Machine Learning for Privacy Auditing: A Comprehensive Review

Prateik Mahendra
Meta
Menlo Park, USA

ABSTRACT
Machine Learning (ML) has emerged as a necessary enabler of privacy auditing and, consequently, more robust compliance frameworks for contemporary data spaces. The ubiquity of interconnected models, especially in use cases like the Internet of Things (IoT), cloud computing, and federated learning (FL), has brought forth daunting challenges around data privacy, security, and support for regulatory requirements. This paper provides a panoramic view of cutting-edge research that falls under the paradigm of ML and privacy auditing and includes recent trends in threat monitoring, data integrity verification, automation of regulatory compliance, and privacy-preserving algorithms. Research studies from 2020-2025 have been included to bring the manuscript up to date on the current techno-regulatory environment. The study delves into basic techniques like differential privacy, integration with blockchain technology, and FL to assess their implications on the role of ML to hold data accountable. Following a recent literature stream, the review outlines current limitations and suggested directions for research on scalable, interpretable, and regulation-aware ML-based systems for privacy auditing.

Keywords
Machine Learning, Privacy Auditing, Data Compliance, Federated Learning, Differential Privacy.

1. INTRODUCTION
The increasing rate of expansion of data-centric technologies has necessitated privacy auditing as an organizational imperative in the management of sensitive information. Widespread use of artificial intelligence (AI), cloud computing, and big data analytics has facilitated the collection, processing, and analysis of large amounts of proprietary and individual data [1], [2]. While digitization has enhanced organizational capabilities and productivity, it has also brought with it issues of data security breaches, unauthorized disclosures, and the possibility of noncompliance with the requirements of regulators [3], due to quick digitization. Instances of cyber-attacks, data breaches, and privacy violations are increasingly common, hence the need for effective systems of privacy auditing that can identify, deter, and contain instances of security breaches in real-time [4]. The development of ML has facilitated the development of automated compliance systems that enhance the security, transparency, and accountability of data management practices. Against the traditional manual, rule-based privacy auditing that is based on pre-defined standards and the judgment of humans, ML-based audit systems have the ability to detect patterns through adaptive learning, identify anomalies, and identify likely security breaches in advance. These methods are critical in an era of the aggregation of structured and unstructured data from a wide range of sources and locations [5], [6]. ML-based privacy auditing necessitates real-time functionality with minimal human intervention, hence facilitating increased efficiency and accuracy.

Legacy audit processes lag the next-generation cyber threat sophistication and changing regulatory requirements. Manpower-based audit processes are slow, error-prone, and inadequate to match the rising regulatory burden imposed by industry and government regulators [7]. Regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), and other data protection laws mandate that organizations have efficient privacy management systems in place. Non-adherence to compliance requirements causes humongous financial losses, organization reputation loss, and loss of customer confidence. Organizations must possess smarter and faster compliance systems powered by machine learning to identify threats in real-time and apply corresponding policies in the dynamic regulatory landscape [8].

Privacy auditing has been the focus of widespread attention in the wake of business enterprises across industries such as healthcare, finance, telecommunication, and government increasingly relying on data for decision-making. The amount of sensitive data gathered and processed has increased manifold, making conventional auditing tools insufficient [9]. In addition, new technologies like the IoT, decentralized finance (DeFi), and edge computing have brought new data privacy issues with the dissemination of data across devices and networks. ML-based privacy auditing can fill these gaps with automated privacy risk assessment, anomaly detection, and adherence to the constantly changing privacy legislation [10].

This paper offers a critical review of the studies conducted to explore the use of ML in privacy auditing, including trends in AI-based compliance models, IoT security, distributed privacy-preserving learning, and verification based on blockchain verification. Through this review of novel applications of ML to privacy auditing, this research seeks to elucidate best practices, challenges, and opportunities for organizations to enhance their privacy governance structures. Further, the review reveals novel trends in FL, differential privacy, and cryptographic techniques that advance privacy auditing without jeopardizing data confidentiality.

1.1 Problem Statement
Even with the evolution of privacy-friendly technology, there are broad gaps in the implementation of automated authentication controls and compliance. With various stakeholders within the data environment, various regulatory requirements, and the constantly changing nature of the cyber-attacks, conventional auditing practices prove to be ineffective. ML-based auditing provides a scalable, dynamic,

and innovative means of controlling the vulnerabilities. Recent studies, however, highlight generalizability, interpretability, and legal compliance uncertainties, necessitating a critical examination of current practices and their implications on privacy auditing.

Compliance is also a significant challenge since organizations are unable to align ML-driven auditing systems with the current legal systems[11]. The speed at which AI models evolve exacerbates the challenge since new threats continue to arise, necessitating ongoing development of compliance tactics. This study aims to elucidate these loopholes and offer insight into enhancing ML approaches for enhanced privacy auditing.

2. OBJECTIVES

The main objectives of this systematic review are multi objective, with the intention to provide a synoptic overview of the status. These are stated as follows:

- Investigate ML-based privacy auditing frameworks in different data environments.
- Study the effectiveness of automated compliance methods based on artificial intelligence.
- Compare new privacy-protecting learning approaches.
- Identify important barriers and suggest areas for future research.
- Discuss FL, differential privacy, and blockchain usage in privacy auditing.
- Assess the business implications and limitations of ML-based privacy audit systems.

2.1 Research Questions

This systematic review analyzes six primary research questions to explore the use of AI in software testing:

RQ1: How do ML models enhance privacy auditing in data ecosystems?

RQ2: What are the basic technical techniques employed in compliance automation using ML?

RQ3: What are the challenges in implementing ML-based privacy-preserving solutions?

RQ4: What are the differences between different ML methods with respect to accuracy, scalability, and compliance with regulations?

RQ5: How does FL empower privacy-aware AI audit architectures?

RQ6: What are the avenues for future research to enhance ML-based privacy auditing systems?

2.2 Approach

The study incorporates the findings of 11 recent studies of research work and categorizes them according to their novel contribution in the domains of auditing privacy, threat detection, and automating compliance. A comparison is drawn between various ML methodologies, i.e., supervised, unsupervised, and FL, and cryptographic protocols such as secure multi-party computation and blockchain. The research method adopted is systematic literature review, and it exposes patterns, similarity, and divergence between the numerous research approaches.

2.3 Significance of Study

This study expands existing debate about AI-based privacy auditing by describing a structured review of recent advancements and their cross-industry applicability. It highlights the best practices, challenges, and potential solutions to the implementation of ML-based compliance systems in data-intensive environments. The findings of this review can aid policymakers, researchers, and business leaders to develop more effective privacy auditing methods, striking a balance between technological practicability and legality.

2.4 Limitations

The study in question primarily deals with theoretical models and controlled experiments and hence restricts their practical applicability in real-world situations. Moreover, regulatory compliance aspects are usually not covered properly, resulting in a gap between legislative enforcement and technical feasibility. The ethical issues pertaining to biased algorithms and data sovereignty need to be studied further. Additionally, the complexity of ML models creates challenges regarding explainability and accountability, as black-box models have no explanation and are difficult to evaluate.

2.5 Definition of Terms

To increase accuracy and ensure definitional clarity, the following major terms will be defined:

- Privacy auditing is a practice of seeking compliance with the relevant legislation and good practice in data protection.
- Federated Learning (FL) is a decentralized ML paradigm where training is performed node-wise without sharing the data.
- Differential Privacy is a mathematical theory that was developed to make sure that the effect of any individual's data does not change the resulting statistics in a noticeable manner.
- Blockchain is the distributed ledger technology applied to make records unalterable.
- Threat Detection is an identification of prospective security risks to computer systems.
- Multi-Party Computation (MPC) is a cryptographic approach that allows computation in cooperation with other parties while at the same time maintaining data confidentiality.

3. RESEARCH METHODOLOGY

3.1 Research Design

The research in ML-based privacy auditing has been reviewed systematically. Literature was chosen based on significance, relevance, and recency. Comparative analysis has been carried out to establish the strengths and limitations of different ML-based privacy auditing models, research trends, and gaps in research. The results have been summarized in a systematic manner on key developments, a summary of common issues, and a future research roadmap.

3.2 Search Strategy

A critical literature review was conducted through authentic sources such as IEEE Xplore, ACM Digital Library, arXiv, etc. The search employed specific keywords such as "privacy auditing," "machine learning for compliance," and "federated learning privacy" to obtain targeted and specific results. The selection criteria involved articles that were published between 2020 and 2025, with particular emphasis on research that examined ML techniques for compliance, privacy preservation, and security as shown in Fig. 1.

3.3 Data Analysis

The selected articles were categorized under core themes like

threat detection, validation of data integrity, privacy-preserving ML, compliance activity automation, and use of blockchain technology in auditing frameworks. Comparative analysis was carried out based on their respective strengths and weaknesses. Furthermore, the research set forth common trends and research gaps in literature, thereby significantly enhancing the comprehension of the prevailing situation of ML-based privacy auditing.

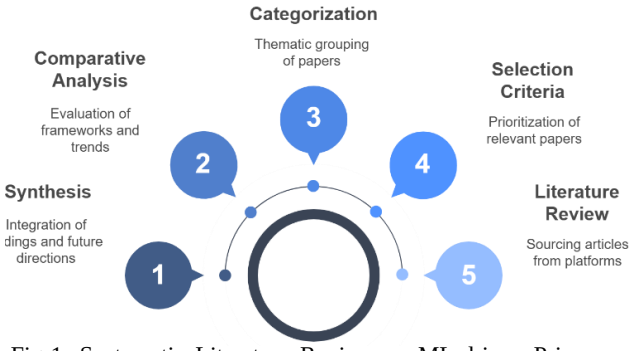

Fig-1: Systematic Literature Review on ML-driven Privacy Auditing

4. RELATED WORK

Various research studies have explored various domains of ML-based privacy auditing and have added the following to the body of literature. A novel IoT security model based on the combination of ML and fog computing was proposed in an effort to further advance the threat detection capabilities [12]. The research offers an overview of IoT network vulnerability and the need for adaptive ML models to detect and counteract the most sophisticated cyber-attacks. Real-time ML-based anomaly detection was employed by the proposed model to advance security in distributed IoT networks to a considerable degree. An AI-compliant system proposed relied on pattern recognition and regulatory mapping processes to facilitate automatic compliance monitoring [13]. The research points out the use of ML algorithms in handling big business data as well as the maintenance of compliance with regulatory regulations like GDPR and CCPA. The system advances compliance audit efficiency through minimized manual intervention as well as maximum real-time compliance enforcement.

A study was conducted to elaborate the efficiency of distributed ML for cloud data integrity verification. [14]. The research suggests a new data integrity verification system applying ML models to detect unauthorized data modification that happens to data stored in the cloud. The suggested system improves data security by detecting inconsistencies and keeping the data unchanged in different nodes in the cloud storage system. Another study evaluated privacy compliance with standards in Android applications and found considerable differences in sharing personal data between mobile applications and third parties [15]. The study found privacy risks embedded in Android devices and illustrated the potential use of ML models in identifying unauthorized data access and imposing privacy policy compliance at the application level.

A critical review of ML privacy protection techniques revealed the limitations of current privacy-protecting techniques [16]. The research concluded that most of the suggested ML privacy mechanisms are not practical in real-world adversarial settings and that more effective and robust privacy-protecting mechanisms are needed. The research necessitates improved testing metrics and adversarial conditions to model the efficacy of ML-based privacy solutions. The use of FL in the scenario of financial audits was explored to maintain data privacy while facilitating collaborative analysis between financial institutions [17]. The study indicates that the use of FL allows organizations to train models without disclosing raw data, thus maintaining data confidentiality and facilitating better identification of fraudulent transactions and financial risk assessment.

Optimized FL with MPC and differential privacy was used in another study to offer better security for privacy-conscious applications [18]. The paper depicts how MPC approaches can be used along with FL in order to even better protect user data without deteriorating model precision. The paper also discusses notable concerns such as computational overhead as well as communications efficiency in FL scenarios. Another selected paper discusses privacy, interpretability, and utility trade-offs in ML systems for tabular data [19]. The paper indicates that privacy-preserving methods, such as differential privacy and FL, will likely lead to less accurate and less interpretable models. The paper provides useful insights into why and how organizations can balance these factors when building ML systems for privacy auditing.

A ML-specific Bayesian differential privacy model has been suggested that provides stronger privacy guarantees for sensitive information [20]. This method enhances the expressiveness of differential privacy by combining Bayesian techniques, thereby making privacy-preserving ML models more adaptable and less vulnerable to inference attacks. A new framework has been put forward for cryptographic auditing to facilitate privacy-preserving ML through cryptographic proofs for adherence compliance while safeguarding sensitive information. The research introduces a secure auditing framework that ensures accountability to stringent privacy requirements [21]. A complete study on privacy-preserving FL has been presented, along with descriptions of challenges and current approaches and future research directions [22]. It provides a solid base for FL and privacy auditing because its usage is presented with reference to the limitations of current implementations, together with recommendations for new approaches to enhancing privacy.

ML has demonstrated its worth in privacy auditing, IoT security enhancement, compliance automation, and cloud data integrity. Research emphasizes ML's capacity to detect threats, enforce rules, and preserve data privacy, particularly via FL and differential privacy. Computational efficiency, regulation adaptation, and model explainability remain challenges. The key points from the literature survey are outlined in Table I.

Table 1. Summary of the Selected Studies (Year Wise)

Year	Publisher Name	Findings	Reference
2020	A. Triastcyn and B. Faltings	Proposed a Bayesian differential privacy model to improve privacy guarantees in ML applications.	[20]
2020	X.-P. Zhao and R. Jiang	Introduced a distributed ML approach for cloud data integrity verification, ensuring security and reliability.	[14]

2021	X. Yin et al.	Conducted a comprehensive survey on privacy-preserving federated learning, identifying challenges and future directions.	[22]
2022	M. Schreyer et al.	Investigated federated learning for financial statement audits, ensuring privacy in collaborative analysis.	[17]
2024	H. Lycklama et al.	Introduced a cryptographic framework for auditing privacy-preserving ML models, ensuring accountability.	[21]
2024	W. Abbasi et al.	Explored trade-offs in ML privacy, explainability, and utility in tabular data analysis.	[19]
2024	C. Zheng et al.	Optimized federated learning with MPC and differential privacy, enhancing security in decentralized AI systems.	[18]
2024	M. Aerni et al.	Critically assessed ML privacy defenses, exposing flaws in evaluation methodologies and effectiveness.	[16]
2024	D. Rodriguez et al.	Analyzed Android app privacy compliance, highlighting inconsistencies in personal data transfers.	[15]
2024	A. M. Almasabi et al.	Developed an ML-powered IoT security framework using fog computing for real-time threat detection.	[12]
2025	S. M. Ali et al.	Proposed an AI-driven compliance automation framework leveraging pattern recognition and regulatory alignment.	[13]

5. RESULT AND ANALYSIS

The growing use of data-driven decision-making and digital technologies has witnessed an unprecedented collection and analysis of data. Organizations in various industries are using advanced analytics, AI, and cloud computing technology to derive insights from big data. Fast growth has also introduced serious privacy and security concerns, especially in terms of complying with regulation standards like the GDPR, the CCPA, and industry-specific regulations like the HIPAA. The latter necessitates organizations to put in place strong privacy controls, institute data protection measures, and build accountability frameworks to comply with regulations.

ML has emerged as a highly influential tool in addressing this problem in an automated manner with its ability in privacy auditing, anomaly detection, and regulatory compliance enforcement. Traditional privacy auditing methods rely on manual effort, which is prone to errors and is faced with significant scalability issues. As organizations collect more data, traditional compliance auditing methods have been found to be insufficient. ML-based methods, however, have enhanced efficiency in the processing of large data sets, the identification of anomalous patterns, and compliance with minimal human intervention.

Improvements in FL, differential privacy, and cryptography have greatly improved the efficiency of ML models in conducting privacy audits without compromising sensitive data. FL allows model training in collaboration without raw data sharing, thus reducing the risk of security breaches. Differential privacy makes each person's contribution to the dataset anonymous, thus preventing re-identification attacks. Blockchain technology has also been integrated into privacy auditing with ML to generate transparent and tamper-evident compliance records, thus promoting accountability and reliability in AI systems.

Despite all these advancements, there are still some problems. Explainability of ML models is one of the key problems, where regulatory bodies require explainability in decision-making. Model poisoning and adversarial attacks also threaten ML-based privacy auditing frameworks, and robust defense strategies are required. Making sure that ML-based compliance frameworks can keep up with evolving legal and regulatory landscapes is another problem, which requires adaptive AI solutions that can dynamically update compliance rules with new legislation.

6. FINDINGS

For RQ1, ML improves privacy auditing with real-time automatic compliance checks, anomaly detection, and security risk mitigation. Unlike non-scalable rule-based audit processes lacking support for expanding data environments, ML models learn more with large data sets and detect privacy breaches prior to violating them. Deep learning and anomaly detection tools improve abnormal data access and usage detection, and organizations can prevent compliance risk ahead of time. Further, predictive analytics on the basis of ML help predict impending threats ahead of time, and privacy auditing is effective and dynamic. With the removal of manual checks and accuracy improvement, ML-based privacy auditing provides strong security and regulation compliance across sectors.

Referring to RQ2, various technical approaches enable ML-based compliance automation, and all enable more secure enforcement of privacy, i.e.: Supervised models tag data behavior to detect non-compliance, while unsupervised approaches detect anomalies that may signal privacy breach. FL enables models to be trained from distributed data without exposing raw data, enabling compliance in data-sensitive industries. Differential privacy controls add noise in datasets, making raw data extraction unattractive while enabling analytical value. Blockchain-based ML platforms enable open and immutable compliance records, enabling audibility. Secure MPC also enables privacy by enabling joint data analysis without exposing single data points. These approaches all enable integrity and volume of ML-based privacy audits.

Based on RQ3, while ML-based privacy auditing is shown to be effective, it is confronted with several challenges, such as those related to explainability, computational complexity, and regulatory flexibility. Black-box models are the most widely used categories of ML models, leading to challenges with explaining the results in relation to regulatory compliance, thus making compliance with regulations difficult. Methods such as FL and differential privacy, while suitable for ensuring privacy, are confronted with inherent compromises between model accuracy and computational cost. Furthermore, adversarial attacks undermine the integrity of ML models, making them susceptible to tampering and thus diminishing privacy protection. Integrating ML-based privacy audits into adaptive legal systems presents another significant challenge, which requires models to be flexible so that they

can be constantly refined based on regulatory feedback.

In the instance of RQ4, one notices a range of ML strategies with different levels of accuracy, scalability, and regulatory adherence. Deep learning strategies demonstrate high accuracy in detecting privacy violations; however, non-explainability poses significant challenges to their implementation in compliance systems. FL enables collaborative model training with guaranteed user privacy protection but is associated with considerable communication overhead and intrinsic security vulnerabilities. Differential privacy ensures data confidentiality but at the expense of model accuracy. Additionally, blockchain-based ML auditing facilitates transparency but is constrained by scalability due to high computational demands. In pursuing an optimal balance among these trade-off factors, researchers have been investigating hybrid artificial intelligence strategies that combine and reconfigure different ML techniques with the aim of enhancing the efficiency of privacy auditing.

To address RQ5, FL is the key to privacy-aware framework development in auditing because it facilitates model training in a decentralized manner and data privacy. FL is most relevant to areas such as healthcare and finance, in which stringent privacy regulation restricts data sharing. It enables HIPAA regulation compliance without raw data sharing, thereby reducing exposure risk. High communication cost, slow model convergence, and susceptibility to poisoning attacks are issues that must be overcome for FL to be effective for privacy auditing. Secure aggregation techniques and adversarial robustness improvements can enable it to be effective for privacy auditing.

To respond to RQ6, future work needs to make privacy auditing using ML legal, transparent, and scalable. Explainable AI (XAI) methods need to be adopted so that transparency is ensured in compliance decisions to make ML models more reliable for regulatory authorities. FL improvements, i.e., minimizing communication overhead and enhancing security mechanisms, will make it more practical in applications. Quantum-resistant cryptographic methods need to be employed in ML auditing so that data security is future-proof. Hybrid AI models integrated with blockchain, differential privacy, and adaptive learning algorithms can also ensure more secure privacy-preserving compliance models. Algorithmic fairness and bias in ML models will also be needed to make privacy

7. CONCLUSION

ML has extensive implications for privacy auditing because it can create scalable, automated, and efficient compliance processes. ML surpasses the conventional method in threat detection, data consistency checks, and testifying regulatory compliance. Malleability of law, over-reliance on computational power, and interpretability of black-box model justification are concerns, but ML algorithms complicate transparency and make it impossible in some instances because the internal process is unknown. In addition, dynamic data privacy law environments need adaptive AI frameworks that adapt dynamically to dynamic rules and regulations. Sophisticated privacy techniques such as differential privacy and FL offer secure data analysis with leakage of sensitive data without compromise but at the expense of performance at the cost of scalability. Blockchain integration enhanced auditability of open and unalterable data logs but is energy-intensive, non-extensible, and expensive. XAI design consideration will be required in future development to enhance model interpretability and enable trust in compliance decision-making. FL must be developed to enhance efficiency, security, and adversarial robustness. AI compliance systems must be designed to incorporate self-learning so that they are able to learn from compliance with changing regulations. Quantum-resistant cryptographic protocols will be required for long-term information security. Lastly, ethical concerns like algorithmic bias and fairness must be addressed in order to avoid discriminatory decision-making in compliance systems.

8. REFERENCES

[1] E. Berghout, R. Fijneman, L. Hendriks, M. de Boer, and B.-J. Butijn, Advanced Digital Auditing, Progress in IS, Springer International Publishing, 2022.https://doi.org/10.1007/978-3-031-11089-4

[2] A. Agarwal, “AI-Powered Data Management and Governance in Retail,” International Journal of Data Mining & Knowledge Management Process (IJDKP), vol. 15, no. 2, pp. 89–102, Mar. 2025. https://aircconline.com/ijdkp/V15N2/15225ijdkp07.pdf

[3] A. Agarwal, S. Kumar, P. Chilakapati, and S. Abhichandani, “Artificial Intelligence in Data Governance Enhancing Security and Compliance in Enterprise Environments,” Nanotechnology Perceptions, vol. 20, no. 1, pp. 34–45, 2024. [Online]. Available: https://nano-ntp.com/index.php/nano/article/view/4984

[4] E. De Cristofaro, "An overview of privacy in machine learning," arXiv preprint arXiv:2005.08679, 2020. https://doi.org/10.48550/arXiv.2005.08679

[5] A. Daghighi, "Application of an Artificial Neural Network as a Third-Party Database Auditing System," M.S. thesis, St. Cloud State University, 2019.https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1118&context=msia_etds

[6] V. Jain, A. V. Balakrishnan, D. Beeram, M. Najana, and P. Chintale, "Leveraging Artificial Intelligence for Enhancing Regulatory Compliance in the Financial Sector," International Journal of Computer Trends and Technology, vol. 72, no. 5, p. 124, 2024. https://doi.org/10.14445/22312803/ijctt-v72i5p116

[7] A. R. M. Pant, "Importance of data security and privacy compliance," International Journal for Research in Applied Science and Engineering Technology, vol. 11, no. 11, p. 1561, 2023. https://doi.org/10.22214/ijraset.2023.56862

[8] M. Sun and Y. Qu, "IT audit education implemented under cloud accounting," in Proceedings of the 2020 International Conference on Advanced Education and Management Science (AEMS), 2020. https://doi.org/10.2991/assehr.k.200801.009

[9] A. M. Tall, J. Wang, and D. Han, "Survey of data intensive computing technologies application to security log data management," in Proceedings of the 3rd IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT), 2016, p. 268. [Online]. Available: https://doi.org/10.1145/3006299.3006336

[10] M. Yin, "Data security and privacy preservation in big data age," in Proceedings of the 2017 International Conference on Management Engineering, Information Technology, and Management Innovation (ICMEIT), 2017. [Online]. Available: https://doi.org/10.2991/icmeit-

17.2017.76

[11] A. Raj and R. Deora, “AI and ML Powered Feature Prioritization in Software Product Development,” International Journal of Data Mining & Knowledge Management Process (IJDKP), vol. 15, no. 1, pp. 23–30, Jan. 2025.https://aircconline.com/ijdkp/V15N1/15125ijdkp02.pdf

[12] A. M. Almasabi, M. Khemakhem, F. E. Eassa, A. Ahmed Abi Sen, A. B. Alkhodre and A. Harbaoui, "A Smart Framework to Detect Threats and Protect Data of IoT Based on Machine Learning," IEEE Access, vol. 12, pp. 176833-176844, 2024.https://doi.org/10.1109/ACCESS.2024.3498603

[13] S. M. Ali, A. Razzaque, M. Yousaf and R. U. Shan, "An Automated Compliance Framework for Critical Infrastructure Security Through Artificial Intelligence," IEEE Access, vol. 13, pp. 4436-4459, 2025.https://doi.org/10.1109/ACCESS.2024.3524496

[14] X. -P. Zhao and R. Jiang, "Distributed Machine Learning Oriented Data Integrity Verification Scheme in Cloud Computing Environment," IEEE Access, vol. 8, pp. 26372-26384, 2020.https://doi.org/10.1109/ACCESS.2020.2971519

[15] D. Rodriguez, J. M. Del Alamo, C. Fernández-Aller and N. Sadeh, "Sharing is Not Always Caring: Delving into Personal Data Transfer Compliance in Android Apps," IEEE Access, vol. 12, pp. 5256-5269, 2024.https://doi.org/10.1109/ACCESS.2024.3349425

[16] M. Aerni, J. Zhang, and F. Tramèr, "Evaluations of Machine Learning Privacy Defenses are Misleading," in Proceedings of the 2024 ACM Conference on Computer and Communications Security (CCS '24), Zurich, Switzerland.https://doi.org/10.1145/3658644.3690194

[17] M. Schreyer, T. Sattarov, and D. Borth, "Federated and Privacy-Preserving Learning of Accounting Data in Financial Statement Audits," in Proceedings of the 3rd ACM International Conference on AI in Finance (ICAIF '22), New York, NY, USA, Nov. 2022.https://doi.org/10.1145/3533271.3561674

[18] C. Zheng, L. Wang, Z. Xu, and H. Li, "Optimizing Privacy in Federated Learning with MPC and Differential Privacy," in Proceedings of the 2024 3rd Asia Conference on Algorithms, Computing and Machine Learning (CACML 2024), Shanghai, China, Mar. 2024.https://doi.org/10.1145/3654823.3654854

[19] W. Abbasi, P. Mori, and A. Saracino, "Further Insights: Balancing Privacy, Explainability, and Utility in Machine Learning-based Tabular Data Analysis," in Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024), Vienna, Austria, Jul. 2024https://doi.org/10.1145/3664476.3670901

[20] A. Triastcyn and B. Faltings, "Bayesian Differential Privacy for Machine Learning," in Proceedings of the 37th International Conference on Machine Learning (ICML 2020), Online, PMLR 119, 2020.https://doi.org/10.5555/3524938.3525826

[21] H. Lycklama, A. Viand, N. Küchler, C. Knabenhans, and A. Hithnawi, "Holding Secrets Accountable: Auditing Privacy-Preserving Machine Learning," arXiv preprint, 2024.https://doi.org/10.48550/arXiv.2402.15780

[22] X. Yin, Y. Zhu, and J. Hu, "A Comprehensive Survey of Privacy-Preserving Federated Learning: A Taxonomy, Review, and Future Directions," ACM Computing Surveys (CSUR), vol. 54, no. 6, art. 131, Jul. 2021.https://doi.org/10.1145/3460427