Clean Energy and Smart Technology

Clean Energy and Smart Technology
Volume 04, Number 01, October 2025
DOI : https://doi.org/10.58641/cest.v4i1.169

e-ISSN : 2964-2647

CHALLENGES IN DATA SECURITY: TECHNOLOGICAL AND REGULATORY CHALLENGES IN THE PROTECTION OF PERSONAL DATA IN THE DIGITAL ERA

Muhamad Fuat Asnawi[1)*], Muhammad Alif Muwafiq Baihaqy[2)], Saifu Rohman[3)], Nur Hasanah[4)], Dian Asmarajati[4)]
[1)2)3)4)5)] Universitas Sains Al-Qur'an, Indonesia

*fuat@unsiq.ac.id

Submitted :18 Oktober 2025 | **Accepted** : 24 Oktober 2025 | **Published** : 31 Oktober 2025

Abstract: This study examines the challenges of personal data security in the digital era, focusing on encryption technology and the role of artificial intelligence (AI) in protecting personal data in an increasingly complex digital environment. Adopting a Systematic Literature Review (SLR) method, this study examines 91 articles obtained from IEEE Xplore and ScienceDirect to identify trends and challenges in personal data security, particularly in the context of cloud computing and the Internet of Things (IoT). The results show that although encryption technology and AI offer advanced solutions, major challenges remain in the implementation of global regulations such as GDPR and differences in policies and infrastructure across countries. This study also discusses potential solutions such as blockchain and the implementation of adaptive encryption to address weaknesses in personal data security.

Keywords: Data Security, Artificial Intelligence, Encryption, Cloud Computing,

1. INTRODUCTION

Personal data protection has become a key issue in today's digital world, with the increasing use of digital technology and internet-based platforms. Personal data, such as financial information, health information, and online behavior, is increasingly becoming a primary target for cyberattacks that can compromise individual privacy and harm organizations. With the rapid development of technologies such as cloud computing, the Internet of Things (IoT), and artificial intelligence (AI), threats to data security are also becoming increasingly complex and difficult to address. These increasingly sophisticated technologies offer opportunities to improve efficiency and service quality, but they also open significant opportunities for potential misuse of personal data (Isaac Abiodun et al. 2022; Li and Saxunová 2020; Miller, Lukic, and Skiera 2025).

The main challenge in personal data protection is the imbalance between technological advancements and the readiness of systems to manage and secure such data. Often, data collected and processed by various digital platforms is used without adequate oversight. This risks personal data leaks that can be exploited by irresponsible parties. In this context, regulation is crucial to ensure that personal data protection complies with standards set by countries and international organizations (Azam et al. 2023; Guaman, Del Alamo, and Caiza 2021; Miller et al. 2025).

One important regulation governing personal data protection is the General Data Protection Regulation (GDPR) implemented in the European Union. The GDPR provides a clear legal framework for how personal data should be treated, protecting individuals' rights to control their personal information. However, despite the GDPR's implementation, challenges remain in its implementation, particularly in cross-border surveillance between countries and organizations. Implementing the GDPR on a global scale still faces numerous challenges, including regulatory differences between countries and challenges in managing personal data on cloud-based and IoT platforms (Li and Saxunová 2020; Miller et al. 2025; Wang et al. 2023; Zafir et al. 2024).

In addition to existing regulations, the technology used to secure personal data also faces significant challenges. Encryption methods, often used to protect data during transmission and storage, can face vulnerabilities if not implemented properly. For example, outdated encryption techniques or the use of weak keys can provide hackers with vulnerabilities to exploit protected data (Alouffi et al. 2021; Isaac Abiodun et al. 2022; Taherdoost, Le, and Slimani 2025). In this context, technologies such as homomorphic encryption and blockchain-based encryption have been introduced to address the inadequacy of traditional encryption in the face of today's sophisticated threats (Dai et al. 2020; Isaac Abiodun et al. 2022; Marwan et al. 2024; Niu et al. 2020).

Furthermore, another equally significant challenge is managing personal data in cloud computing and IoT environments. Cloud-based platforms allow for more efficient data storage and access, but they also pose a significant risk of data breaches. Personal data stored in the cloud must be protected with adequate security layers, such as end-to-end encryption and multifactor authentication (Dou et al. 2024; Yu et al. 2025; Zafir et al. 2024). Data management in the IoT also adds complexity to data protection, given the large number of connected devices operating with little human oversight, increasing opportunities for hackers to exploit system vulnerabilities (Adam et al. 2024; Isaac Abiodun et al. 2022; Miller et al. 2025; Zhang et al. 2024).

Regulatory challenges in personal data protection are exacerbated when data collection crosses borders. The use of cloud services by multinational companies or IoT applications operating in multiple countries presents challenges in ensuring compliance with applicable regulations in each country. Although the GDPR has established global standards, not all countries outside the European Union have equivalent data protection policies. Therefore, cross-border regulation of personal data protection becomes crucial (Cejas et al. 2023; Isaac Abiodun et al. 2022; Zafir et al. 2024).

Furthermore, a lack of awareness among users about the importance of personal data protection is also a major challenge. Many individuals are unaware of how their personal data is collected, processed, and shared by companies. They may also be unaware that the data they share online could be used without their consent, opening up the potential for data misuse. Therefore, it is crucial for organizations to implement clear and transparent privacy policies and educate users on how to protect their personal data (Li and Saxunová 2020; Miller et al. 2025; Seiling et al. 2024; Ye et al. 2024).

On the other hand, the adoption of new technologies such as artificial intelligence (AI) also adds challenges to personal data management. AI is used to analyze data on a large scale and generate automated decisions. While this provides efficiency and innovation, AI can also raise concerns about the unauthorized use of personal data or potential algorithmic discrimination (Isaac Abiodun et al. 2022; Marelli 2023; Miller et al. 2025; Mishra and Pandey 2021). Therefore, it is crucial to develop an ethical and transparent approach to AI in processing personal data.

Personal data protection also requires a comprehensive approach, involving various parties within the organization, from the technical teams managing security systems to the legal authorities ensuring compliance with policies and regulations. The government also plays a crucial role in establishing personal data protection standards that all parties can adhere to, as well as ensuring that there are clear sanctions for data protection violations.

Given the challenges, it is crucial for organizations to continue innovating in developing data security solutions that are more adaptive and responsive to evolving threats. In the increasingly complex digital era, artificial intelligence (AI) and cloud computing have introduced new challenges in protecting personal data. The use of these advanced technologies opens up numerous opportunities, but also increases the potential for threats to privacy and data integrity. Therefore, the implementation of regulations such as the General Data Protection Regulation (GDPR) has been a crucial step in establishing a global framework for personal data protection. While the GDPR has proven effective in curbing privacy violations and raising global awareness of personal data protection, its implementation needs to be continuously evaluated to better align with evolving technological innovations. As technology advances, AI, blockchain, and machine learning (ML)-based technologies offer significant potential in enhancing personal data security and meeting increasingly stringent regulatory demands. Adapting to these technologies is necessary to maintain user trust and ensure better data protection in the future.

2. METHOD

This study adopted a Systematic Literature Review (SLR) approach to identify and analyze existing trends and challenges in data security technology (Alouffi et al. 2021; Bliznak, Munk, and Pilkova 2024; Ghebreselassie, Hammen, and Hustad 2025). The SLR process was conducted by reviewing 91 articles collected from reputable sources, namely IEEE Xplore and ScienceDirect.

a. Search Strategy

The literature search strategy in this study involved a series of systematic steps, as shown in Figure 1. The databases used included IEEE Xplore and ScienceDirect. Keywords used for the search included: 'data security technologies', 'recent trends in data encryption', 'artificial intelligence in data security', 'AI for encryption and data security', and 'data protection challenges in IoT'. The process began with the identification of primary keywords, which were then combined to search for relevant articles. Search results were filtered based on relevance and publication period between 2020 and 2025. Articles that met the inclusion criteria were then collected, and their full texts were downloaded for further analysis. Figure 1 illustrates the stages of the search strategy, while Figure 2 shows the final distribution of articles based on the databases used.

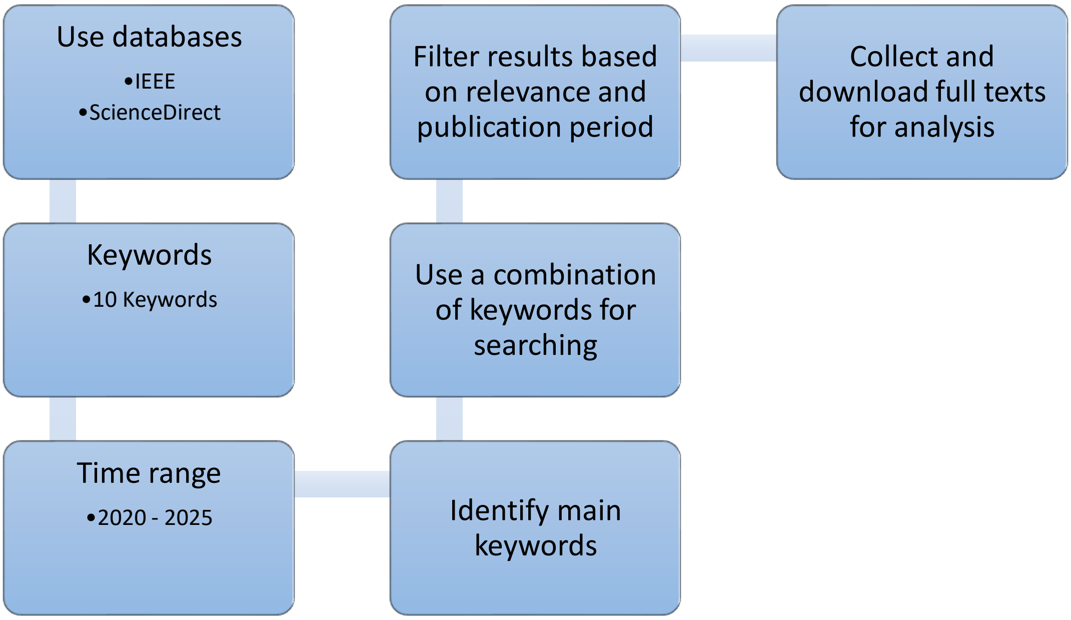
Use databases
•IEEE
•ScienceDirect
Keywords
•10 Keywords
Time range
•2020 - 2025
Identify main keywords
Use a combination of keywords for searching
Filter results based on relevance and publication period
Collect and download full texts for analysis

Figure 1. Stages of Search Strategy

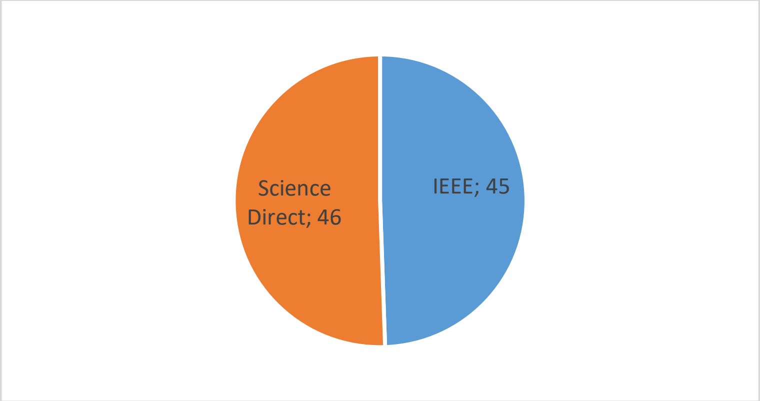

Figure 2. Distribution of selected articles based on database

b. Research Questions

To guide and focus this review, the following research questions will be used:
RQ1: What are the main challenges in securing personal and sensitive data in the digital world, particularly in the context of cloud computing and IoT?
RQ2: How can artificial intelligence (AI) technologies address the challenges of securing personal data in an increasingly complex digital environment?
RQ3: What are the challenges faced in implementing global personal data protection regulations, such as the GDPR, across countries with differing policies?
RQ4: To what extent is the GDPR effective in protecting personal data in the digital age, and what are the obstacles to its implementation globally?

3. RESULT AND DISCUSSION

a. Key Challenges in Securing Personal Data in the Digital Era

Digital transformation has made personal and sensitive data a primary commodity across various online services. However, this has brought new complexities and challenges to data protection, particularly in cloud computing and the Internet of Things (IoT) environments. In the context of cloud computing, the most fundamental challenge is the shift of data control from users to third-party cloud service providers. Users often lose control over the location, management, and access to their data (Isaac Abiodun et al. 2022; Lingga et al. 2024; Marwan et al. 2024; Zafir et al. 2024). The public cloud model, while offering scalability and cost efficiency, actually increases the risk of insider attacks, data leaks due to misconfigurations, and unauthorized access by unauthorized parties (Lingga et al. 2024; Zafir et al. 2024).

Furthermore, authentication and authorization challenges remain key issues, with weak security systems making it easier for hackers to gain access to sensitive data. Data breaches in cloud environments are often caused by poor encryption key management, weak passwords, or failure to implement role-based access controls (Lingga et al. 2024; Salih and Jasim Mohammad 2024; Zhang et al. 2022). Another issue is the difficulty of data provenance and conducting security audits due to the highly dynamic and distributed cloud architecture (Isaac Abiodun et al. 2022; Nayak n.d.).

On the other hand, the implementation of IoT expands the attack surface due to millions of smart devices connected to the network, often without adequate security protections. Many IoT devices are built with limited resources and therefore cannot implement encryption algorithms or provide regular system updates (Cheng et al. 2025; Harbi et al. 2021). The lack of security standards among IoT device manufacturers and the lack of patching create vulnerabilities that are vulnerable to exploitation by hackers.

User privacy is also threatened by the massive and continuous data collection on IoT devices, where users are not always given transparency or control over how their data is used and stored (Li and Saxunová 2020; Miller et al. 2025). Personal data from IoT sensors can be used to build behavioral profiles of individuals, which are vulnerable to misuse if they fall into the wrong hands. Another challenge arises in the process of transmitting data between devices and the cloud, which, if not properly encrypted, can potentially be hijacked during transit (Awaysheh et al. 2022; Ghebreselassie et al. 2025; Zhang et al. 2022).

Beyond technical factors, regulatory and compliance challenges are also significant. Differences in data protection standards across countries complicate cross-border data protection efforts, especially when cloud infrastructure and IoT devices operate globally (Li and Saxunová 2020). Some countries have strict data protection regulations, such as the GDPR, but their implementation in the cloud and IoT still faces numerous obstacles, both technologically and through implementation costs, and across agencies (Miller et al. 2025; Zafir et al. 2024).

Ultimately, the biggest challenge in securing personal and sensitive data in the cloud and IoT is ensuring comprehensive security from end-to-end, from devices, networks, and cloud systems to data storage and processing. The development of adaptive encryption technology, multifactor authentication, AI-based anomaly monitoring, and the adoption of security-by-design principles throughout the digital ecosystem are crucial in addressing the challenges of today's digital era.

b. The Role of Encryption Technology and Artificial Intelligence in Addressing Data Security Challenges

Artificial intelligence (AI) is increasingly playing a crucial role in addressing the challenges of securing personal data in an increasingly complex digital world. One key application of AI is in threat detection, where it uses machine learning (ML) and deep learning (DL) techniques to analyze big data patterns and detect suspicious anomalies. AI-based intrusion detection systems, which continuously learn from previous attacks, become more effective at quickly identifying new threats (Chakraborty and Tsokos 2023; Miller et al. 2025). Furthermore, AI is being used to manage privacy and sensitive data by detecting unusual access patterns and implementing automated access control through biometric-based authentication (Isaac Abiodun et al. 2022; Miller et al. 2025).

Furthermore, AI assists in data provenance management to ensure data integrity, particularly in cloud and IoT environments (Isaac Abiodun et al. 2022; Liu 2025). This technology also plays a role in managing and protecting connected IoT devices, which often have security vulnerabilities (Adam et al. 2024; Zhang et al. 2024). The advantage of AI is its ability to learn and adapt to new threats, thereby increasing the effectiveness of detection and response to evolving cyberattacks.

AI, combined with strong encryption, creates a multi-layered defense framework to protect personal and sensitive data in the digital environment. The collaboration between AI and encryption technology can provide a more efficient and effective solution for securing personal data, both in cloud computing and on IoT devices.

Table 1. Most Used AI/ML Technologies in Data Security (2020–2025)

No.	AI/ML Methods	Article Source	Uses in Data Security
1	Intrusion Detection System (IDS) berbasis AI	(Chakraborty and Tsokos 2023; Ieropoulos et al. 2025; Miller et al. 2025; Ye et al. 2024)	Attack/anomaly detection and classification
2	Deep Learning untuk Threat Detection	(Behera et al. 2025; Isaac Abiodun et al. 2022; Sanober et al. 2021)	Automated malware and cyberattack detection
3	Machine Learning untuk Enkripsi Adaptif	(Alarfaj et al. 2022; Gupta et al. 2022; Hashemi, Mirtaheri, and Greco 2023; Khan et al. 2022; Tanouz et al. 2021)	Encryption process automation and attack pattern detection
4	AI untuk Analisis Data Provenance	(Isaac Abiodun et al. 2022)	Digital forensics in the cloud and IoT
5	AI untuk Privacy Preservation	(Harbi et al. 2021; Miller et al. 2025; Mitra and Pal 2025)	Sensitive data management and regulatory compliance

Table 1 shows the various artificial intelligence (AI) and machine learning (ML) technologies most widely used in data security between 2020 and 2025, along with article sources and their uses. AI-based Intrusion Detection System (IDS) technology is used to detect and classify attacks or anomalies (Chakraborti & Tsokos, 2023; Ye et al., 2024), while Deep Learning for Threat Detection is used to automatically detect malware and cyberattacks (Behera et al., 2025; Isaac Abiodun et al., 2022). Machine Learning for Adaptive Encryption functions to automate encryption and detect attack patterns (Alaffar et al., 2022), and AI for Data Provenance Analysis is applied in digital forensics in the cloud and IoT for data provenance tracking (Isaac Abiodun et al., 2022). Additionally, AI for Privacy Preservation is used to manage sensitive data and ensure compliance with privacy regulations (Harbi et al., 2021; Miller et al., 2025). These technologies strengthen data security by automating detection and encryption processes and protecting personal and sensitive data in digital environments.

c. Challenges in Implementing Global Personal Data Protection Regulations

The implementation of global personal data protection regulations, such as the General Data Protection Regulation (GDPR), faces significant challenges across countries due to differences in legal policies, culture, and existing infrastructure. While the GDPR has set high standards for personal data protection in the European Union, challenges arise when implementing this regulation globally, particularly in countries with weaker or divergent data protection policies (Azam et al. 2023; Li and Saxunová 2020; Zafir et al. 2024). Countries with less stringent policies often struggle to adapt their systems to GDPR standards, increasing the risk of data breaches and privacy violations.

Furthermore, GDPR implementation also faces challenges in cross-border data management. Data stored and processed in one country often involves third parties located in other countries. Legal differences between the country of origin and the country where the data is stored can complicate monitoring and enforcement of the regulation (Miller et al. 2025). Furthermore, countries without regulations equivalent to the GDPR often lack mechanisms to address these issues, adding to the risks for users and companies operating internationally (Azam et al. 2023; Han and Park 2022; De Winter, Houben, and Lopriore 2024; Zhang et al. 2024).

Another issue is the inconsistency in oversight and the application of sanctions. Some countries have limited capacity among regulatory bodies to effectively implement and monitor these regulations. Even in countries with strong regulations, GDPR implementation can be hampered by limited resources to investigate violations and ensure compliance (Isaac Abiodun et al. 2022).

Finally, differences in cultural perceptions of privacy and personal data across countries also influence the implementation of these regulations. In some countries, people are more concerned about privacy and personal data management, while in others, there is a tendency to be less concerned about these aspects. This creates additional challenges in creating global awareness and uniform protection standards (Miller et al. 2025).

d. Effectiveness and Constraints of GDPR Implementation in Personal Data Protection

The General Data Protection Regulation (GDPR) has brought significant changes to the way personal data is protected in the European Union and around the world. Overall, the GDPR is considered effective in providing stronger protection for personal data by establishing clearer individual rights, such as the right to be forgotten and the right to access personal data. This provides greater protection for individual privacy and increases transparency about how data is collected, stored, and used by companies (Miller et al. 2025).

However, while the GDPR has been effective in minimizing the use of unauthorized online trackers and giving individuals greater control over their personal data, significant challenges remain in its implementation. One of the biggest obstacles is the difficulty of implementing it in non-EU countries that have different regulations or do not have personal data protection policies equivalent to the GDPR. This creates difficulties in monitoring and enforcing regulations at the global level, especially when personal data crosses national borders (Alves et al. 2023; Isaac Abiodun et al. 2022; Li and Saxunová 2020; Moenck et al. 2025; Yang et al. 2024).

Furthermore, while the GDPR provides a robust legal framework, a lack of awareness and understanding of the rights it provides among individuals and companies also poses a barrier. Many organizations struggle to comply with GDPR regulations due to the complexity and cost of implementation, particularly small and medium-sized enterprises that lack the resources to establish adequate compliance systems (Azam et al. 2023; Cejas et al. 2023; Guaman et al. 2021; Miller et al. 2025; Wang et al. 2023; Zafir et al. 2024).

Overall, while the GDPR has successfully improved personal data protection, implementation challenges remain, both technical and legal, as well as organizational and public awareness. Therefore, despite its significant positive impact, adjustments and ongoing efforts are still needed to ensure global compliance with this regulation.

4. CONCLUSION

Securing personal data in the digital era is increasingly complex with technological advances and the rapid use of internet-based platforms. The main challenges lie in managing distributed data and using technologies that open up opportunities for misuse, such as cloud computing and the Internet of Things (IoT). Although the GDPR was implemented with the aim of protecting personal data, its implementation still faces significant obstacles, particularly in terms of cross-border data management and regulatory differences between countries. Furthermore, the development of encryption technology and the application of artificial intelligence (AI) provide potential solutions to address these challenges, particularly in detecting threats and securing data. However, adjustments in regulations and technology are still needed to address evolving challenges, so that personal data protection can continue to be improved across various sectors. Adaptation to new technologies and policies that are more responsive to change are necessary to ensure better personal data security and privacy.

5. REFERENCES

Adam, Mumin, Mohammad Hammoudeh, Rana Alrawashdeh, and Basil Alsulaimy. 2024. ‘A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems’. *IEEE Access* 12:57128–49. doi:10.1109/ACCESS.2024.3382709.

Alarfaj, Fawaz Khaled, Iqra Malik, Hikmat Ullah Khan, Naif Almusallam, Muhammad Ramzan, and Muzamil Ahmed. 2022. ‘Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms’. *IEEE Access* 10:39700–715. doi:10.1109/ACCESS.2022.3166891.

Alouffi, Bader, Muhammad Hasnain, Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, and Muhammad Ayaz. 2021. ‘A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies’. *IEEE Access* 9:57792–807. doi:10.1109/ACCESS.2021.3073203.

Alves, Paulo Henrique, Fernando Correia, Isabella Frajhof, Clarisse Sieckenius De Souza, and Helio Lopes. 2023. 'Designing Intelligent Agents in Normative Systems Toward Data Regulation Representation'. *IEEE Access* 11:51590–605. doi:10.1109/ACCESS.2023.3276294.

Awaysheh, Feras M., Mohammad N. Aladwan, Mamoun Alazab, Sadi Alawadi, Jose C. Cabaleiro, and Tomas F. Pena. 2022. 'Security by Design for Big Data Frameworks Over Cloud Computing'. *IEEE Transactions on Engineering Management* 69(6):3676–93. doi:10.1109/TEM.2020.3045661.

Azam, Naila, Lito Michala, Shuja Ansari, and Nguyen Binh Truong. 2023. 'Data Privacy Threat Modelling for Autonomous Systems: A Survey from the GDPR's Perspective'. *IEEE Transactions on Big Data* 9(2):388–414. doi:10.1109/TBDATA.2022.3227336.

Behera, Sadananda, Neelamadhab Padhy, Rasmita Panigrahi, and Sanjay Kumar Kuanar. 2025. 'Crop Disease Prediction Using Deep Learning in a Federated Learning Environment: Ensuring Data Privacy and Agricultural Sustainability'. *Procedia Computer Science* 254:137–46. doi:10.1016/j.procs.2025.02.072.

Bliznak, Karol, Michal Munk, and Anna Pilkova. 2024. 'A Systematic Review of Recent Literature on Data Governance (2017-2023)'. *IEEE Access*.

Cejas, Orlando Amaral, Muhammad Ilyas Azeem, Sallam Abualhaija, and Lionel C. Briand. 2023. 'NLP-Based Automated Compliance Checking of Data Processing Agreements Against GDPR'. *IEEE Transactions on Software Engineering* 49(9):4282–4303. doi:10.1109/TSE.2023.3288901.

Chakraborty, Aditya, and Chris P. Tsokos. 2023. 'An AI-Driven Predictive Model for Pancreatic Cancer Patients Using Extreme Gradient Boosting'. *Journal of Statistical Theory and Applications* 22(4):262–82. doi:10.1007/s44199-023-00063-7.

Cheng, Zhuo, Jiangxin Li, Jianjun Zhang, Chen Wang, Hui Wang, and Juyin Wu. 2025. 'Application of Edge Computing Technology in Smart Grid Data Security'. *Measurement: Sensors* 37. doi:10.1016/j.measen.2024.101412.

Dai, Weiqi, Chunkai Dai, Kim Kwang Raymond Choo, Changze Cui, Deiqing Zou, and Hai Jin. 2020. 'SDTE: A Secure Blockchain-Based Data Trading Ecosystem'. *IEEE Transactions on Information Forensics and Security* 15:725–37. doi:10.1109/TIFS.2019.2928256.

Dou, Haochen, Zhenwu Dan, Peng Xu, Wei Wang, Shuning Xu, Tianyang Chen, and Hai Jin. 2024. 'Dynamic Searchable Symmetric Encryption With Strong Security and Robustness'. *IEEE Transactions on Information Forensics and Security* 19:2370–84. doi:10.1109/TIFS.2024.3350330.

Ghebreselassie, Meron Yonas, Henrik Hammen, and Eli Hustad. 2025. 'Challenges and Considerations in Migration to Cloud Solutions: A Systematic Literature Review'. Pp. 214–21 in *Procedia Computer Science*. Vol. 256. Elsevier B.V.

Guaman, Danny S., Jose M. Del Alamo, and Julio C. Caiza. 2021. 'GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps'. *IEEE Access* 9:15961–82. doi:10.1109/ACCESS.2021.3053130.

Gupta, Palak, Anmol Varshney, Mohammad Rafeek Khan, Rafeeq Ahmed, Mohammed Shuaib, and Shadab Alam. 2022. 'Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques'. Pp. 2575–84 in *Procedia Computer Science*. Vol. 218. Elsevier B.V.

Han, Sejin, and Sooyong Park. 2022. 'A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review'. *IEEE Access* 10:103888–905.

Harbi, Yasmine, Zibouda Aliouat, Allaoua Refoufi, and Saad Harous. 2021. 'Recent Security Trends in Internet of Things: A Comprehensive Survey'. *IEEE Access* 9:113292–314.

Hashemi, Seyedeh Khadijeh, Seyedeh Leili Mirtaheri, and Sergio Greco. 2023. 'Fraud Detection in Banking Data by Machine Learning Techniques'. *IEEE Access* 11:3034–43. doi:10.1109/ACCESS.2022.3232287.

Ieropoulos, Vasilis, Eirini Anthi, Theodoros Spyridopoulos, Pete Burnap, Ioannis Mavromatis, Aftab Khan, and Pietro Carnelli. 2025. 'Collaborative Intrusion Detection in Resource-Constrained IoT Environments: Challenges, Methods, and Future Directions a Review'. *Journal of Information Security and Applications* 93. doi:10.1016/j.jisa.2025.104127.

Isaac Abiodun, Oludare, Moatsum Alawida, Abiodun Esther Omolara, and Abdulatif Alabdulatif. 2022. 'Data Provenance for Cloud Forensic Investigations, Security, Challenges, Solutions and Future Perspectives: A Survey'. *Journal of King Saud University - Computer and Information Sciences* 34(10):10217–45.

Khan, Shahnawaz, Abdullah Alourani, Saudi Arabia, Bharavi Mishra, Ashraf Ali, and Mustafa Kamal. 2022. 'Developing a Credit Card Fraud Detection Model Using Machine Learning Approaches'. *IJACSA) International Journal of Advanced Computer Science and Applications* 13(3):2022. www.ijacsa.thesai.org.

Li, Yuanxin, and Darina Saxunová. 2020. 'A Perspective on Categorizing Personal and Sensitive Data and the Analysis of Practical Protection Regulations'. Pp. 1110–15 in *Procedia Computer Science*. Vol. 170. Elsevier B.V.

Lingga, Patrick, Jaehoon Jeong, Jinhyuk Yang, and Jeonghyeon Kim. 2024. 'SPT: Security Policy Translator for Network Security Functions in Cloud-Based Security Services'. *IEEE Transactions on Dependable and Secure Computing* 21(6):5156–69. doi:10.1109/TDSC.2024.3371788.

Liu, Yu. 2025. 'The Latest Application and Security Analysis of Cryptography in Cloud Storage Data Audit'. Pp. 984–90 in *Procedia Computer Science*. Vol. 259. Elsevier B.V.

Marelli, Massimo. 2023. 'The Law and Practice of International Organizations' Interactions with Personal Data Protection Domestic Regulation: At the Crossroads between the International and Domestic Legal Orders'. *Computer Law and Security Review* 50. doi:10.1016/j.clsr.2023.105849.

Marwan, Mbarek, Abdelkarim Ait Temghart, Said Ouhmi, and Mohamed Lazaar. 2024. 'Security, QoS and Energy Aware Optimization of Cloud-Edge Data Centers Using Game Theory and Homomorphic Encryption: Modeling and Formal Verification'. *Results in Engineering* 24. doi:10.1016/j.rineng.2024.102902.

Miller, Klaus M., Karlo Lukic, and Bernd Skiera. 2025. 'The Impact of the General Data Protection Regulation (GDPR) on Online Tracking'. *International Journal of Research in Marketing*. doi:10.1016/j.ijresmar.2025.03.002.

Mishra, Kamta Nath, and Subhash Chandra Pandey. 2021. 'Fraud Prediction in Smart Societies Using Logistic Regression and K-Fold Machine Learning Techniques'. *Wireless Personal Communications* 119(2):1341–67. doi:10.1007/s11277-021-08283-9.

Mitra, Arnab, and Anabik Pal. 2025. 'On Signal Encryption at MapReduce and Collaborative Attribute-Based Access with ECAs for a Preprocessed Data Set with ML in a Privacy-Preserving Health 4.0'. *E-Prime - Advances in Electrical Engineering, Electronics and Energy* 12. doi:10.1016/j.prime.2025.100983.

Moenck, Keno, Niklas Wais, Martin Gomse, Thorsten Schüppstuhl, and Boris Paal. 2025. 'Legal Implications of Vision-Language Foundation Models (VLFM) in Industrial Applications in Europe: An Inquiry into Data Protection, Copyright, and AI Regulation'. *Procedia CIRP* 134:999–1004. doi:10.1016/j.procir.2025.02.223.

Nayak, Debabrata. n.d. *Understanding the Security, Privacy and Trust Challenges of Cloud Computing*. Vol. 1.

Niu, Jie, Xuelian Li, Juntao Gao, and Yue Han. 2020. 'Blockchain-Based Anti-Key-Leakage Key Aggregation Searchable Encryption for IoT'. *IEEE Internet of Things Journal* 7(2):1502–18. doi:10.1109/JIOT.2019.2956322.

Salih, Bassim M., and Omer K. Jasim Mohammad. 2024. 'Cloud Data Leakage, Security, Privacy Issues and Challenges: Review'. Pp. 592–601 in *Procedia Computer Science*. Vol. 242. Elsevier B.V.

Sanober, Sumaya, Izhar Alam, Sagar Pande, Farrukh Arslan, Kantilal Pitambar Rane, Bhupesh Kumar Singh, Aditya Khamparia, and Mohammad Shabaz. 2021. 'An Enhanced Secure Deep Learning Algorithm for Fraud Detection in Wireless Communication'. *Wireless Communications and Mobile Computing* 2021. doi:10.1155/2021/6079582.

Seiling, Lukas, Rita Gsenger, Filmona Mulugeta, Marte Henningsen, Lena Mischau, and Marie Schirmbeck. 2024. 'Beware: Processing of Personal Data - Informed Consent Through Risk Communication'. *IEEE Transactions on Professional Communication* 67(1):4–25. doi:10.1109/TPC.2024.3361328.

Taherdoost, Hamed, Tuan Vinh Le, and Khadija Slimani. 2025. 'Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review'. *Cryptography* 9(1).

Tanouz, D., R. Raja Subramanian, D. Eswar, G. V. Parameswara Reddy, A. Ranjith Kumar, and C. H. V. N. M. Praneeth. 2021. 'Credit Card Fraud Detection Using Machine Learning'. Pp. 967–72 in *Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021*. Institute of Electrical and Electronics Engineers Inc.

Wang, Lipeng, Zhi Guan, Zhong Chen, and Mingsheng Hu. 2023. 'Enabling Integrity and Compliance Auditing in Blockchain-Based GDPR-Compliant Data Management'. *IEEE Internet of Things Journal* 10(23):20955–68. doi:10.1109/JIOT.2023.3285211.

De Winter, Derek P., Nina A. M. Houben, and Enrico Lopriore. 2024. *How Bureaucracy Is Bleeding Science Dry: International Observational Research under the General Data Protection Regulation*. http://data.europa.eu/eli/reg/2016/679/oj;

Yang, Fan, Mohammad Zoynul Abedin, Yanan Qiao, and Lvyang Ye. 2024. 'Toward Trustworthy Governance of AI-Generated Content (AIGC): A Blockchain-Driven Regulatory Framework for Secure Digital

Ecosystems'. *IEEE Transactions on Engineering Management* 71:14945–62. doi:10.1109/TEM.2024.3472292.

Ye, Xiongbiao, Yuhong Yan, Jia Li, and Bo Jiang. 2024. 'Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective'. *Telecommunications Policy* 48(10). doi:10.1016/j.telpol.2024.102851.

Yu, Mingyang, Bo Jin, Lei Zheng, Wei Zhan, and Chenxi Dong. 2025. 'Application of Data Encryption Technology in Computer Network Security'. Pp. 1187–93 in *Procedia Computer Science*. Vol. 261. Elsevier B.V.

Zafir, Ehsanul Islam, Afifa Akter, M. N. Islam, Shahid A. Hasib, Touhid Islam, Subrata K. Sarker, and S. M. Muyeen. 2024. 'Enhancing Security of Internet of Robotic Things: A Review of Recent Trends, Practices, and Recommendations with Encryption and Blockchain Techniques'. *Internet of Things (Netherlands)* 28.

Zhang, Lei, Hu Xiong, Qiong Huang, Jiguo Li, Kim Kwang Raymond Choo, and Jiangtao Li. 2022. 'Cryptographic Solutions for Cloud Storage: Challenges and Research Opportunities'. *IEEE Transactions on Services Computing* 15(1):567–87. doi:10.1109/TSC.2019.2937764.

Zhang, Yongxin, Jiacheng Yang, Hong Lei, Zijian Bao, Ning Lu, Wenbo Shi, and Bangdao Chen. 2024. 'PACTA: An IoT Data Privacy Regulation Compliance Scheme Using TEE and Blockchain'. *IEEE Internet of Things Journal* 11(5):8882–93. doi:10.1109/JIOT.2023.3321308.