Law Studies and Justice Journal (LAJU)
Vol 1(1) 2024 : 15-24

Data Privacy and the Law: Balancing Security and Individual Rights

Privasi Data dan Hukum: Menyeimbangkan Keamanan dan Hak Individu

Amaliasyifa Agustina, Mutiara Oktavia Cahyania, Muhammad Syaoqibihillah
Universitas Indraprasta PGRI
*amaliasyifa.Agustina@unindra.ac.id, mutiaraoktavia15@gmail.com,syaoqibihillah@gmail.com

**Corresponding Author*

ABSTRACT
Data privacy regulations are undergoing significant changes in the face of challenges presented by technological advances, particularly in the context of artificial intelligence (AI) and the Internet of Things (IoT). This study describes the evolution of data privacy regulations, the challenges in adapting regulations to AI and IoT, and the implementation of data privacy regulations related to AI and IoT. In conducting this research, researchers used a systematic literature review method to identify and analyze the latest articles in relevant literature. The findings of this study show that efforts to adapt data privacy regulations to developments in new technologies such as AI and IoT introduce new complexities that demand innovative solutions. Nonetheless, this research highlights the potential of solutions such as Federated Learning (FL) and Blockchain integration with IoT in improving data security and privacy. The implications of this research include the importance of paying attention to flexible and adaptable regulations, as well as the need for collaborative efforts in facing increasingly complex data privacy challenges in the era of AI and IoT.
Keywords: Data privacy regulations, artificial intelligence, Internet of Things, evolution, systematic literature review, Federated Learning, Blockchain, data security, data privacy.

ABSTRAK
Regulasi privasi data mengalami perubahan yang signifikan dalam menghadapi tantangan yang dihadirkan oleh kemajuan teknologi, khususnya dalam konteks kecerdasan buatan (AI) dan Internet of Things (IoT). Studi ini menggambarkan evolusi regulasi privasi data, tantangan dalam mengadaptasi regulasi terhadap AI dan IoT, serta implementasi regulasi privasi data terkait AI dan IoT. Dalam melakukan penelitian ini, peneliti menggunakan metode systematic literature review untuk mengidentifikasi dan menganalisis artikel terbaru dalam literatur yang relevan. Temuan studi ini menunjukkan bahwa upaya untuk menyesuaikan regulasi privasi data dengan perkembangan teknologi baru seperti AI dan IoT menimbulkan kompleksitas baru yang menuntut solusi inovatif. Meskipun demikian, penelitian ini menyoroti potensi solusi seperti Federated Learning (FL) dan integrasi Blockchain dengan IoT dalam meningkatkan keamanan dan privasi data. Implikasi dari penelitian ini mencakup pentingnya memperhatikan regulasi yang fleksibel dan beradaptasi, serta perlunya upaya kolaboratif dalam menghadapi tantangan privasi data yang semakin kompleks dalam era AI dan IoT.
Kata Kunci: Regulasi privasi data, kecerdasan buatan, Internet of Things, evolusi, systematic literature review, Federated Learning, Blockchain, keamanan data, privasi data.

1. Introduction

Data privacy and the law pose a complex challenge in balancing security measures with individual rights. The emergence of technologies such as wiretapping, surveillance systems, and data encryption has raised concerns about privacy infringement and the necessity for legal frameworks to protect personal information (Natamiharja et al., 2022; Shifa et al., 2020). Legislation like the General Data Protection Regulation (GDPR) has played a crucial role in enhancing privacy rights and establishing new standards for data management (Gao et al., 2021). However, the enforcement of such laws demands a careful equilibrium to ensure the preservation of both security and individual rights.

Copyright © 2024 THE AUTHOR(S). This article is distributed under a a Creative Commons Attribution-NonCommercial 4.0 International license.

In the realm of research, privacy and security issues surface, especially in areas like citizen science and health research applications. The ethical and privacy principles that govern data access and usage are vital in upholding confidentiality and respecting individuals' privacy rights (Evans, 2020; Tovino, 2020). Moreover, the utilization of mobile applications in research environments requires adherence to data protection laws to prevent privacy breaches (Tovino, 2020). The convergence of privacy, security, and public health safety has become more prominent, particularly during crises like pandemics. The trade-off between privacy, public health safety, and digital security underscores the significance of transparency and accountability measures in data collection and retention (Akinsanmi & Salami, 2021). Additionally, the ethical considerations surrounding unregulated health research using mobile devices emphasize the need for policies that strike a balance between innovation and privacy protection (Rothstein et al., 2020).

As technology progresses, new challenges arise, such as the security risks linked to eHealth cloud systems. Centralizing healthcare data on the cloud raises substantial privacy concerns, necessitating robust security measures to safeguard sensitive information (Al-Issa et al., 2019). Furthermore, the ethical implications of sharing health data for research purposes underscore the importance of informed consent and ensuring individuals have a say in the use of their data (Cumyn et al., 2021). In conclusion, navigating the complexities of data privacy and the law demands a nuanced approach that considers both security imperatives and individual rights. By implementing robust legal frameworks, promoting transparency, and upholding ethical standards, it is feasible to strike a balance that safeguards personal privacy while ensuring security in an increasingly data-driven world.

In the rapidly evolving landscape of new technologies like Artificial Intelligence (AI) and the Internet of Things (IoT), the importance of data privacy regulations cannot be overstated. As highlighted by (Śmietanka et al., 2021), the rise of federated learning and the need for privacy-preserving data access underscore the critical nature of safeguarding sensitive information. This is further reinforced by (Mathews & Assefa, 2022), who emphasize the significance of regulations like the General Data Protection Regulation (GDPR) in ensuring data privacy and user consent.

The complexity of balancing data security with individual privacy rights is a major challenge, especially with the dynamic nature of technology, as noted by (Barati et al., 2020). The General Data Protection Regulation (GDPR) plays a pivotal role in addressing these challenges, as highlighted by (Hadzovic et al., 2021), serving as a robust framework for data protection globally. In the realm of IoT, data privacy concerns persist, as seen in the work of (Obaid & Salman, 2022), stressing the integration of security and privacy in IoT-based healthcare systems. Additionally, Thorburn et al. (2019) propose a Privacy-By-Design framework for IoT, emphasizing the need to align regulatory requirements with industry best practices.

The intersection of AI and IoT further complicates data privacy issues, with GDPR and similar regulations playing a crucial role, as discussed by (Nguyen et al., 2021). The advent of Artificial Intelligence of Things (AIoT), as highlighted by (Zhang & Tao, 2021), underscores the need for robust privacy protection measures in this evolving landscape. In conclusion, as new technologies continue to advance, the role of data privacy regulations in safeguarding sensitive information and balancing data security with individual privacy rights becomes increasingly vital. Regulations like GDPR serve as essential tools in addressing these challenges, emphasizing the need for continuous adaptation to the evolving technological landscape.

In the current literature, there is still a knowledge gap that needs to be filled regarding the adaptation of data privacy regulations to these new technologies. Some aspects, such as the development of adequate policies, effective law enforcement, and protection of individual rights, still require deeper understanding. Therefore, this research aims to fill this knowledge gap through a systematic approach in exploring recent developments in data privacy

regulations related to AI and IoT. In this research, researchers adopted a systematic literature review method to identify and analyze the latest articles in relevant literature. The novelty of this research lies in the systematic approach we use to explore the latest information about data privacy regulations related to AI and IoT. It is hoped that this research contribution will enrich understanding of the complex relationship between data privacy regulations, security and individual rights in the context of this new technology. Thus, it is hoped that this research can provide valuable insights for policy makers, legal practitioners, researchers and society at large.

2. Research Methods

In conducting a systematic literature review for this research, several methodological steps have been taken to ensure the accuracy and objectivity of the article collection and analysis process. First of all, we chose a reputable international database, namely Scopus, as the main source for collecting articles. Scopus was chosen because it is one of the largest and most trusted databases in the field of science and technology, which includes various international journals relevant to this research topic.

Next, we formulated a list of keywords used in the search for relevant articles. The selected keywords include terms related to data privacy regulations, artificial intelligence, Internet of Things, data security, and individual rights. The use of relevant keywords helped us identify articles that best suited our research focus.

After searching using these keywords, we carry out an article selection process. The number of articles obtained from the initial search results was recorded in detail. Article inclusion and exclusion criteria were established to ensure that the selected articles met the standards of quality and relevance required for this research. Relevant articles are those that directly relate to data privacy regulations, AI, IoT, data security and individual rights. Articles that were not appropriate to the research topic or did not meet sufficient methodological quality were excluded from the analysis.

In addition, we used the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method as a guide for the article selection process. This method helps ensure transparency and consistency in the article selection process and ensures that all steps have been followed systematically and are well documented. Thus, using the PRISMA method allows us to carry out a systematic literature review in a structured and accurate way.

3. Results and Discussion

3.1. The Evolution of Data Privacy Regulations

In recent years, there has been a significant focus on data privacy regulations related to Artificial Intelligence (AI) and Internet of Things (IoT). The General Data Protection Regulation (GDPR) has played a crucial role in shaping the landscape of data privacy protection (Barati et al., 2020). With the increasing concerns about data security and privacy in IoT applications due to potential cyberattacks and data leakage (Zhang & Tao, 2021), there is a growing need for robust frameworks and technologies to address these challenges (Obaid & Salman, 2022).

Federated Learning (FL) has emerged as a promising solution for ensuring data privacy in IoT systems (Nguyen et al., 2021). FL enables collaborative training of machine learning models across IoT devices while adhering to privacy constraints, thus offering a way to improve data privacy using AI methods (Jiang et al., 2022). However, challenges persist in protecting data privacy while maintaining data utility through machine learning (Yin et al., 2021).

The integration of AI into IoT systems has introduced new capabilities to enhance security and meet the requirements of IoT security protection (Wu et al., 2020). AI-driven solutions have been explored to address security issues in IoT systems, highlighting the potential of AI in securing IoT services (Abed & Anupam, 2022). Additionally, Artificial Intelligence of Things (AIoT), which combines AI and IoT, has been identified as an advanced

technology that can create intelligent ecosystems across various applications (Zhang et al., 2022).

As data privacy preservation remains vital for the proliferation of IoT services (Alsheikh, 2023), there is a need to develop privacy-preserving mechanisms for IoT data sharing (Ghayyur et al., 2020). Recent regulations such as the GDPR and California Consumer Privacy Act have mandated enhanced processing of shared data with privacy-preserving mechanisms before release to service providers (Ghayyur et al., 2020). In conclusion, the intersection of AI and IoT has brought both opportunities and challenges regarding data privacy regulations. While FL and AI technologies offer promising solutions for enhancing data privacy in IoT systems, there is a continuous need to address the evolving landscape of data privacy regulations to ensure the security and privacy of AI and IoT applications.

Data privacy regulations have evolved significantly in response to challenges posed by advancing technologies. The General Data Protection Regulation (GDPR) has played a crucial role in shaping the landscape of data privacy (Degeling et al., 2019). Studies have indicated that the GDPR has increased transparency on the web, although there are still deficiencies in providing users with effective mechanisms to control the processing of their personal data (Degeling et al., 2019). Privacy regulations, including the GDPR, have been essential in safeguarding individual privacy and balancing data-related privacy concerns with surveillance issues (Li et al., 2022). Efforts to enhance privacy in technologies like face biometrics have been influenced by legislative requirements such as the GDPR, leading to the development of privacy-enhancing techniques (Meden et al., 2021). Similarly, the introduction of privacy regulations like the GDPR and the California Consumer Privacy Act (CCPA) has prompted ad networks to provide configurations to help app developers comply with these regulations (Tahaei et al., 2022). The GDPR, along with increasing public awareness of personal data privacy, has posed challenges to centralized data collection for server-based training in federated learning (Gao, 2023).

Privacy laws and privacy by design schemes, influenced by regulations such as the GDPR, are crucial for ensuring privacy in the Internet of Things (IoT) (Aljeraisy et al., 2021). The GDPR, along with regulations like the Health Insurance Portability and Accountability Act (HIPAA), govern the secure sharing of healthcare data, emphasizing the need for stringent measures against unauthorized access and data breaches (Upadrista et al., 2023). The GDPR has established new norms to promote free data flow and protect personal data privacy in the digital economy (Abdelrehim et al., 2021). In conclusion, data privacy regulations, particularly the GDPR, have evolved to address the challenges brought by technological advancements. These regulations have influenced the development of privacy-enhancing technologies, shaped data sharing practices, and emphasized the importance of individual privacy rights in the digital age.

Data privacy regulations have evolved in response to technological advancements such as artificial intelligence (AI) and the Internet of Things (IoT). Initially, regulations focused on protecting personal data against unauthorized use (Nguyen, 2021). With the emergence of AI and IoT, there is a growing need to adapt regulations to address the challenges posed by these technologies (Sadique et al., 2020). The rapid development of AI allows for automatic data collection and analysis, raising concerns about data governance and protection (Cai, 2024). Similarly, IoT devices continuously generate vast amounts of data, presenting new privacy and security challenges (Wazirali, 2022).

Jurisdictions are responding to these challenges by introducing new regulations or amending existing ones. Some countries are developing specific frameworks to govern AI use, including data privacy protection (Manzoor et al., 2023). Efforts are also underway to adjust current data privacy regulations to accommodate the needs arising from IoT technologies (Abdulghani et al., 2019). However, the evolution of data privacy regulations remains dynamic and ongoing, necessitating continuous monitoring to ensure that regulations can effectively

address emerging challenges without compromising individuals' privacy rights (Hadzovic et al., 2021).

To understand the effectiveness of existing regulations and identify areas for improvement, case studies and analyses of data privacy regulations in the context of AI and IoT are crucial (Zhang & Tao, 2021). These studies can provide insights into how regulations are being implemented and whether they are sufficient to safeguard individuals' data privacy in the face of advancing technologies. By examining real-world applications and compliance with regulations, researchers can assess the adequacy of current measures and propose enhancements where necessary. In conclusion, as AI and IoT technologies continue to advance, data privacy regulations must evolve to keep pace with these developments. Monitoring the implementation of regulations and conducting in-depth analyses are essential to ensure that individuals' rights to data privacy and security are protected effectively in the digital age.

3.2. Challenges in Adapting Data Privacy Regulations to AI and IoT

Adapting data privacy regulations to the challenges posed by Artificial Intelligence (AI) and the Internet of Things (IoT) involves addressing significant security and individual rights concerns. The integration of IoT devices and sensors into various systems, including healthcare, raises substantial security and privacy challenges that necessitate robust frameworks and technologies (Obaid & Salman, 2022). Privacy and security are identified as major hurdles in the IoT landscape (Tawalbeh et al., 2020). While AI technologies offer new methods for enhancing IoT security and data privacy, they also introduce new challenges and potential negative impacts on data, algorithms, and IoT architecture (Jiang et al., 2022).

To tackle these challenges, industry stakeholders are exploring new technical solutions to mitigate privacy and security risks in smart homes, developing standards, influencing regulations, and fostering communities of learning to address common issues (Cannizzaro & Procter, 2023). Additionally, the implementation of security and privacy guidelines is crucial to prevent IoT data breaches and mitigate individual privacy violations (Abdulghani et al., 2022; Abdulghani et al., 2019). Federated Learning (FL) has emerged as a promising approach to address data privacy concerns by enabling collaborative machine learning across IoT devices while adhering to privacy constraints (Manzoor et al., 2023).

Furthermore, the limited computing power of IoT devices, the diversity of IoT devices and providers, and the massive amounts of data collected and shared in IoT environments contribute to unique security and privacy challenges (Ranjan et al., 2020; Wazirali, 2022). The integration of Blockchain with IoT is highlighted as a potential solution to enhance security and privacy in IoT systems (Ahmed, 2022). Moreover, promoting individual awareness, information privacy protection, and ethical use of IoT platforms are essential in addressing the challenges of the interconnected digital world (Mugariri et al., 2022). In conclusion, adapting data privacy regulations to AI and IoT involves navigating complex security and individual rights challenges. Industry efforts to develop technical solutions, establish standards, and promote collaborative learning, along with the implementation of security guidelines and awareness initiatives, are crucial steps in addressing these evolving privacy concerns.

3.3. Implementation of Data Privacy Regulations related to AI and IoT

The implementation of data privacy regulations related to Artificial Intelligence (AI) and Internet of Things (IoT) is crucial in ensuring the protection of sensitive information in these interconnected systems. With the proliferation of IoT services, the need for data privacy preservation has become increasingly important (Alsheikh, 2023). Traditional AI techniques often involve centralized data collection and processing, which may not be feasible in realistic IoT application scenarios due to scalability issues and growing data privacy concerns (Nguyen, 2021).

Under stringent data privacy protection legislation like the General Data Protection Regulation (GDPR), data movement faces unprecedented difficulties, highlighting the need for personalized federated learning frameworks for intelligent IoT applications (Wu et al., 2020). Federated Learning (FL) has emerged as a key research area to enable collaborative training of machine learning models across smart IoT devices while adhering to privacy constraints, addressing the serious societal concern of data privacy (Manzoor et al., 2023).

In healthcare IoT systems, implementing technologies such as pseudonymization and data masking ensures compliance with privacy regulations, safeguarding patient data and trust (Obaid & Salman, 2022). Regulatory concerns in IoT services primarily focus on personal information and privacy protection, emphasizing the importance of addressing privacy issues in academic research and legislation (Na, 2023).

AI plays a significant role in analyzing data collected by IoT devices, highlighting the need for research on AI-enhanced IoT security to meet evolving security requirements (Thakare et al., 2022). The integration of AI with IoT in the form of Artificial IoT (AIoT) creates a network capable of processing data efficiently while addressing security and privacy challenges (Wu et al., 2020). In conclusion, the synthesis of these references underscores the importance of implementing data privacy regulations in AI and IoT systems. By leveraging technologies like federated learning, pseudonymization, and AI-enhanced security measures, organizations can navigate the complexities of data privacy in interconnected environments effectively.

4. Conclusions

This study illustrates the evolution of data privacy regulations in the face of challenges presented by technological advances, particularly in the context of artificial intelligence (AI) and the Internet of Things (IoT). Regulations such as the General Data Protection Regulation (GDPR) have played an important role in establishing a data privacy protection framework. However, the presence of AI and IoT creates new complexities that require adaptation to existing regulations.

In facing this challenge, we see industry efforts to find new technical solutions, such as the use of Federated Learning (FL) in protecting data privacy in IoT systems. FL offers a way to collaboratively train machine learning models on IoT devices without compromising data privacy. Apart from that, Blockchain integration with IoT is also a focus in efforts to increase security and privacy in IoT systems.

Implementation of data privacy regulations related to AI and IoT is crucial in ensuring the protection of sensitive information in these interconnected systems. In the healthcare sector, the use of technologies such as pseudonymity and data masking have proven effective in complying with privacy regulations, which in turn strengthens trust in patient data.

However, challenges remain in implementing these regulations, especially in the context of data movement faced with new barriers under strict regulations such as GDPR. The need for a federated learning framework tailored to the needs of intelligent IoT applications is becoming increasingly important in addressing these challenges.

This study has important implications for stakeholders in various fields, including policy makers, technology practitioners, and researchers. These findings highlight the importance of paying attention to data privacy regulations that are flexible and can adapt quickly to technological developments. Additionally, efforts to integrate new technologies, such as FL and Blockchain, within the data privacy regulatory framework can help overcome the challenges faced by AI and IoT.

While this study provides valuable insight into the evolution of data privacy regulations related to AI and IoT, several limitations need to be acknowledged. One of them is limited resources and time in conducting literature research, which may have overlooked some relevant studies. In addition, the focus of this study is primarily on the existing regulatory

framework and technology, without taking into account social, economic, or political factors that may influence the implementation of these regulations.

For future research, it is recommended to further expand the scope of analysis to cover more literature resources, including studies covering social, economic, and political aspects of data privacy regulations related to AI and IoT. Additionally, further studies could also explore the ethical implications of using technologies such as AI and IoT in the context of data privacy regulations. By broadening the scope of research and considering these additional aspects, future research can make a more comprehensive contribution to the understanding of the relationship between data privacy regulations, security, and emerging technologies.

5. References

Abdelrehim, A., Khan, A., & Soomro, N. (2021). Digital economy barriers to trade regulation status, challenges, and china's response. International Journal of Social Sciences Perspectives, 8(2), 41-49. https://doi.org/10.33094/7.2017.2021.82.41.49

Abdulghani, H., Nijdam, N., & Konstantas, D. (2022). Analysis on security and privacy guidelines: rfid-based iot applications. Ieee Access, 10, 131528-131554. https://doi.org/10.1109/access.2022.3227449

Abdulghani, H., Nijdam, N., Collen, A., & Konstantas, D. (2019). A study on security and privacy guidelines, countermeasures, threats: iot data at rest perspective. Symmetry, 11(6), 774. https://doi.org/10.3390/sym11060774

Abed, A. and Anupam, A. (2022). Review of security issues in internet of things and artificial intelligence-driven solutions. Security and Privacy, 6(3). https://doi.org/10.1002/spy2.285

Ahmed, M. (2022). Integration of blockchain with the internet of things: a systematic review.. https://doi.org/10.14293/s2199-1006.1.sor-.ppgvo0b.v1

Akinsanmi, T. and Salami, A. (2021). Evaluating the trade-off between privacy, public health safety, and digital security in a pandemic. Data & Policy, 3. https://doi.org/10.1017/dap.2021.24

Al-Issa, Y., Ottom, M., & Tamrawi, A. (2019). Ehealth cloud security challenges: a survey. Journal of Healthcare Engineering, 2019, 1-15. https://doi.org/10.1155/2019/7516035

Aljeraisy, A., Barati, M., Rana, O., & Perera, C. (2021). Privacy laws and privacy by design schemes for the internet of things. Acm Computing Surveys, 54(5), 1-38. https://doi.org/10.1145/3450965

Alsheikh, M. (2023). Five common misconceptions about privacy-preserving internet of things. Ieee Communications Magazine, 61(5), 151-157. https://doi.org/10.1109/mcom.001.2200097

Barati, M., Rana, O., Petri, I., & Theodorakopoulos, G. (2020). Gdpr compliance verification in internet of things. Ieee Access, 8, 119697-119709. https://doi.org/10.1109/access.2020.3005509

Cai, L. (2024). Privacy-preserving iot system based on blockchain and proxy re-encryption.. https://doi.org/10.1117/12.3026400

Cannizzaro, S. and Procter, R. (2023). How is the internet of things industry responding to the cybersecurity challenges of the smart home?.. https://doi.org/10.5772/intechopen.106012

Cumyn, A., Dault, R., Barton, A., Cloutier, A., & Ethier, J. (2021). Citizens, research ethics committee members and researchers' attitude toward information and consent for the secondary use of health data: implications for research within learning health systems. Journal of Empirical Research on Human Research Ethics, 16(3), 165-178. https://doi.org/10.1177/1556264621992214

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We value your privacy ... now take some cookies: measuring the gdpr's impact on web privacy.. https://doi.org/10.14722/ndss.2019.23378

Evans, B. (2020). The perils of parity: should citizen science and traditional research follow the same ethical and privacy principles?. The Journal of Law Medicine & Ethics, 48(S1), 74-81. https://doi.org/10.1177/1073110520917031

Gao, H. (2023). Towards trustworthy federated learning: a blockchain-based architecture for auditing, traceability, and verification.. https://doi.org/10.1117/12.3009373

Gao, Y., Guo, Y., Jumani, A., & Shankar, A. (2021). Internet industry data openness and personal information protection based on privacy laws.. https://doi.org/10.21203/rs.3.rs-924655/v1

Ghayyur, S., Pappachan, P., Wang, G., Mehrotra, S., & Venkatasubramanian, N. (2020). Designing privacy preserving data sharing middleware for internet of things.. https://doi.org/10.1145/3419016.3431484

Hadzovic, S., Mrdovic, S., & Radonjic, M. (2021). Identification of iot actors. Sensors, 21(6), 2093. https://doi.org/10.3390/s21062093

Hadzovic, S., Mrdovic, S., & Radonjic, M. (2021). Identification of iot actors. Sensors, 21(6), 2093. https://doi.org/10.3390/s21062093

Jiang, H., Gai, J., Zhao, S., Chaudhry, P., & Chaudhry, S. (2022). Applications and development of artificial intelligence system from the perspective of system science: a bibliometric review. Behavioral Science, 39(3), 361-378. https://doi.org/10.1002/sres.2865

Li, C., Chu, J., & Zheng, L. (2022). Better not let me know. Journal of Global Information Management, 30(1), 1-22. https://doi.org/10.4018/jgim.306246

Manzoor, S., Jain, S., Singh, Y., & Singh, H. (2023). Federated learning based privacy ensured sensor communication in iot networks: a taxonomy, threats and attacks. Ieee Access, 11, 42248-42275. https://doi.org/10.1109/access.2023.3269880

Mathews, S. and Assefa, S. (2022). Federated learning: balancing the thin line between data intelligence and privacy.. https://doi.org/10.48550/arxiv.2204.13697

Meden, B., Rot, P., Terhörst, P., Damer, N., Kuijper, A., Scheirer, W., … & Štruc, V. (2021). Privacy–enhancing face biometrics: a comprehensive survey. Ieee Transactions on Information Forensics and Security, 16, 4147-4183. https://doi.org/10.1109/tifs.2021.3096024

Mugariri, P., Abdullah, H., García-Torres, M., Parameshachari, B., & Sattar, K. (2022). Promoting information privacy protection awareness for internet of things (iot). Mobile Information Systems, 2022, 1-11. https://doi.org/10.1155/2022/4247651

Na, H. (2023). Which attributes should be considered in regulating the internet of things? evidence from conjoint analysis. Sage Open, 13(4). https://doi.org/10.1177/21582440231209806

Natamiharja, R., Sabatira, F., Banjarani, D., Davey, O., & Setiawan, I. (2022). Balancing two conflicting perspectives on wiretapping act: rights to privacy and law enforcement. Al-Risalah, 22(1), 18-30. https://doi.org/10.30631/alrisalah.v22i1.1226

Nguyen, D., Ding, M., Pathirana, P., Seneviratne, A., Li, J., & Poor, H. (2021). Federated learning for internet of things: a comprehensive survey. Ieee Communications Surveys & Tutorials, 23(3), 1622-1658. https://doi.org/10.1109/comst.2021.3075439

Nguyen, D. (2021). Federated learning for internet of things: a comprehensive survey.. https://doi.org/10.48550/arxiv.2104.07914

Obaid, O. and Salman, S. (2022). Security and privacy in iot-based healthcare systems: a review., 29-40. https://doi.org/10.58496/mjcsc/2022/007

Ranjan, R., Hsu, C., Chen, L., & Georgakopoulos, D. (2020). Holistic technologies for managing internet of things services. Ieee Transactions on Services Computing, 13(4), 597-601. https://doi.org/10.1109/tsc.2020.3000844

Rothstein, M., Wilbanks, J., Beskow, L., Brelsford, K., Doerr, M., Evans, B., … & Tovino, S. (2020). Unregulated health research using mobile devices: ethical considerations and policy recommendations. The Journal of Law Medicine & Ethics, 48(S1), 196-226. https://doi.org/10.1177/1073110520917047

Sadique, K., Rahmani, R., & Johannesson, P. (2020). Enhancing data privacy in the internet of things (iot) using edge computing., 231-243. https://doi.org/10.1007/978-3-030-66763-4_20

Shifa, A., Asghar, M., Fleury, M., Kanwal, N., Ansari, M., Lee, B., … & Qiao, Y. (2020). Mulvis: multi-level encryption based security system for surveillance videos. Ieee Access, 8, 177131-177155. https://doi.org/10.1109/access.2020.3024926

Śmietanka, M., Pithadia, H., & Treleaven, P. (2021). Federated learning for privacy-preserving data access. International Journal of Data Science and Big Data Analytics, 1(2), 1. https://doi.org/10.51483/ijdsbda.1.2.2021.1-13

Tahaei, M., Ramokapane, K., Li, T., Hong, J., & Rashid, A. (2022). Charting app developers' journey through privacy regulation features in ad networks. Proceedings on Privacy Enhancing Technologies, 2022(3), 33-56. https://doi.org/10.56553/popets-2022-0061

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). Iot privacy and security: challenges and solutions. Applied Sciences, 10(12), 4102. https://doi.org/10.3390/app10124102

Thakare, V., Khire, G., & Kumbhar, M. (2022). Artificial intelligence (ai) and internet of things (iot) in healthcare: opportunities and challenges. Ecs Transactions, 107(1), 7941-7951. https://doi.org/10.1149/10701.7941ecst

Thorburn, R., Margheri, A., & Paci, F. (2019). Towards an integrated privacy protection framework for iot: contextualising regulatory requirements with industry best practices.. https://doi.org/10.1049/cp.2019.0170

Tovino, S. (2020). Mobile research applications and state data protection statutes. The Journal of Law Medicine & Ethics, 48(S1), 87-93. https://doi.org/10.1177/1073110520917033

Tovino, S. (2020). Privacy and security issues with mobile health research applications. The Journal of Law Medicine & Ethics, 48(S1), 154-158. https://doi.org/10.1177/1073110520917041

Upadrista, V., Nazir, S., & Tianfield, H. (2023). Secure data sharing with blockchain for remote health monitoring applications: a review. Journal of Reliable Intelligent Environments, 9(3), 349-368. https://doi.org/10.1007/s40860-023-00204-w

Wazirali, R. (2022). A review on privacy preservation of location-based services in internet of things. Intelligent Automation & Soft Computing, 31(2), 767-779. https://doi.org/10.32604/iasc.2022.019243

Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: a survey. Ieee Access, 8, 153826-153848. https://doi.org/10.1109/access.2020.3018170

Wu, Q., He, K., & Chen, X. (2020). Personalized federated learning for intelligent iot applications: a cloud-edge based framework. Ieee Open Journal of the Computer Society, 1, 35-44. https://doi.org/10.1109/ojcs.2020.2993259

Yin, X., Zhu, Y., & Hu, J. (2021). A comprehensive survey of privacy-preserving federated learning. Acm Computing Surveys, 54(6), 1-36. https://doi.org/10.1145/3460427

Zhang, J. and Tao, D. (2021). Empowering things with intelligence: a survey of the progress, challenges, and opportunities in artificial intelligence of things. Ieee Internet of Things Journal, 8(10), 7789-7817. https://doi.org/10.1109/jiot.2020.3039359

Zhang, J. and Tao, D. (2021). Empowering things with intelligence: a survey of the progress, challenges, and opportunities in artificial intelligence of things. Ieee Internet of Things Journal, 8(10), 7789-7817. https://doi.org/10.1109/jiot.2020.3039359

Zhang, Z., Wen, F., Sun, Z., Guo, X., He, T., & Lee, C. (2022). Artificial intelligence-enabled sensing technologies in the 5g/internet of things era: from virtual reality/augmented reality to the digital twin. Advanced Intelligent Systems, 4(7). https://doi.org/10.1002/aisy.202100228