A. Munoz, J. Lopez, C. Alcaraz and F. Martinelli, "Trusted Platform and Privacy Management in Cyber Physical Systems: The DUCA Framework", *IFIP Annual Conference on Data and Applications Security and Privacy*, vol. 15722, 2025.
http://doi.org/10.1007/978-3-031-96590-6_12
NICS Lab. Publications: https://www.nics.uma.es/publications

Trusted Platform and Privacy Management in Cyber Physical Systems: The DUCA Framework

Antonio Muñoz[1][0000−0002−6751−0625], Javier Lopez[1][0000−0001−8066−9991], Cristina Alcaraz[1][0000−0003−0545−3191], and Fabio Martinelli[2]

[1] Network, Information and Computer Security Lab (NICS), Languages and Computer Science Department, University of Malaga, Malaga, Spain.
{anto,javierlopez,alcaraz}@uma.es
[2] Security Group Istituto di Informatica e Telematica - IIT, National Research Council - C.N.R., Pisa, Italy Fabio.Martinelli@iit.cnr.it

Abstract. This paper explores the application of the DUCA (Data Usage Control and Compliance Architecture) framework for privacy management in Cyber-Physical Systems (CPS). DUCA integrates Privacy-by-Design (PbD) principles, Privacy-Enhancing Technologies (PETs), and context-aware policy enforcement to support regulatory compliance and protect data throughout its lifecycle. A key focus of this work is the integration of Secure Elements (SEs)—including Trusted Execution Environments (TEE), Trusted Platform Modules (TPM), and Intel SGX—to enable privacy protection during data processing, complementing traditional safeguards for data at rest and in transit. The framework also supports emerging standards such as DICE and MARS to facilitate scalable trust management in heterogeneous CPS environments. We present DUCA's modular architecture and evaluate its applicability across representative use cases, including smart grids, eHealth, and AI-enabled infrastructures, demonstrating its effectiveness in enforcing privacy without compromising functionality.

Keywords: Privacy Management · Secure Elements · Privacy-by-Design · Data Usage Control · Cyber-Physical Systems · GDPR Compliance

1 Introduction

Cyber-Physical Systems (CPS) are increasingly central to sectors such as energy, healthcare, transportation, and manufacturing, where the interplay between digital intelligence and physical processes enables real-time, data-driven decision-making. However, the dynamic, distributed, and heterogeneous nature of CPS introduces significant challenges for privacy and security, particularly regarding the protection of sensitive data throughout its lifecycle. Ensuring robust privacy in these environments requires not only regulatory compliance—such as adherence to the General Data Protection Regulation (GDPR)—but also the integration of security mechanisms that operate effectively at both software and hardware levels.

Traditional privacy strategies, rooted in Privacy-by-Design (PbD) principles, employ Privacy-Enhancing Technologies (PETs) such as anonymization, pseudonymization, encryption, and differential privacy. While effective for securing data at rest and in transit, these techniques often fall short when it comes to safeguarding data during computation—a critical stage in CPS where information is actively processed and acted upon in real time. This limitation has prompted interest in Secure Elements (SEs), such as Trusted Execution Environments (TEEs), Trusted Platform Modules (TPMs), and Intel Software Guard Extensions (SGX), which enable privacy policy enforcement within tamper-resistant hardware contexts.

This work is conducted within the scope of the DUCA (Data Usage Control and Compliance Architecture) project, which investigates scalable, policy-driven approaches to privacy in CPS. DUCA combines PETs, dynamic and context-aware policy enforcement, and Secure Elements into a modular architecture that supports compliance and privacy-aware data usage. In this paper, we focus specifically on the integration and evaluation of Secure Elements within this framework, analyzing their suitability for runtime enforcement of privacy policies in heterogeneous CPS scenarios.

The main contribution of this work lies in the detailed examination of how hardware-based Secure Elements can be employed to extend privacy protection to data-in-use, addressing a gap in conventional PET-centric frameworks. We provide a comparative analysis of SE technologies—including TEE, TPM, SGX, SEV, DICE, and MARS—highlighting their trade-offs in terms of isolation guarantees, attestation capabilities, performance, and applicability across CPS domains. Furthermore, we demonstrate the relevance of these technologies through three representative use cases: smart grids, eHealth, and big data analytics, each with distinct operational and regulatory constraints.

The remainder of the paper is structured as follows. Section 2 presents background and related work on privacy management in CPS. Section 3 describes the DUCA architecture and its privacy-relevant components. Section 4 examines the integration of Secure Elements and analyzes their capabilities. Section 5 presents representative application scenarios and evaluation insights. Finally, Section 6 concludes the paper and outlines directions for future work.

2 Background and Related Work

Ensuring privacy in Cyber-Physical Systems (CPS) has become a pressing challenge as these systems manage vast volumes of sensitive data across interconnected and dynamic infrastructures. Unlike conventional IT environments, CPS operate in real-time contexts where continuous data flows introduce complex privacy risks. These challenges have led to the adoption of Privacy-by-Design (PbD) principles and Privacy-Enhancing Technologies (PETs), integrating privacy directly into system architectures.

Historically, privacy evolved from the notion of "the right to be alone" [1] to the modern concept of information privacy, centered on individuals' control

over personal data [2]. The General Data Protection Regulation (GDPR) [3], enforced since 2018, formalizes these principles, mandating not only protection measures but also demonstrable compliance. PbD, codified in GDPR Article 25 [4] and conceptualized by Cavoukian [5], promotes the proactive embedding of privacy throughout the system lifecycle. DUCA adopts PbD not just as a regulatory response but as a core design principle, embedding protections from the outset—particularly vital in CPS environments characterized by high-frequency processing of sensitive data.

CPS tightly integrate computational and physical components [6, 7], and are deployed in critical sectors such as energy, healthcare, manufacturing, and transportation [8–10]. Their heterogeneity, inclusion of legacy technologies, and diverse operational contexts pose privacy and security challenges. For instance, in healthcare, CPS handle sensitive patient data under strict confidentiality requirements [11]. DUCA addresses these risks through a distributed, adaptable framework that ensures consistent enforcement of privacy policies across components and stakeholders with distinct obligations. This approach mitigates risks such as service disruption or public safety threats by embedding privacy within both data management and decision-making processes.

DUCA operationalizes PbD through the use of PETs including data minimization, anonymization, and user-centric privacy controls [12]. These technologies secure data across its lifecycle—from collection and processing to storage and sharing—without compromising utility. Complementing this, DUCA incorporates privacy risk assessment tools that support early vulnerability detection and continuous monitoring, essential for real-time CPS. Transparent interfaces further empower users to manage privacy preferences, reinforcing GDPR principles and supporting DUCA's sustainable deployment.

PETs such as anonymization and pseudonymization reduce re-identification risks, while encryption safeguards data at rest and in transit [13]. Differential privacy enhances analytics by introducing statistical noise, maintaining aggregate utility while protecting individual identities. DUCA integrates these PETs with dynamic, policy-driven enforcement mechanisms, allowing adaptation to regulatory and operational demands across domains.

Beyond technical controls, CPS privacy governance requires policy management, auditing, and accountability [14]. DUCA supports context-aware privacy enforcement that adapts controls to data types and operational contexts. Mechanisms such as audit trails and secure logging establish transparency, enabling compliance verification and fostering trust.

The DUCA framework builds upon prior research emphasizing the need for adaptable and modular privacy management. Approaches using digital twins for dynamic policy adjustment [15] and privacy architectures such as Sovereign [16] and Eden [17] demonstrate the viability of embedded privacy in complex environments. DUCA extends these concepts by combining PbD and PETs throughout the system lifecycle and across heterogeneous CPS deployments.

3 DUCA Architecture and Privacy-Oriented Integration

The DUCA (Data Usage Control and Compliance Architecture) framework is designed to support privacy-preserving, regulation-compliant data usage in complex CPS environments, including smart grids, healthcare systems, and large-scale analytics infrastructures. It adopts a modular architecture that integrates Privacy-Enhancing Technologies (PETs), dynamic usage control, and hardware-based Secure Elements (SEs) to protect data throughout its lifecycle.

Figure 1 provides an overview of DUCA's main components. The DSA Lifecycle Infrastructure (DLI) manages the specification and storage of Data Sharing Agreements (DSAs) through a user interface, a policy authoring tool that converts high-level rules into controlled natural language (CNL), and a DSA Mapper that translates these policies into enforceable formats (e.g., U-XACML). The DSA Store enables persistence and retrieval of DSAs.

The DLI connects to the DSA Enforcement Infrastructure (DEI), which interprets and enforces usage policies in real time. Supporting this process are two additional layers: the Common Security Infrastructure (CSI), which provides identity management, encryption services, and auditing; and the Advanced Security Infrastructure (ASI), which handles PET integration and anonymization functions. Together, these components ensure that privacy policies are enforceable, traceable, and adaptable across distributed CPS components.

To validate the flexibility of the architecture, DUCA has been applied to several representative use cases. In smart grid systems, anonymization modules within ASI and enforcement via DEI ensure that real-time consumption data is protected using Intel SGX enclaves. In big data analytics, DUCA combines PETs (e.g., differential privacy) with CSI's auditing and enforcement capabilities to regulate large-scale query operations. In transportation systems, DUCA supports the definition of context-aware DSAs through the DLI, while CSI handles identity abstraction and consent tracking, and ASI ensures anonymization prior to data release.

A key feature of DUCA is its integration of Secure Elements to support privacy policy enforcement during computation—an area typically underserved by software-only approaches. TEEs such as ARM TrustZone and Intel SGX isolate execution environments, enabling secure analytics. TPMs provide attestation and secure key storage, while confidential computing platforms such as AMD SEV facilitate encrypted processing at the virtualization layer. Unlike previous frameworks relying solely on software controls [14, 18], DUCA embeds hardware-backed trust anchors that enhance resilience against privileged-level attacks.

This integration of Secure Elements complements existing PETs and reinforces DUCA's capacity to enforce privacy policies across all stages of the data lifecycle. It specifically addresses the challenge of protecting data during use—a critical vulnerability in CPS—by executing sensitive operations within hardware-isolated environments. This prevents privacy policies from being bypassed even by privileged software components, thereby enhancing compliance assurance and improving system resilience in real-time settings.

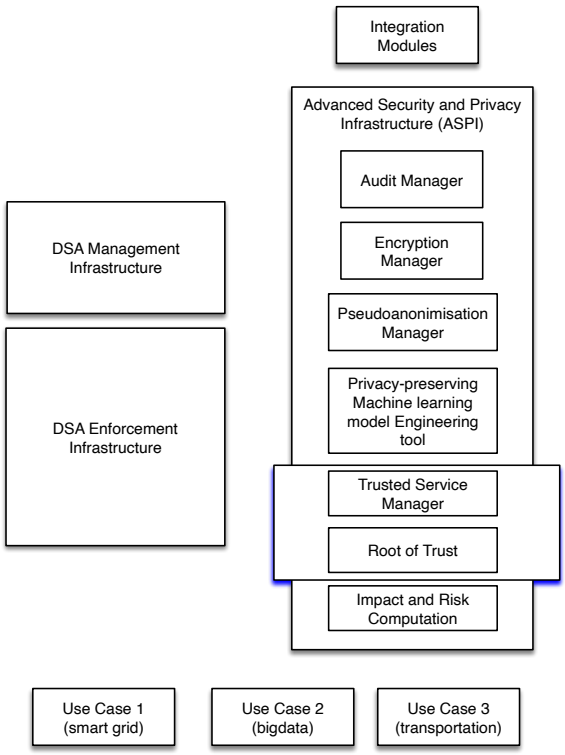

Fig. 1. DUCA Architecture

4 Secure Elements in DUCA: Comparative Analysis and Selection Criteria

The DUCA framework incorporates SE such as TEE, TPM, and Intel Software Guard Extensions (SGX) to ensure robust and tamper-resistant enforcement of privacy policies, especially during data processing, a well-known gap in traditional privacy frameworks.

Table 1 presents a technical comparison of common secure elements used in CPS. It contrasts their isolation levels, latency overhead, memory constraints, platform compatibility, and typical use cases.

Figure 2 presents a comparative overview of all Secure Elements integrated or considered within DUCA, namely TPM 2.0, Intel SGX, AMD SEV, TEE (e.g., TrustZone), DICE, and MARS. Each element is assessed across five critical dimensions: isolation level, latency overhead (normalized inversely), memory capacity, platform flexibility, and resistance to side-channel attacks. Values are

Table 1. Technical Comparison of Secure Elements for CPS Integration

SE	*Isolation*	*Latency*	*Memory*	*Platform*	*Example*
TEE	Medium (isolated OS world)	Low (10–30%) [19]	Moderate (OS shared)	ARM, Mobile, IoT	Smart meters, connected vehicles, medical devices [20]
TPM 2.0	High (discrete chip)	Very Low (sub-ms) [21]	N/A	Windows, Linux, IoT	Device attestation, secure boot, key management [22]
Intel SGX	Very High (enclave-based)	Medium–High (20–60%) [23]	Strict (128MB pre-SGX2)	Intel CPUs	eHealth analytics, encrypted ML, smart grid optimization [24]
AMD SEV	High (VM-level isolation)	Low (VM encryption) [25]	High (full VM encryption)	AMD EPYC servers	Secure cloud data processing, federated learning [25]
DICE	Low–Medium (device-level identity chaining)	Negligible	Minimal (low footprint)	Constrained IoT, ARM Cortex-M	Secure identity for IoT, low-power CPS nodes [26]
MARS	High (modular, attestation-focused)	Low–Medium (platform-dependent)	Flexible (scalable)	General-purpose, Edge/Cloud	Dynamic trust in heterogeneous CPS, fog computing [27, 28]

normalized on a scale from 1 to 5 to facilitate visual comparison and support evidence-based selection in Cyber-Physical System (CPS) contexts.

TPM 2.0 excels in device attestation with negligible latency and broad platform compatibility, making it a foundational element for secure bootstrapping and key management. Intel SGX provides the highest isolation for secure computation, though it is constrained by limited memory and reduced platform flexibility. TEEs offer balanced performance for latency-sensitive CPS tasks, particularly at the edge, while AMD SEV supports scalable virtual machine-level privacy enforcement in cloud infrastructures.

DICE exhibits minimal overhead and maximal flexibility, making it ideal for constrained IoT nodes and low-power CPS environments requiring lightweight identity derivation. MARS contributes enhanced modularity and scalability for attestation and measurement, addressing the trust management needs of heterogeneous, cloud-edge CPS deployments. Collectively, this comparison informs the strategic selection of Secure Elements tailored to specific privacy, performance, and trust requirements in diverse CPS scenarios.

The integration of secure elements into CPS must be guided by application-specific requirements such as real-time responsiveness, data sensitivity, and trust assurance. The selection of the appropriate hardware-based security primitive depends on the operational context, performance constraints, and the level of isolation needed to mitigate threats. This subsection outlines key deployment recommendations tailored to different CPS environments.

Latency-sensitive CPS (e.g., smart grids, autonomous vehicles): Implement TEE (e.g. TrustZone) to enforce privacy policies on the edge with minimal overhead. TEEs enable real-time decision making without significant delay, as demonstrated in privacy-preserving smart metering systems [29].

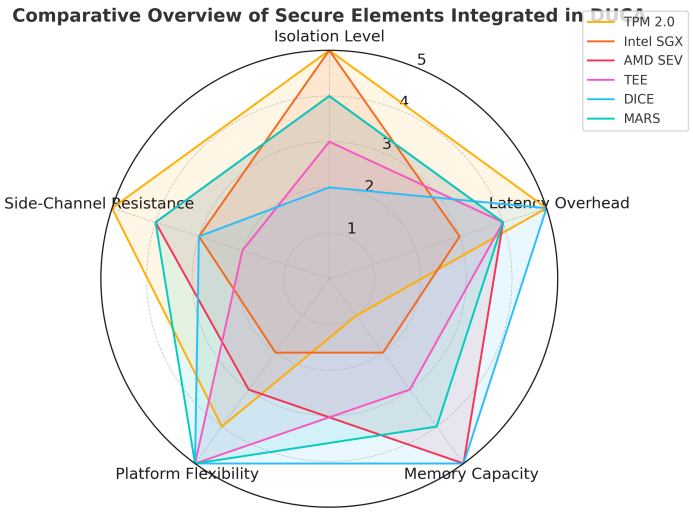

Fig. 2. Comparative overview of Secure Elements integrated or considered in DUCA. The radar chart evaluates TPM 2.0, Intel SGX, AMD SEV, TEE (e.g., TrustZone), DICE, and MARS across five critical dimensions: isolation level, latency overhead (inverted), memory capacity, platform flexibility, and side-channel resistance. Scores are normalized (1–5) for comparative visualization.

Data-intensive environments (e.g., healthcare, big data analytics): Use Intel SGX or AMD SEV to process sensitive data securely. SGX enclaves are ideal for the isolated computation of encrypted health data [30]. AMD SEV, by encrypting entire virtual machines, enables secure analytics in federated learning setups [31].

Device Trust Establishment: TPMs offer hardware-backed attestation and secure key storage, critical in environments requiring proof of device integrity (e.g., in smart manufacturing and IoT deployments) [32].

Although secure elements bring significant benefits for CPS integration, each technology introduces inherent limitations and trade-offs that must be considered during system design. Factors such as memory constraints, performance overhead, and vulnerability to specific attack vectors can affect their suitability for certain applications. This subsection highlights key technical drawbacks associated with leading secure element architectures.

- *SGX Limitations:* Prior to SGX2, enclave memory is limited to 128MB. Paging induces significant performance penalties. SGX is vulnerable to side-channel attacks (e.g. Foreshadow [33]), requiring careful mitigation.
- *TEE Constraints:* TEEs share system resources with the OS, which can pose risks if the OS is compromised. TrustZone's limited cryptographic acceleration restricts complex computation.
- *TPM Boundaries:* TPMs do not support data processing. Their role is limited to key storage, attestation, and secure boot, necessitating complementarity with TEEs/SGX.

DUCA adopts a hybrid Secure Element (SE) integration model in which TPMs are deployed on all CPS nodes to ensure device integrity and secure bootstrapping. TEEs are used to enforce local, context-aware privacy policies on edge devices, such as smart sensors and IoT nodes. In addition, SGX enclaves are used to protect sensitive data during AI processing or analytics in cloud or fog computing environments.

This modular approach allows DUCA to scale privacy enforcement while optimizing for performance and security contextually.

While DUCA currently leverages mainstream Secure Elements (TEE, TPM, SGX), emerging technologies offer enhanced capabilities for privacy protection in CPS.

Intel SGX2: SGX2 introduces dynamic memory management, allowing enclave memory to expand or shrink at runtime. This addresses SGX's earlier 128MB limitation and improves performance for large-scale analytics [34].

ARM Realm Management Extension (RME): An evolution of TrustZone, ARM RME supports finer-grained isolation and improved security management. RME introduces Realms, isolated from both the OS and the hypervisor, which improves the privacy enforcement of edge devices [35].

RISC-V Keystone Enclave: Keystone is an open source, flexible TEE designed for RISC-V platforms. It enables customized enclave security, which is potentially suitable for low-cost CPS nodes and IoT systems [36].

Confidential AI Accelerators: Hardware such as NVIDIA Confidential GPUs and Intel TDX (Trusted Domain Extensions) aims to extend enclave-like protections to GPU and virtualized AI workloads, a promising direction for DUCA's secure AI analytics.

DUCA Roadmap: DUCA's architecture is modular, enabling seamless integration of these next-generation SEs. Future versions will support SGX2 and RME, enhancing scalability and security in complex CPS deployments.

In addition to mainstream Secure Elements such as TPM 2.0 and Intel SGX, the DUCA framework can be extended to incorporate alternative trusted computing standards, enhancing flexibility and platform compatibility. *Trusted Platform Module (TPM) 2.0* provides secure storage for cryptographic keys and hardware-backed attestation capabilities, essential for device integrity validation in Cyber-Physical Systems (CPS) [21]. TPM 2.0 is widely supported across operating systems and hardware, and has been standardized by the Trusted Computing Group (TCG) to ensure robust security baselines [22]. We can see how

DICE and MARS offer lightweight identity derivation and modular attestation capabilities respectively, complementing traditional SEs for diverse CPS scenarios.

Complementing TPM 2.0, the DICE offers a lightweight and scalable alternative. DICE, also standardized by TCG, is designed for constrained devices, enabling secure device identity derivation and trust establishment without requiring a discrete TPM. Its minimal resource requirements make DICE particularly suitable for IoT nodes and low-power edge devices in CPS deployments [37].

Moreover, *Measurement and Attestation Roots (MARS)* represents an emerging framework that emphasizes flexible attestation mechanisms and trust anchors tailored for diverse platforms. MARS enables fine-grained measurement of system states and supports scalable trust establishment across heterogeneous CPS environments [37]. Its modular design accommodates dynamic CPS infrastructures, aligning with DUCA's goals of real-time, context-aware privacy enforcement.

By supporting TPM 2.0, DICE, and MARS, DUCA can adapt trust enforcement mechanisms to diverse operational environments—ranging from high-resource cloud platforms to resource-constrained edge nodes. This flexibility enhances DUCA's ability to manage privacy risks dynamically, ensuring that data usage policies are enforced securely even in heterogeneous and evolving CPS landscapes.

4.1 SE-based Policy Enforcement

Secure Elements (SEs) serve as hardware-based anchors for the enforcement of privacy and security policies in CPS. Unlike frameworks that implement privacy enforcement exclusively in software [14, 18], DUCA relies on SEs to provide trusted execution environments that isolate sensitive computations from the rest of the system stack. This design enhances the enforcement of privacy policies by mitigating risks of tampering or bypass, especially during the data-in-use phase.

Trusted Platform Modules (TPMs) offer a hardware root of trust and enable cryptographic attestation, secure boot, and key sealing. While effective for system integrity verification, TPMs do not provide runtime execution isolation. Trusted Execution Environments (TEEs), such as ARM TrustZone, allow execution of code in a secure world that is isolated from the normal world, offering moderate protection against compromised OS layers but often requiring hardware-specific integration.

Intel Software Guard Extensions (SGX) provide stronger guarantees by allowing designated code to run within enclaves—isolated memory regions that are protected even from privileged software, including the OS and hypervisor. This capability makes SGX particularly suitable for enforcing privacy policies tied to specific data processing tasks. DUCA leverages this feature to ensure that analytics or access decisions on sensitive data are carried out within hardware-protected contexts.

Emerging standards such as DICE (Device Identifier Composition Engine) and MARS (Measurement and Attestation Roots) extend these principles by enabling scalable identity management and layered attestation across resource-constrained

CPS components. Their integration into DUCA supports device-level privacy assertions and supply-chain trust anchoring.

By embedding enforcement mechanisms within SEs, DUCA enhances the resilience of CPS against advanced adversaries and complements PETs by securing data not only at rest or in transit but also during computation. The framework supports dynamic and context-aware privacy policies that are evaluated and enforced in real time, tailored to operational context, user roles, and risk posture.

Table 2. Comparison of Secure Elements for CPS Privacy Enforcement

Technology	**Isolation**	**Attestation**	**Performance**	**Enforcement Scope**
TPM	None (boot-time only)	Supported	Low impact	System integrity verification
ARM TrustZone	Medium (dual-world)	Limited	Low to medium	Secure execution on mobile/IoT
Intel SGX	High (enclaves)	Supported	High for I/O-bound tasks	In-enclave policy enforcement
DICE	None (identity derivation)	Supported	Minimal overhead	Hardware-based device identity
MARS	Not isolation-based	Supported	Minimal overhead	Root-of-trust attestation across platforms

Table 2 summarizes key properties of Secure Elements relevant for privacy enforcement in CPS, comparing their isolation level, attestation support, performance overhead, and scope of enforcement.

5 Application Scenarios and Privacy-Preserving Strategies in Cyber-Physical Systems

This section provides an in-depth overview of three specific use cases addressed by the DUCA project. The following scenarios illustrate how TPM 2.0, SGX, SEV, TEE, and emerging standards such as DICE and MARS are used contextually to enhance privacy enforcement and trust assurance in diverse CPS applications.

5.1 Use Case 1: Smart Grids and Surveillance Systems

The increasing deployment of smart grids enhances efficiency and reliability in energy distribution, but also raises significant privacy concerns, particularly with the integration of surveillance systems that collect data from public environments. Addressing these concerns requires robust security mechanisms to ensure data confidentiality, integrity, and compliance with privacy regulations. End-to-end encryption [38] and real-time pseudonymization techniques such as keyed hash functions [4] have been proposed to secure data transmission and mitigate identity linkage risks in IoT-enabled infrastructures. DUCA builds upon these methodologies by embedding them into a comprehensive data usage control architecture that enforces policies dynamically across interconnected smart grid devices.

A study by [39] explores the privacy challenges in Industry 4.0, emphasizing the importance of differential privacy, federated learning, and homomorphic encryption to secure large-scale, AI-driven data operations. DUCA aligns with these strategies, ensuring privacy-preserving analytics and compliance with GDPR and CCPA by PbD principles and PETs into its core.

The Sovereign framework [40] offers a decentralized smart home model utilizing Named Data Networking (NDN) and data-centric security to enable local control of IoT devices, eliminating reliance on external cloud services. DUCA draws on this approach for privacy-aware data handling in smart grids, emphasizing decentralized control and end-to-end encryption.

Further, a comprehensive review [41] categorizes IoT security frameworks into encryption-based solutions, identity management techniques, and self-protecting data models. DUCA incorporates homomorphic encryption, k-anonymity, and policy enforcement mechanisms to ensure regulatory compliance and data protection even across domain boundaries.

Blockchain's immutability and secure data-sharing capabilities [42] support GDPR compliance through pseudonymization and encryption. DUCA adopts blockchain-based measures to safeguard data throughout its lifecycle. Burnable pseudo-identities [43] enable anonymous, unlinkable interactions in blockchain systems, aligning with DUCA's approach to privacy-centric identity management in CPS.

GDPR-compliant SIEM frameworks [44] highlight early-stage pseudonymization and sanitizable digital signatures for secure and auditable data processing. DUCA integrates these techniques to maintain data usability for security incident detection while protecting personal information.

Overall, DUCA systematically addresses privacy and security challenges in smart grids and surveillance systems through the integration of PETs, decentralized control, and dynamic policy enforcement. Future research includes AI-driven privacy risk assessment and enhanced real-time adaptation of privacy policies.

Enhancing Smart Grid Privacy with Secure Elements: DUCA strengthens privacy protections using Secure Elements:

- *TPM*: Attests the authenticity of smart meters, ensuring trusted data sources.
- *Intel SGX*: Enables real-time grid optimization within secure enclaves, protecting sensitive energy data during processing.
- *TEE*: Enforcement of privacy policies within isolated execution environments, safeguarding energy consumption patterns.
- *DICE*: Provides a lightweight, hardware-backed identity derivation for constrained IoT nodes, enabling trust establishment with minimal overhead.
- *MARS*: Facilitates scalable, platform-independent attestation for heterogeneous smart grid infrastructures, enhancing dynamic policy enforcement.

5.2 Use Case 2: Usage Control for eHealth: Trust-aware Cooperative Services in Mobility

The domain of eHealth, particularly in scenarios enabled by cooperative and cooperative automated mobility (CCAM), presents complex challenges related to

data integrity, trust, and privacy. The continuous exchange of sensitive medical and mobility data increases exposure to potential breaches, particularly when data traverse heterogeneous infrastructures. Distributed ledger technologies (DLTs) have been used to ensure data authenticity and traceability [45], yet these solutions often lack integrated pseudonymization and encryption, leaving personal information vulnerable during transmission.

DUCA addresses this gap by incorporating real-time encryption and pseudonymization of IoT device identities, alongside dynamic context aware data sharing policies. These policies adapt based on factors such as asset location and role, and are enforced with remote attestation techniques to verify the trustworthiness of third-party nodes, thereby ensuring end-to-end data integrity and compliance.

A review by [46] identifies the major privacy challenges in blockchain systems, such as linkage transaction and smart contract vulnerabilities, and proposes cryptographic solutions including Secure Multi-Party Computation (SMPC), Zero Knowledge Proofs (ZKP), homomorphic encryption, and differential privacy. These align with DUCA's objective of enabling secure, privacy-preserving analytics and support for Self-Sovereign Identity (SSI) models, which enhance user control over personal data.

Complementary research by [47] presents a Pseudonym Revocation System (PRS) for IoT healthcare, utilizing elliptic curve cryptography (ECC) to manage pseudonym lifecycles without centralized control. DUCA integrates these principles to balance patient privacy with regulatory compliance.

In addition, a mobile library [48] to anonymize FHIR-compliant health data prior to transmission enables local processing and consent-based data sharing, an approach consistent with DUCA's emphasis on minimizing raw data exposure. Similar objectives are reflected in the methods of minimization of offline data and pseudonymization in real time by [49], further supporting DUCA's strategy.

The EDEN framework [50], employing federated learning for privacy-preserving location data management, illustrates the potential to balance data utility with privacy, informing the approach of DUCA in securing mobility-related eHealth data.

Enhancing eHealth Privacy with Secure Elements: DUCA strengthens privacy in mobile healthcare environments through:

- *Intel SGX*: Enables secure analytics on encrypted patient data within enclaves, preventing unauthorized access.
- *TPM*: Verifies the integrity of mobile healthcare and telemedicine devices, ensuring that only authenticated nodes handle sensitive data.
- *ARM TrustZone*: Executes privacy policies securely on mobile and IoT healthcare devices, protecting data at the edge.
- *DICE*: Supports secure identity chaining for lightweight mobile health devices, ensuring trusted data collection and transmission.
- *MARS*: Enables real-time attestation of third-party healthcare nodes, supporting dynamic and context-aware data sharing policies.

Through these Secure Elements, DUCA ensures robust, context-aware, and regulation-compliant privacy protection across dynamic and distributed eHealth ecosystems.

5.3 Use Case 3: Usage Control for Big Data and AI

Big Data and AI applications pose substantial challenges in managing personal data, especially under stringent privacy regulations such as GDPR. Traditional data protection techniques—anonymization, differential privacy, and homomorphic encryption [51]—provide foundational safeguards but often fall short when data traverse heterogeneous environments, including local and cloud-based infrastructures. DUCA addresses these limitations by enabling flexible, granular data protection through seamless enforcement of data usage policies across diverse platforms. Its architecture integrates PETs to ensure compliance and data security even in evolving threat landscapes.

A comprehensive review by [52] explores privacy risks in Beyond 5G (B5G) and 6G networks, such as unauthorized surveillance and AI-driven re-identification. The study advocates for decentralized AI, homomorphic encryption, and differential privacy—approaches DUCA adopts for privacy-preserving analytics throughout the data lifecycle.

In addition, [53] examines privacy in location-based services via centralized and federated frameworks like MOOD and SAFER. These systems assess privacy risks and enforce protections prior to data publication, supporting DUCA's implementation of PbD in AI environments and federated privacy assessments.

Research by [18] on Data-Centric Security (DCS) using Apache Ranger highlights dynamic data masking and role-based access control, aligning with the aim of DUCA to embed privacy policies in AI infrastructure. Automation via REST APIs enhances DUCA's scalability and interoperability.

Furthermore, [54] presents digital twins in System-of-Systems (SoS) architectures to dynamically manage pseudonymization and encryption critical to DUCA's context-aware privacy enforcement in AI-driven applications. The de-identification techniques explored by [55], including k-anonymity and l-diversity, inform the balance of DUCA between data protection and analytic utility.

Lastly, [56] discusses attribute-centric anonymization and synthetic data generation using Generative Adversarial Networks (GANs). DUCA leverages these methods to enable privacy-preserving AI model training while minimizing personal data exposure.

Enhancing Big Data Privacy and AI Security with Secure Elements: DUCA integrates Secure Elements to ensure privacy-compliant and secure analytics:

- *Intel SGX / AMD SEV*: Supports privacy-preserving machine learning on encrypted data within secure enclaves, maintaining model and data integrity.
- *TPM*: Verifies the authenticity and integrity of the data sources, mitigating the risks of adversarial data poisoning.
- *TEE*: Executes privacy-preserving analytics in isolated environments, enabling dynamic enforcement of privacy policies across cloud and edge infrastructures.

– *MARS*: Provides scalable trust attestation across federated AI infrastructures, ensuring trustworthiness of diverse computing environments during model training and data exchange.

Through these technologies, DUCA enhances AI-driven decision-making while ensuring GDPR compliance and scalable big data privacy protection. While DICE is optimized for constrained environments and is therefore less applicable in this context, MARS contributes effectively to federated trust management by enabling scalable and reliable attestation across diverse AI infrastructures.

5.4 Transversal to Three-Use Cases

Beyond the specific use cases presented, several complementary research efforts contribute transversally to DUCA's privacy-preserving objectives, particularly to advance compliance, data security, and the effective integration of PETs. A comprehensive review [57] of PETs in the automotive sector identifies technological parallels relevant to smart grids, eHealth, and AI analytics, supporting DUCA's adoption of differential privacy, homomorphic encryption, federated learning, and secure multi-party computation. This review also highlights the complexity of cross-organizational data sharing—an inherent challenge addressed within DUCA's modular and policy-driven architecture.

To illustrate how DUCA operationalizes PbD, PETs, and dynamic policy enforcement, Figure 3 outlines its privacy management framework. This model demonstrates DUCA's embedded privacy protections throughout CPS infrastructures, ensuring regulatory compliance while maintaining data utility and operational efficiency.

In line with this, Privacy Level Agreements (PLAs) [58] formalize user-defined privacy preferences within Industrial Data Spaces, complementing DUCA's model-based enforcement of data minimization and purpose limitation. Additionally, scalable anonymization techniques, such as clustering-based k-anonymity with α-deassociation [59], are applicable across DUCA's healthcare and smart grid domains.

A dual layer protection strategy combining blowfish encryption with pseudonymization [60] aligns with DUCA's security model for data confidentiality, particularly during inter-domain sharing. In the IoT context, the categorization of pseudonyms into short-term, session-based, and location-based types [61] informs DUCA's identity management mechanisms, enhancing secure communication in CPS environments.

Moreover, the application of homomorphic encryption to text mining services [5] exemplifies the potential for privacy-preserving analytics, an approach that DUCA extends to surveillance systems and AI-driven decision-making.

Taken together, these contributions reinforce DUCA's commitment to robust, scalable, and regulation-compliant privacy management across diverse CPS applications. Future research will aim to further enhance DUCA's capabilities in privacy-preserving AI, adaptive policy refinement, and real-time privacy risk assessment, thereby supporting its continued evolution as a comprehensive and forward-looking privacy framework.

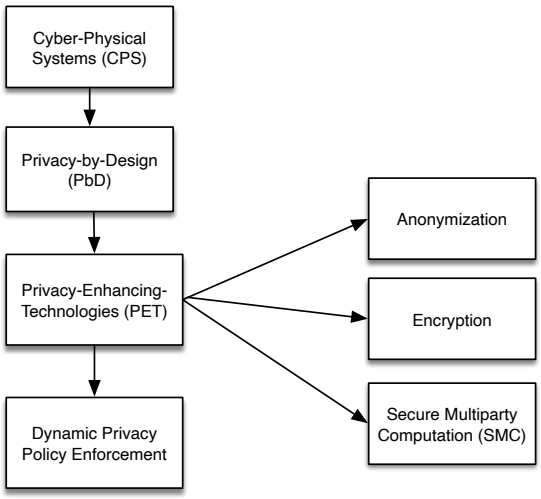

Fig. 3. DUCA Privacy Management Framework: Integration of PbD, PETs, and Dynamic Policy Enforcement

6 Discussion and Conclusions

Designing privacy-aware Cyber-Physical Systems (CPS) remains a complex challenge due to their dynamic, distributed, and heterogeneous nature. The DUCA framework addresses these demands through a holistic Privacy-by-Design (PbD) approach, embedding protection mechanisms across the entire data lifecycle—from generation to storage and sharing—while supporting real-time CPS functionalities.

At its core, DUCA integrates Privacy-Enhancing Technologies (PETs) to enable fine-grained control over data processing without compromising analytical utility. Techniques such as anonymization, pseudonymization, encryption, and differential privacy are combined with adaptive, context-aware policy enforcement to ensure continuous alignment with evolving regulations like the GDPR. This architectural flexibility allows DUCA to accommodate the distinct regulatory and operational needs of various domains, including energy, healthcare, and mobility.

The practical applicability of DUCA has been demonstrated across diverse use cases—ranging from smart grids and industrial systems to AI-enabled healthcare—confirming its ability to reconcile robust privacy protection with the performance constraints inherent to CPS. A key differentiator of DUCA is its

integration of Secure Elements (SEs), such as Trusted Execution Environments (TEE), Trusted Platform Modules (TPM), and Intel SGX. These components enable secure, tamper-resistant execution of privacy policies, enhancing trustworthiness across data in use, in transit, and at rest—surpassing the capabilities of software-only approaches.

Further extending its capabilities, DUCA incorporates emerging trusted computing technologies like DICE and MARS. DICE offers lightweight identity derivation and attestation suited for resource-constrained devices, supporting edge trust establishment with minimal overhead. MARS provides scalable, modular attestation mechanisms for heterogeneous infrastructures. DUCA's modular architecture supports seamless integration of such components, ensuring adaptability as new standards and SE technologies evolve.

Despite its strengths, DUCA must address ongoing challenges related to scalability, interoperability, and dynamic policy orchestration. Large-scale CPS introduce complexities in achieving low-latency policy enforcement across diverse infrastructures. Interoperability is further hindered by varied data formats, protocols, and legacy components. Moreover, SE integration entails trade-offs involving system complexity, energy consumption, and performance overhead.

Future work will focus on developing autonomous, adaptive policy orchestration mechanisms, potentially leveraging machine learning for real-time privacy risk assessment and automated policy tuning. The integration of advanced privacy-preserving AI techniques—such as federated learning, secure multi-party computation, and homomorphic encryption—can further enable compliant analytics without compromising confidentiality. Additionally, DUCA's modular design should continue evolving to accommodate emerging cryptographic primitives and SE standards with minimal system disruption.

In summary, DUCA delivers a comprehensive and adaptable solution for privacy management in CPS. Through its fusion of dynamic policy enforcement, extensive PET integration, and hardware-backed security, it provides scalable, regulation-compliant privacy safeguards. Its demonstrated versatility and extensibility position DUCA as a reference architecture for the next generation of privacy-aware cyber-physical infrastructures.

Acknowledgments. This work has been supported by the EU project DUCA under GA No 101086308 (HORIZON-MSCA-2021-SE-01).

Disclosure of Interests. *Authors have no competing interests.*

References

1. S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Review*, vol. 4, no. 5, pp. 193–220, 1890.
2. A. F. Westin, *Privacy and Freedom.* New York: Atheneum, 1967.
3. A. Tsohou and G. Kokolakis, "Gdpr in practice: Privacy statements and fair processing," *Computer Law & Security Review*, vol. 36, p. 105406, 2020.

4. E. Parliament and Council, "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), article 25: Data protection by design and by default," Official Journal of the European Union, pp. 1–88, 2020.
5. A. Cavoukian, "Privacy by design: The 7 foundational principles," *Information and Privacy Commissioner of Ontario*, 2011.
6. A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the 3rd Conference on Hot Topics in Security*. USENIX Association, 2008, pp. 1–6.
7. E. A. Lee, "Cyber-physical systems: Design challenges," in *Proceedings of the 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*. IEEE, 2008, pp. 363–369.
8. M. Broy, "Cyber-physical systems – innovation durch software-intensive eingebettete systeme," *Informatik-Spektrum*, vol. 35, p. 61–66, 2012.
9. S. V. Khaitan and J. D. McCalley, "Design techniques and applications of cyber-physical systems: A survey," *IEEE Systems Journal*, vol. 9, no. 2, pp. 350–365, 2015.
10. R. Zhong, X. Feng, and Q. Li, "Cyber-physical systems in intelligent manufacturing," *Advanced Robotics*, vol. 31, no. 19-20, pp. 1175–1190, 2017.
11. E. Baloyi and D. Le Guennec, "Privacy in cyber-physical systems: Issues and solutions," *International Journal of Cyber-Physical Systems (IJCS)*, vol. 4, no. 2, pp. 40–58, 2019.
12. J.-H. Hoepman, "Privacy design strategies," in *IFIP International Information Security Conference*. Springer, 2014, pp. 446–459.
13. S. Cha, H. Lee, and H. K. Kang, "Privacy-enhancing technologies: A review," *Journal of Information Processing Systems*, vol. 15, no. 1, pp. 1–16, 2019.
14. M. Mont, K. Harrison, and J. R. Clark, "Privacy management for portable healthcare records," in *Proceedings of the 18th IEEE Symposium on Computer-Based Medical Systems (CBMS)*. IEEE, 2005, pp. 459–464.
15. A. D. Zemskov, Y. Fu, R. Li, X. Wang, V. Karkaria, Y.-K. Tsai, W. Chen, J. Zhang, R. Gao, J. Cao *et al.*, "Security and privacy of digital twins for advanced manufacturing: A survey," *arXiv preprint arXiv:2412.13939*, 2024.
16. M. Volkmann, S. S. Tripathi, S. Kaven, C. Frank, and V. Skwarek, "Privacy in local energy markets: A framework for a self-sovereign identity based p2p-trading authentication system," in *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*. IEEE, 2023, pp. 1–7.
17. S. Vargaftik, R. B. Basat, A. Portnoy, G. Mendelson, Y. B. Itzhak, and M. Mitzenmacher, "Eden: Communication-efficient and robust distributed mean estimation for federated learning," in *International Conference on Machine Learning*. PMLR, 2022, pp. 21 984–22 014.
18. L. Ponchione, "Implementation of policies in data-centric security solutions: A case study," Ph.D. dissertation, Politecnico di Torino, 2023.
19. K. Suzaki, K. Nakajima, T. Oi, and A. Tsukamoto, "Ts-perf: General performance measurement of trusted execution environment and rich execution environment on intel sgx, arm trustzone, and risc-v keystone," *IEEE Access*, vol. 9, pp. 133 520–133 530, 2021.
20. M. Akgün, E. U. Soykan, and G. Soykan, "A privacy-preserving scheme for smart grid using trusted execution environment," *IEEE Access*, vol. 11, pp. 9182–9196, 2023.

21. J. Camenisch, L. Chen, M. Drijvers, A. Lehmann, D. Novick, and R. Urian, "One tpm to bind them all: Fixing tpm 2.0 for provably secure anonymous attestation," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 901–920.
22. E. B. Fernandez and A. Muñoz, "A cluster of patterns for trusted computing," *International Journal of Information Security*, vol. 24, no. 1, p. 72, 2025.
23. N. Weichbrodt, P.-L. Aublin, and R. Kapitza, "sgx-perf: A performance analysis tool for intel sgx enclaves," in *Proceedings of the 19th International Middleware Conference*, 2018, pp. 201–213.
24. Z. M. Rajeh, S. A. Alhomdy, and F. Thabit, "Secure authentication in smart home environment using sgx and biometrics: Survey," in *2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI)*. IEEE, 2024, pp. 1–10.
25. S. A. Atiiq and A. C. Risdianto, "Demystifying amd sev performance penalty for nfv deployment," in *Proceedings of the 2024 13th International Conference on Networks, Communication and Computing*, 2024, pp. 1–8.
26. L. Jäger and R. Petri, "Dice harder: a hardware implementation of the device identifier composition engine," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–8.
27. Trusted Computing Group, "TCG Cyber Resilient Module and Building Block Requirements Version 1.00, Rev. 0.08," Trusted Computing Group, TCG Specifications, October 2020. [Online]. Available: https://trustedcomputinggroup.org/resource/
28. ——, "TCG Reference Integrity Manifests (RIM) Information Model Version 1.00, Rev. 0.16," Trusted Computing Group, TCG Specifications, November 2020. [Online]. Available: https://trustedcomputinggroup.org/resource/tcg-reference-integrity-manifest-rim-information-model/
29. S. Sultan, "Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey," *Computers & Security*, vol. 84, pp. 148–165, 2019.
30. E. Birrell, A. Gjerdrum, R. van Renesse, H. Johansen, D. Johansen, and F. B. Schneider, "Sgx enforcement of use-based privacy," in *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*, 2018, pp. 155–167.
31. S. Zobaed and M. Amini Salehi, "Confidential computing across edge-to-cloud for machine learning: A survey study," *Software: Practice and Experience*, 2025.
32. D. R. Safford and M. Wiseman, "Hardware rooted trust for additive manufacturing," *IEEE Access*, vol. 7, pp. 79 211–79 215, 2019.
33. J. Van Bulck, M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx, "Foreshadow: Extracting the keys to the intel {SGX} kingdom with transient {Out-of-Order} execution," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 991–1008.
34. A. Lutsch, M. El-Hindi, M. Heinrich, D. Ritter, Z. IstvĂĄn, and C. Binnig, "Benchmarking analytical query processing in intel sgxv2," *arXiv preprint arXiv:2403.11874*, 2024.
35. M. Kaplan, H. Raj, V. Scarlata, and K. Vinayagamoorhty, "Enabling realms with the arm confidential compute architecture," *USENIX ;login:*, 2021. [Online]. Available: https://www.usenix.org/publications/loginonline/enabling-realms-arm-confidential-compute-architecture
36. D. Lee, D. Kohlbrenner, S. Shinde, K. Asanović, and D. Song, "Keystone: An open framework for architecting trusted execution environments," in *Proceedings of the Fifteenth European Conference on Computer Systems*, 2020, pp. 1–16.

37. S. Said, J. E. Hajlaoui, and M. N. Omri, "A survey on the optimization of security components placement in internet of things," *Journal of Network and Systems Management*, vol. 32, no. 4, p. 77, 2024.
38. D. Dhinakaran, S. Sankar, D. Selvaraj, and S. E. Raja, "Privacy-preserving data in iot-based cloud systems: A comprehensive survey with ai integration," *arXiv preprint arXiv:2401.00794*, 2024.
39. J. Tanisha, P. A. Rajesh, R. G. Singh, K. Adhip, K. Stuti, and D. Ajitha, "Privacy and data protection challenges in industry 4.0: An ai-driven perspective," 2024.
40. Z. Zhang, T. Yu, X. Ma, Y. Guan, P. Moll, and L. Zhang, "Sovereign: Self-contained smart home with data-centric network and security," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13 808–13 822, 2022.
41. A. Al-Hasnawi, Y. Niu, J. F. Tawfeq, M. R. Pradhan, M. Salahat, and T. M. Ghazal, "Iot security frameworks: A comparative review with a focus on privacy," in *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024, pp. 01–10.
42. L. Campanile, M. Iacono, F. Marulli, M. Mastroianni *et al.*, "Privacy regulations challenges on data-centric and iot systems: A case study for smart vehicles." in *IoTBDS*, 2020, pp. 507–518.
43. I. Gutiérrez-Agüero, S. Anguita, X. Larrucea, A. Gomez-Goiri, and B. Urquizu, "Burnable pseudo-identity: A non-binding anonymous identity method for ethereum," *IEEE Access*, vol. 9, pp. 108 912–108 923, 2021.
44. F. Menges, T. Latzo, M. Vielberth, S. Sobola, H. C. Pöhls, B. Taubmann, J. Köstler, A. Puchta, F. Freiling, H. P. Reiser *et al.*, "Towards gdpr-compliant data processing in modern siem systems," *Computers & Security*, vol. 103, p. 102165, 2021.
45. M. Asante, G. Epiphaniou, C. Maple, H. Al-Khateeb, M. Bottarelli, and K. Z. Ghafoor, "Distributed ledger technologies in supply chain security management: A comprehensive survey," *IEEE Transactions on Engineering Management*, vol. 70, no. 2, pp. 713–739, 2021.
46. J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *Ieee Access*, vol. 7, pp. 164 908–164 940, 2019.
47. N. Bermad, "Pseudonym revocation system for iot-based medical applications," *Available at SSRN 4865840*.
48. S. Dimopoulou, C. Symvoulidis, K. Koutsoukos, A. Kiourtis, A. Mavrogiorgou, and D. Kyriazis, "Mobile anonymization and pseudonymization of structured health data for research," in *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*. IEEE, 2022, pp. 1–6.
49. M. Kangwa, "Prevention of personally identifiable information leakage in ecommerce using offline data minimization and online pseudonymisation." Ph.D. dissertation, The University of Zambia, 2023.
50. B. Khalfoun, S. Ben Mokhtar, S. Bouchenak, and V. Nitu, "Eden: Enforcing location privacy through re-identification risk assessment: A federated learning approach," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, no. 2, pp. 1–25, 2021.
51. J. Salas and J. Domingo-Ferrer, "Some basics on privacy techniques, anonymization and their big data challenges," *Mathematics in Computer Science*, vol. 12, pp. 263–274, 2018.
52. C. Sandeepa, B. Siniarski, N. Kourtellis, S. Wang, and M. Liyanage, "A survey on privacy for b5g/6g: New privacy challenges, and research directions," *Journal of Industrial Information Integration*, vol. 30, p. 100405, 2022.
53. B. Khalfoun, "Privacy preserving location based services: From centralized to federated approaches," Ph.D. dissertation, INSA de Lyon, 2022.

54. T. E. Jost, "Privacy management for cyber-physical systems - a system of systems architecture based on digital twins," 2021.
55. K. Baumer, "Identification and evaluation of concepts for privacy-enhancing big data analytics using de-identification methods on wrist-worn wearable data," Ph.D. dissertation, Technische Universität München, 2020.
56. A. Majeed, "Attribute-centric and synthetic data based privacy preserving methods: A systematic review," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 638–661, 2023.
57. G. Munilla Garrido, K. Schmidt, C. Harth-Kitzerow, J. Klepsch, A. Luckow, and F. Matthes, "Exploring privacy-enhancing technologies in the automotive value chain," *arXiv e-prints*, pp. arXiv–2209, 2022.
58. A. S. Ahmadian, J. Jürjens, and D. Strüber, "Extending model-based privacy analysis for the industrial data space by exploiting privacy level agreements," in *Proceedings of the 33rd annual ACM symposium on applied computing*, 2018, pp. 1142–1149.
59. J. A. Onesimu, J. Karthikeyan, and Y. Sei, "An efficient clustering-based anonymization scheme for privacy-preserving data collection in iot based healthcare services," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1629–1649, 2021.
60. R. Fazal, M. A. Shah, H. A. Khattak, H. T. Rauf, and F. Al-Turjman, "Achieving data privacy for decision support systems in times of massive data sharing," *Cluster Computing*, vol. 25, no. 5, pp. 3037–3049, 2022.
61. M. Akil, L. Islami, S. Fischer-Hübner, L. A. Martucci, and A. Zuccato, "Privacy-preserving identifiers for iot: a systematic literature review," *IEEE Access*, vol. 8, pp. 168 470–168 485, 2020.