MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3118-3122

Privacy Assurance Routine Using Natural Attributes (PARUNA): A Hybrid Framework for Privacy Assurance

[1]M. Kannan, [2] Balaji Seshan
[1]Assistant Professor,[2] Ph.D Research Scholar,
Départment of Computer Science and Applications,
Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, Enathur, Kanchipuram, India.
Email:saikannan1999@kanchiuniv.ac.in, vibal@rediffmail.com

Abstract

Privacy is widely recognized as a fundamental human right, forming the cornerstone of individual autonomy and trust in digital interactions. However, safeguarding this right in today's AI-driven, hyper-connected ecosystem presents significant challenges. The complexity arises from the sheer scale of data flows, algorithmic decision-making, and cross-border processing, which amplify risks of misuse and erosion of user control. Traditional privacy engineering techniquessuch as anonymization (removing identifiers from datasets), encryption (mathematical methods to secure data in transit and at rest), differential privacy (adding statistical noise to protect individual records), and synthetic data generation (creating artificial datasets for analysis)—offer essential technical defenses. Yet, these measures alone do not fully address broader dimensions like governance frameworks, regulatory compliance obligations, and human behavioral factors such as consent fatigue or trust perception.

Keywords: Privacy by Design, Privacy Engineering, Differential Privacy, Anonymization, Encryption, Governance, Consent, Human-Centric Design, Behavioral Privacy, Privacy Enhancing Technologies -PETs, ARUNA.

1.Introduction

Organizations today collect, store, process, and analyze enormous volumes of data for diverse business purposes and frequently share data with third party vendors and service providers across borders, creating complex privacy risks and regulatory obligations. Technical privacy solutions are advancing rapidly: a comprehensive survey on privacy enhancing technologies (PETs)[1] for collaborative machine learning details secure multiparty computation, homomorphic encryption, differential privacy, and confidential computing—each tied to explicit threat models and implementation guidelines for practitioners. In sensitive domains such as healthcare, federated learning with differential privacy mitigates leakage during distributed model training while retaining utility, and homomorphic encryption based predictive schemes demonstrate privacy preserving clinical decision support. However, engineering techniques only partially satisfy broader privacy protection objectives (purpose limitation, data minimization, consent lifecycle, data subject rights, retention and secure disposal, and grievance redressal). PbD guidance emphasizes embedding privacy from inception, continuous monitoring, and robust governance to achieve accountability and verifiable compliance.

Complementary IEEE and Systemsstandards [6] (e.g., IEEE 7002 for the data privacy process; ISO/IEC 27701 for Privacy Information Management Systems; ISO/IEC 29184 [6] for online notices and consent) further underscore the importance of integrating policy enforcement and lifecycle controls with technical measures.

In parallel, a recent systematic literature review on Privacy Requirements Engineering argues for a holistic, standardized process across the software development lifecycle—combining technical, organizational, and regulatory dimensions—reinforcing the need for hybrid frameworks like PARUNA.

This paper introduces PARUNA—Privacy Assurance Routine Using Natural Attributes—a conceptual framework grounded in the principles of Privacy by Design (PbD). PARUNA is built on three interdependent layers:

1. Technical Controls: Mechanisms that provide runtime enforcement and safeguard data integrity and confidentiality. These include encryption, anonymization, consent management APIs, and privacy-preserving machine learning techniques such as differential privacy.
2. Policy-Driven Governance: Formal structures and processes that ensure compliance with legal and regulatory obligations. This layer encompasses Data Protection Impact Assessments (DPIAs), lawful basis mapping, vendor risk management, and adherence to frameworks like GDPR and India's DPDPA.
3. Human-Centric Design Principles: Rooted in natural attributes such as autonomy (user control over personal data), transparency (clear and timely communication of data practices), and accountability (verifiable evidence of compliance). This layer ensures that privacy is not only technically enforced but also perceived and trusted by end users.

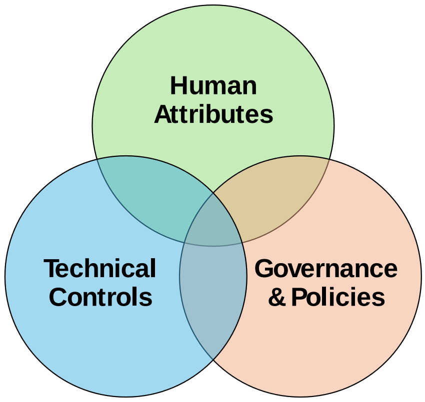

Fig 1: Privacy Assurance Routine Using Natural Attributes-.PARUNA

Together, these layers form a holistic assurance routine that is adaptive to evolving risks, measurable through defined metrics, and resilient against emerging threats in AI-driven ecosystems. To operationalize this approach, the framework introduces Privacy Maturity Levels (PML)a structured scoring model based on these parameters. PML enables product and application owners to monitor privacy posture continuously and take mid-course corrective or preventive actions to meet compliance and trust objectives.

PARUNA is positioned to adapt to dynamic environments influenced by Agentic AI, IoT, big data analytics, and emerging quantum era risks, thereby enhancing usability, trust, and compliance across the data lifecycle. Guidance from PbD practice and IEEE/ISO standards underscores the need for such hybrid models.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3118-3122

Table 1. Privacy-Enhancing Technologies (PETs) and Their Roles in the PARUNA Framework

Technique	What It Does	Role in PARUNA
Homomorphic Encryption (HE) [3][11][12]	Enables computations on encrypted data without decryption. Example: Cloud can process encrypted health records securely.	Strengthens Technical Controls by allowing secure processing in untrusted environments while maintaining confidentiality.
Differential Privacy (DP)- [3][11][12]	Adds statistical noise to datasets to prevent identification of individuals while preserving aggregate insights.	Supports Human-Centric Design by reducing re-identification risk and ensuring transparency in data analytics.
Federated Learning (FL) [3][11][12]	Trains machine learning models across multiple devices without sharing raw data; only model updates are exchanged.	Enhance Technical Controls for AI systems by keeping personal data local and reducing exposure risk.
Synthetic Data Generation [3][11][12]	Creates artificial datasets that mimic real data patterns without exposing actual personal information.	Helps Governance & Compliance by enabling testing and analytics without violating privacy laws or user trust.

2. Literature Review

State of the art Privacy Enhancing Techniques -PETs [1] span differential privacy, homomorphic encryption, secure multiparty computation, and confidential computing, each addressing distinct threat vectors in data analysis, sharing, and model training. Biometric systems pose unique privacy risks due to inherent identifiability and potential extraction of sensitive attributes. A comprehensive survey of privacy enhancing face biometrics catalogs Biometric PETs, evaluation strategies, datasets, and legal obligations under GDPR, highlighting critical open issues. PbD practice emphasizes proactive controls, privacy by default, end to end security, transparency, and user centricity[5], and recommends PIAs/DPIAs and governance procedures to align technical safeguards with regulatory demands. [10][15].

The literature indicates privacy engineering [2] is necessary but not sufficient. Achieving comprehensive privacy assurance requires hybrid models that integrate engineering with governance and human centric design, supported by a holistic Privacy Requirements Engineering process.

Table 2. Literature Review Summary – Privacy Approaches and Research Gaps

Study / Source	Focus Area	Key Contributions	Limitations / Research Gaps
IEEE Access Survey on PETs [1] https://ieeexplore.ieee.org/document/9875277)	Privacy-Enhancing Technologies for ML	Comprehensive review of PETs (DP, HE, SMPC, Confidential Computing); threat models and implementation guidelines	Limited coverage of governance and user-centric aspects; scalability challenges for PETs
EMBC 2022 – Federated Learning [2] https://ieeexplore.ieee.org/document/9871742	Healthcare AI	Demonstrates DP in federated learning for disease prediction; strong technical privacy	Does not address consent lifecycle or regulatory compliance; usability impact not studied
INFOCOM Workshops – Homomorphic Encryption [3] https://ieeexplore.ieee.org/document/8116480)	E-Health Predictive Models	Privacy-preserving clinical decision-making using HE; resilience against inference attacks	High computational overhead; lacks integration with governance and behavioral safeguards
IEEE T-IFS – Face Biometrics Survey [4] https://ieeexplore.ieee.org/document/9481149)	Biometric Privacy	Catalogs PETs for biometrics; GDPR compliance considerations; evaluation strategies	No holistic framework; behavioral and UX aspects missing
IEEE Digital Privacy – PbD Guidance [5] https://digitalprivacy.ieee.org/publications/topics/architecting-privacy-by-design-from-concept-to-application/)	Privacy by Design Principles	Emphasizes proactive controls, privacy-by-default, transparency, accountability	Conceptual guidance only; lacks technical implementation and behavioral integration
IEEE data privacy Standards Overview [6] https://digitalprivacy.ieee.org/standards/)	Governance & Compliance	Provides structured processes (IEEE 7002, ISO/IEC 27701, 29184) for privacy management	Does not address technical PETs or adaptive resilience for AI/IoT contexts
IEEE Access – Privacy Requirements Engineering [7] https://ieeexplore.ieee.org/document/10478000)	Holistic Privacy Engineering	Advocates embedding privacy requirements across SDLC; identifies gaps in current methods	No operational model combining PETs, governance, and human-centric design
ICCWAMTIP 2021 – Cloud Privacy[8] https://ieeexplore.ieee.org/document/9674141	Data Encryption	Enhances cloud data privacy using encryption; strong technical security	Narrow scope; does not address consent, purpose limitation, or behavioral factors
Privacy by design and the privacy aspects of personal data in the context of inclusive design and services https://www.researchgate.net/publication/368300522_Privacy_by_design_and_the_privacy_aspects_of_personal_data_in_the_context_of_inclusive_design_and_services	Secure Software Development Lifecycle embedded into each phase	Integrating security into each SDLC phase to improve resilience.	Limited coverage of privacy assurance as a first-class outcome and Human centric privacy UX (consent fatigue, explainability etc..)
A systematic literature review of security and privacy by design principles norms and strategies for digital technologies Full article: A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies	proactivity, embeddedness, user-centricity, transparency and stronger regulatory grounding for Privacy By Design	Integrates and contrasts security by Design (SbD)vs. Privacy By Design (PbD) across three lenses—principles, norms, strategies; shows PbD's greater maturity/consensus and normative embedding	Stops at comparative synthesis—no operational assurance model. Quantification of Assurance maturity
Integrating Privacy by Design (PbD) in the system development life cycle https://journalwjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-0538.pdf	Conceptual and theoretical integration of PbD into SDLC models (Agile, Waterfall, DevOps) with emphasis on principles, PETs	Consolidated review of how Privacy by Design (PbD) can be embedded across SDLC phases to mitigate breaches and regulatory risks	Not addressing the gap between privacy policy intention vs execution by providing a systematic method (routine) for enforcing privacy at runtime; lack of granularity in PbD by using natural attributes to automate decisions and reduce human error.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3118-3122

A Critical Approach to Building Secure and Resilient Software _ International Journal of Advanced Engineering Technologies and Innovations https://ijaeti.com/index.php/Journal/article/view/754	Focuses on a security-centric expansion of the SDLC, covering threat modeling, secure coding, vulnerability scanning, and secure architecture	Emphasizes the importance of embedding security controls across all SDLC phases to reduce vulnerabilities early, prevent costly late-stage fixes, and improve resilience against breaches.	Not addressing the execution gap between privacy policies and real-world implementation. insufficient enforcement of privacy principles lack of attribute-driven privacy decisions, and missing automation for ongoing compliance and minimization.
Privacy by design from technologies to architecture https://link.springer.com/chapter/10.1007/978-3-319-06749-0_1	systematic architectural analysis, formal modeling, and design-space exploration	shifting PbD toward architectural-level methodologies. Highlights the importance of formal methods and architecture-driven exploration of privacy design choices.	Not enforcing privacy constraints continuously at runtime across services and data flows. This is also not addressing privacy methodology into repeatable routines (policy as code)
Our work	Privacy Assurance Routine using Natural Attributes (PARUNA)	Enhanceprivacy assurance by considering the natural attributes in Technical and regulatory & Compliance layer- A multi-layered, adaptive framework combining technical controls, governance policies, and human-centric attributes for resilient privacy assurance while developing new system. This can also help the product owner /Solution architect to understand the maturity level of the existing system.	

3.Problem Statement

Despite mature PETs, organizations struggle to consistently enforce purpose limitation, consent lifecycle, rights enablement, and retention/disposal while maintaining usability and business functionality. AI& Data engineering systems exacerbate these challenges through dynamic data flows: AI systems often operate in environments where data is continuously changing (e.g., real-time transactions, IoT streams, social media feeds). This creates a moving target for models. If dynamic data flow is not managed then models may make decisions based on stale or incomplete data, leading to errors or bias.

Privacy Engineering concern: Continuous and real-time data streams make it harder to enforce privacy controls consistently. Sensitive data may move across systems without proper anonymization or consent checks, increasing the risk of unauthorized access or leakage

Model drift:The statistical properties of input data or the relationship between features and outcomes change. This is common in fraud detection, recommendation systems, etc. If drift is ignored, model accuracy degrades silently, leading to poor decisions and compliance failures.

Types of Drift:

- Data Drift: Input data distribution changes (e.g., new customer behavior patterns).
- Concept Drift: The underlying relationship between features and labels changes (e.g., what constitutes “fraud” evolves).

Privacy preserving (governance and policy) concern: As models adapt to new patterns, they may start using features in ways that violate privacy principles (e.g., inferring sensitive attributes indirectly). Drift can also lead to outdated consent assumptions, causing compliance gaps under laws like GDPR or DPDPA.

Opaque decision-making: Many AI models, especially deep learning systems, operate as “black boxes,” making it hard to explain why a decision was made. Lack of explainability can lead to reputational damage, legal penalties, and ethical concerns

Privacy Assurance concern: Lack of transparency means individuals cannot understand how their data is used or why certain decisions are made. This undermines data subject rights (like the right to explanation) and makes auditing for privacy compliance extremely difficult

Hence, a unified framework is required to bridge technical safeguards with policy enforcement and behavioral safeguards in a verifiable, adaptive manner—consistent with PbD guidance and standards.

4. Proposed Framework: PARUNA

PARUNA is a conceptual Research framework that integrates three complementary layers:

Assurance Routine → Emphasizes systematic, repeatable processes for privacy assurance. (helps to understand the current level of maturity of the requirements and Maturity level of the developed system)

Privacy Assurance → Clearly states the purpose of the framework (ensuring privacy resilience).

Using Natural Attributes → Retains the human-centric focus

1. Technical Control Layer (TCL)
2. Governance & Policy Enforcement Layer (GPL)
3. Human-Centric Design Layer (HCL)

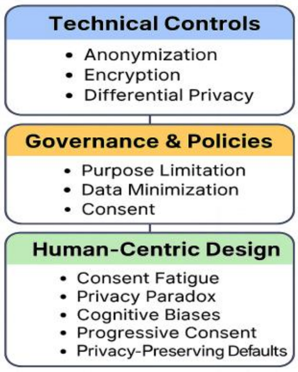

Fig2: Layered approach for Privacy Assurance

1. Technical Controls Layer (Privacy Engineering): Anonymization/Pseudonymization, Differential Privacy, Encryption, Federated Learning, Secure Multi Party Computation, Confidential Computing. The Goal is to Minimize privacy risks through robust technical measures that prevent unauthorized access, leakage, and inference attacks
This layer focuses on privacy engineering principles and Privacy-Enhancing Technologies (PETs) that provide strong technical safeguards for data protection [1]. It includes:

- Anonymization & Pseudonymization
  Removing or masking personally identifiable information so individuals cannot be easily identified.
- Encryption (Data at Rest and in Transit)
  Using cryptographic techniques to secure data during storage and transmission, ensuring confidentiality and integrity.
- Differential Privacy
  Adding controlled noise to datasets or query results to prevent re-identification while preserving statistical utility.
- Federated Learning & Secure Multi-Party Computation
  Enabling collaborative model training without sharing raw data, reducing exposure risks.
- Confidential Computing
  Protecting data during processing using secure enclaves or hardware-based isolation.

2.Governance & Policy Enforcement Layer: Machine-readable policies for purpose limitation, data minimization, retention schedules, cross border transfer safeguards, DPIAs/PIAs, and auditability. The goal is to align technical operations with legal and ethical obligations, ensuring transparency, accountability, and regulatory compliance
This layer ensures compliance with global privacy regulations and organizational accountability. It includes:

- Purpose Limitation
  Data should only be collected and used for clearly defined, legitimate purposes.
- Data Minimization
  Collect only the minimum amount of data necessary for the intended purpose.
- Retention & Secure Disposal
  Define retention periods and ensure secure deletion of data after its intended use.
- Consent Management
  Obtain, track, and manage user consent throughout the data lifecycle.
- Data Subject Rights Enablement
  Provide mechanisms for individuals to exercise rights such as access, correction, erasure, and portability.
- Cross-Border Compliance & DPIAs
  Implement safeguards for international data transfers and conduct Data Protection Impact Assessments for high-risk processing.

3. Human Centric Design Layer (Natural Attributes): Behavioral safeguards addressing consent fatigue, privacy paradox, and cognitive biases via progressive consent, privacy preserving defaults, neutral choice architecture, contextual notices, explainability, and usable recourse. The goal is to embed privacy into user experience by addressing natural human behaviors and cognitive limitations. This layer ensures that privacy controls are intuitive, transparent, and easy to use, reducing user fatigue and preventing manipulative design patterns.
The Human-Centric Design Layer is about making privacy easy and understandable for people. It focuses on how users behave and what they need, so they don’t get overwhelmed or tricked. Make privacy human-friendly, so compliance and protection happen naturally without burdening the user. It includes:

- Consent fatigue: People get tired of too many consent requests. Solution: show clear, simple steps (progressive consent).
- Privacy paradox: People say they care about privacy but often share data easily. Solution: set privacy-friendly defaults.
- Cognitive biases: People can be influenced by how choices are shown. Solution: use neutral, fair design (no dark patterns).
- Contextual notices: Give information at the right time, in the right context.
- Explainability: Make it clear why data is collected and how it’s used.
- Usable recourse: Give easy ways to change settings, withdraw consent, or complain.

5.Methodology

Phase 1: Framework Design: Define PARUNA controls per layer with interface specifications, assurance artifacts, and evidence requirements.
Phase 2: Evaluation Metrics and KPIs: Privacy Risk Index, Privacy Maturity Level, Policy Violation Rate, Consent Quality Score, Rights Fulfillment SLA, Deletion Verifiability, User Trust & Satisfaction.
Phase 3: Comparative Benchmarking: Benchmark PARUNA against engineering only baselines, Compliance only process models, and hybrid models in literature.

6.Conclusion And Scope for the Future Development

Privacy engineering alone cannot deliver comprehensive privacy protection in complex, AI enabled ecosystems. The PARUNA framework offers a robust, hybrid approach that unifies technical controls, policy enforcement, and human centric design, providing end to end assurance across the data lifecycle. By embedding natural human attributes into consent, transparency, and recourse mechanisms, PARUNA enhances usability and trust while maintaining regulatory alignment.

- Quantifying Behavioral Impact
- Governance Automation
- Quantum Resilient Privacy
- Context Drift Detection
- Interoperability Standards
- Machine learning algorithm to implement layered approach

7. References

[1] Y. Liu et al., “A Survey and Guideline on Privacy Enhancing Technologies for Collaborative Machine Learning,” IEEE Access, vol. 10, pp. 97495–97519, 2022.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3118-3122

[2] A. Khanna et al., "Privacy Preserving Model Training for Disease Prediction Using Federated Learning with Differential Privacy," in Proc. IEEE Engineering in Medicine and Biology Conference (EMBC), 2022.
[3] X. Zhang et al., "PCD: A Privacy Preserving Predictive Clinical Decision Scheme with E-Health Big Data Based on RNN," in Proc. IEEE INFOCOM Workshops, 2017.
[4] A. Drozdowski et al., "Privacy-Enhancing Face Biometrics: A Comprehensive Survey," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4147–4183, 2021.
[5] A. Cavoukian, "Architecting Privacy by Design: From Concept to Application," IEEE Digital Privacy Initiative, 2019.
[6] IEEE, "IEEE 7002: Data Privacy Process," 2022. ISO/IEC 27701:2019, "Privacy Information Management". ISO/IEC 29184:2020, "Online Privacy Notices and Consent."
[7] G. B. Herwanto and A. M. Tjoa, "Toward a Holistic Privacy Requirements Engineering Process: Insights From a Systematic Literature Review," IEEE Access, 2024.
[8] S. Sharma et al., "Enhancing Cloud Data Privacy Using Pre-Internet Data Encryption," in Proc. ICCWAMTIP, 2021.
[9] A. Monreale, S. Rinzivillo, F. Pratesi, F. Giannotti, and D. Pedreschi, "Privacy-by-Design in Big Data Analytics and Social Mining," EPJ Data Science, 2014.
[10] S. Wairimu, S. Lindskog, L. Hornivaya, and L. Fritsch, "On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies," in Proc. IEEE Security and Privacy Workshops, 2018.
[11] A. Pattakou, A.-G. Mavroeidi, and C. Kalloniatis, "Towards the Design of Usable Privacy by Design Methodologies," in Proc. Privacy Engineering and Social Informatics, University of the Aegean, 2020.
[12] G. B. Herwanto and A. M. Tjoa, "Toward a Holistic Privacy Requirements Engineering Process: Insights From a Systematic Literature Review," IEEE Access, 2024.
[13] Government of India, The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Aug. 11, 2023.
[14] European Parliament and Council, "Regulation (EU) 2016/679 (General Data Protection Regulation)," Official Journal of the European Union, L119, May 4, 2016.
[15] L. Edwards, "From Privacy Impact Assessment to Social Impact Assessment," in Proc. IEEE Symposium on Security and Privacy Workshops, 2018.
[16] A. A. Klein, "Privacy by Design and the Privacy Aspects of Personal Data in the Context of Inclusive Design and Services," ResearchGate preprint, 2019.
[17] C. Del-Real, E. De Busser, and B. van den Berg, "A Systematic Literature Review of Security and Privacy by Design Principles, Norms and Strategies for Digital Technologies," Computer Law & Security Review, 2021.
[18] I. N. Obiokafor, M. E. Ajonuma, and F. C. Aguboshim, "Integrating Privacy by Design in the System Development Life Cycle for Enhanced Data Protection," International Journal of Information Management, 2022.
[19] J. Adam, "Secure Software Development Lifecycle: A Critical Approach to Building Secure and Resilient Software," Tulane State University, 2020.
[20] T. Antignac and D. Le Métayer, "Privacy by Design: From Technologies to Architectures," in Privacy Technologies and Policy, Springer, 2014.
[21] G. Menon and K. S. G. Narayan, "Data Protection and Data Privacy," ISACA Journal, 9th ed., 2021.
[22] K. Lewis, J. Kaufman, M. Gonzalez, A. Wimmer, and N. Christakis, "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network," Journal of Computer-Mediated Communication, vol. 14, no. 1, pp. 79–100, 2008.
[23] A. Rachovitsa, "Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue," International Journal of Law and Information Technology, vol. 24, no. 4, pp. 374–399, 2016.
[24] J. E. Møller, "Situational Privacy: Theorizing Privacy as Communication and Media Practice," Media, Culture & Society, 2019.
[25] M. J. Taylor and J. M. Paterson, "Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection," International & Comparative Law Quarterly, 2020.
[26] M. Gomez-Barrero, C. Rathgeb, and C. Busch, "Advances in Privacy-Preserving Biometrics: 2025 Update," *IEEE Transactions on Information Forensics and Security*, 2025.
[27] A. Cavoukian, "Operationalizing Privacy by Design in AI-Driven Systems," IEEE Security & Privacy, vol. 23, no. 1, 2025.
[28] T. Antignac and D. Le Métayer, "Engineering Privacy Architectures in the Era of AI Regulation," in Proc. IEEE European Symposium on Security and Privacy (EuroS&P), 2025.