms of realistic parameters. Xiao, Wan, Lu, Zhang, and Wu (2018) presented IoT security techniques based on ML. The authors researched the attack model for IoT systems, reviewed IoT security solutions based on ML techniques such as supervised learning, unsupervised learning, and reinforcement learning. They also focus on ML-based IoT authentication, access control, secure offloading, and malware detection schemes to protect data privacy, and discuss the implementation of these ML-based security schemes in practical IoT systems. One of the important conclusions presented in the paper is that ML-based security schemes assume that each learning agent knows the accurate state and evaluates the immediate reward for each action in time and needs to tolerate the bad strategies. Usually, it is difficult for IoT devices to accurately assess the network and attack state, thus this should be avoided at the beginning of the learning process. The authors suggest the solution of Transfer Learning, which explores existing defense experiences with data mining to reduce random exploration, accelerates the learning speed, and decreases the risks of choosing bad defense policies at the beginning of the learning process. Liu, Huang, Yan, Wang, and Zhang (2022) discuss the growing importance of privacy and personal information protection in the context of smart speakers in China. Yan et al. applied a socio-technical system framework to analyze the interactions between the technology, industry/market and law/regulation subsystems, and regulators.

Chinese brands dominate the global smart speaker market and collect user data, making privacy a crucial issue. The study analyzes the laws and regulations related to privacy and personal information protection, with focus on the potential impact of the Personal Information Protection Law (PIPL) on smart speakers. The study also includes focus group discussions that highlight user concerns about privacy and the industry's implementation of personal information protection. The participants expressed concerns about disruption to privacy, unequal policies, information collection practices, and data security. They relied on legislation and government regulation to address their concerns. The PIPL and other related laws play an important role in protecting personal information and balancing the interests of industry, individuals, and the nation. However, there are recommendations to establish a unified regulator to oversee personal information protection more effectively. Overall, China's legislative efforts align with global trends and aim to balance industrial development with personal information protection. Jin et al. (2018) discuss the problems that emerge as a result of AI regarding consumer privacy and data security due to its use of big data that may be

considered private. The nature of the problem is that both buyers and sellers have an incentive to hide or reveal private information, which is crucial for market efficiency, and is implemented by IoT devices. In the context of a single transaction, less privacy is not necessarily bad for economic efficiency. Data technology that reveals the consumer type could facilitate a better match between the product and the consumer, and data technology that helps buyers assess product quality could encourage high-quality production. The privacy problem which has worsened consequently to technological advances have enabled a substantial decline in the cost of collecting, storing, processing, and using data in mass quantities. Big data refers to large volumes of transaction data that can potentially reveal details about individual consumers. Big data as input in modern AI algorithms assists in understanding, predicting, and influencing consumer behavior, and when used by legitimate companies, it could improve management efficiency, motivate innovations, and better match demand and supply. However, when it is in the wrong hands it can also create a greater chance for fraud, deception and privacy invasions. Manheim and Kaplan (2019) discussed various risks that artificial intelligence poses with reference to privacy, democracy, and other democratic values. They considered threats from data collection and use enabled by technologies such as IoT. They also examined how AI could undermine decisional privacy and autonomy through online behavioral advertising. Other topics that they investigated include threats to elections from hacking and manipulation enabled by AI, as well as issues of opacity, bias, and the lack of explaining abilities in AI systems. The authors propose various responses that governments could take to regulate AI and balance its development while minimizing risks. Tschider (2018) discussed the lack of adequate legal frameworks and regulations for consumers' IoT devices. He described the rapid growth of the IoT market and issues concerning discrimination, privacy, security, and ineffective notice and consent models posed by IoT devices. He explored existing regulations in areas like healthcare, children's privacy, and finance that may provide some guidance. He analyzed policy approaches and considerations for developing a regulatory framework for IoT, including balancing market flexibility with consumer protections. The key areas for regulation that he mentioned included discrimination, privacy, cybersecurity, and working towards a proposed model. Van den Hoven van Genderen (2017) explored the impact of AI and robotics on privacy and data protection. He discussed the challenges in controlling the integration of AI and robotics and the potential disintegration of traditional privacy concepts. He questioned the adequacy of existing data protection regulations like the GDPR in the AI era and examined the vulnerability of AI in processing personal data.

He also considered the societal implications of personal information sharing in an increasingly transparent and technologically advanced society, highlighting the need for legal and ethical frameworks to safeguard privacy in the face of pervasive AI and robotic technologies. Xiong, Zhao, Bhuiyan, Chen, and Tian (2019) proposed an AI-enabled three-party game (ATG) framework to guarantee data privacy in mobile edge crowdsensing (MECS) of IoT. The authors constructed a classification-anonymity (CA) model to protect sensitive data and a three-party game (TG) model to analyze data privacy leakage in MECS. The authors analyzed the Nash equilibrium between strategies and profits of entities in MECS using the CA and TG models. The numerical results show that the proposed framework effectively protects data privacy and is well-suited for MECS. Keshta (2022) discussed the integration of AI with IoT in healthcare, emphasizing the significant security and privacy concerns this convergence raises. The author highlighted the urgent need for well-defined architecture standards, including data models and interfaces, to enhance user security and privacy. Using a qualitative study design, he examined the evolution of AI-driven IoT (AIIoT) in healthcare, to identify key security challenges and recommend solutions that will ensure the privacy and security of users in smart healthcare systems. Sun, Liu, Wang, Cao, and Kato (2020) provided a comprehensive overview of the integration of ML and privacy considerations within the context of sixth generation (6G) communication networks. The authors explored the dual potential of ML to both enhance

privacy protection and pose new risks in 6G environments. The authors discussed the advancements and challenges in ensuring privacy in the face of evolving ML applications, highlighting the critical balance between leveraging ML for improved network performance and safeguarding user privacy. Sedenberg and Chuan (2017) examined the privacy and ethical concerns arising from the use of AI in emotional analysis. The authors delved into how emotional AI can manipulate individuals and impact societal norms by analyzing public emotions through digital means without explicit consent, highlighting the technology's ability to understand and utilize emotional data in various sectors, including security and advertising. The authors call for comprehensive policy and legal frameworks to address these privacy and ethical implications, emphasizing the need for transparency, public awareness, and regulatory measures to safeguard individual privacy in the age of emotion AI. Schiliro, Moustafa, and Beheshti (2020) introduced a model to protect cognitive privacy in EEG signal analysis. They propose an AI-enabled approach that uses long-short term memory (LSTM) in DL to classify and protect individual EEG data. Their model is aimed to secure cognitive information from unauthorized access while maintaining the ability to classify users and tasks based on EEG signals, thereby demonstrating the effectiveness in ensuring privacy in the analysis of brainwave data. Sachdev (2020) discussed the integration of Edge artificial intelligence (Edge AI) in digital marketing in the IoT and Internet of Everything (IoE) environments. He highlights the potential benefits of Edge computing in enhancing security and privacy for consumer data used in digital marketing. However, he also addresses the security and privacy challenges that arise with the implementation of Edge AI and proposes possible mitigation strategies for these issues. His research navigates the complex landscape of ensuring data protection while leveraging the advantages of Edge AI in digital marketing, emphasizing the importance of continuous evolution of security and privacy measures in this rapidly advancing field. Sugianto, Tjondronegoro, Stockdale, and Yuwono (2024) propose a system that utilizes AI to monitor social distancing measures in public areas while emphasizing privacy preservation. Their AI-enabled surveillance system integrates federated learning to process data directly on edge devices, reducing the need to transmit sensitive information to a central server, thus addressing major privacy concerns. The framework they developed, i.e., the Responsible AI Implementation Framework (RAIFF), ensures that AI operates under strict ethical and privacy standards throughout its deployment. The system's effectiveness and responsible design are demonstrated in a case study conducted at an airport, showcasing its capability to enhance public health measures without compromising individual privacy. Gao, Chen, Han, Wu, and Susilo (2023) focused on applying PPDM protection to data that was collected by IoT devices. These devices usually have limited storage space; therefore, data must be stored in a cloud, resulting in significant issues concerning privacy. The paper proposes an economic model to balance privacy protection and data mining performances. The approach is based on game theory. Awad et al. (2024) provide a comprehensive review of how AI enhances biometric authentication within IoT systems. It focuses on the integration of fingerprint and facial recognition technologies with AI to strengthen security, usability, and privacy across various IoT applications. The authors analyze the interdependencies between AI, biometrics, and the IoT, review state-of-the-art solutions and challenges, and propose future directions, especially in sectors like healthcare, smart cities, and industrial IoT. Yepuganti et al. (2021) present an IoT-based plant monitoring system designed to support mental health therapy by making gardening more interactive. Using sensors, Raspberry Pi, and cloud platforms, the system enables users to receive real-time notifications and interact with their plant via voice assistant, creating a personalized, therapeutic experience that fosters emotional well-being.

References

Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. *Journal of Information Security and Applications, 82*, 103748. doi:https://doi.org/10.1016/j.jisa.2025.104052

Elhoseny, M., Haseeb, K., Shah, A. A., Ahmad, I., Jan, Z., & Alghamdi, M. I. (2021). IoT solution for AI-enabled PRIVACY-PREServing with big data transferring: an application for healthcare using blockchain. *Energies, 14*(17), 5364. doi:https://doi.org/10.3390/en14175364

Gao, Y., Chen, L., Han, J., Wu, G., & Susilo, W. (2023). Iot privacy-preserving data mining with dynamic incentive mechanism. *IEEE Internet of Things Journal, 11*(1), 777--790. doi:https://doi.org/10.1109/JIOT.2023.3285894

Giordano, G., Palomba, F., & Ferrucci, F. (2022). On the use of artificial intelligence to deal with privacy in IoT systems: A systematic literature review. *Journal of Systems and Software, 193*, 111475. doi:https://doi.org/10.1016/j.jss.2022.111475

Jin, G. Z., & others. (2018). Artificial intelligence and consumer privacy. National Bureau of Economic Research. Retrieved from http://www.nber.org/papers/w24253

Keshta, I. (2022). AI-driven IoT for smart health care: Security and privacy issues. *Informatics in medicine Unlocked, 30*, 100903. doi:https://doi.org/10.1016/j.imu.2022.100903

Liu, Y.-l., Huang, L., Yan, W., Wang, X., & Zhang, R. (2022). Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. *Telecommunications Policy, 46*(7), 102334. doi:https://doi.org/10.1016/j.telpol.2022.102334

Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale JL & Tech., 21*(106). Retrieved from https://yjolt.org/artificial-intelligence-risks-privacy-and-democracy

Sachdev, R. (2020). Towards security and privacy for edge AI in IoT/IoE based digital marketing environments. *2020 fifth international conference on fog and mobile edge computing (FMEC)* (pp. 341--346). IEEE. doi:https://doi.org/10.1109/FMEC49853.2020.9144755

Schiliro, F., Moustafa, N., & Beheshti, A. (2020). Cognitive privacy: AI-enabled privacy using EEG signals in the internet of things. *2020 ieee 6th international conference on dependability in sensor, cloud and big data systems and application (dependsys)* (pp. 73--79). IEEE. doi:https://doi.org/10.1109/DependSys51298.2020.00019

Sedenberg, E., & Chuang, J. (2017). Smile for the camera: Privacy and policy implications of emotion AI. *arXiv preprint arXiv:1709.00396*. doi:https://doi.org/10.48550/arXiv.1709.00396

Sugianto, N., Tjondronegoro, D., Stockdale, R., & Yuwono, E. I. (2024). Privacy-preserving AI-enabled video surveillance for social distancing: Responsible design and deployment for public spaces. *Information Technology & People, 37*(2), 998--1022. doi:https://doi.org/10.1108/ITP-07-2020-0534

Sun, Y., Liu, J., Wang, J., Cao, Y., & Kato, N. (2020). When machine learning meets privacy in 6G: A survey. *IEEE Communications Surveys & Tutorials, 22*(4), 2694--2724. doi:https://doi.org/10.1109/COMST.2020.3011561

Tschider, C. A. (2018). Regulating the internet of things: discrimination, privacy, and cybersecurity in the artificial intelligence age. *Denv. L. Rev., 96*(87). Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/denlr96&div=6&id=&page=

Van den Hoven van Genderen, R. (2017). Privacy and data protection in the age of pervasive technologies in AI and robotics. *Eur. Data Prot. L. Rev., 3*(338). Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl3&div=62&id=&page=

Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine, 35*(5), 41--49. doi:https://doi.org/10.1109/MSP.2018.2825478

Xiong, J., Zhao, M., Bhuiyan, M. Z., Chen, L., & Tian, Y. (2019). An AI-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of IoT. *IEEE Transactions on Industrial Informatics, 17*(2), 922--933. doi:https://doi.org/10.1109/TII.2019.2957130

Yepuganti, k., Awasthi, S., & Sharma, R. (2021). IoT plant monitoring system for mental health therapy. *AI & Society*, 1--6. doi:https://doi.org/10.1007/s00146-020-01140-6