International Journal of Information Science and Computing
Citation: *IJISC*: **11**(01): 13-27, June 2024
DOI: 10.30954/2348-7437.1.2024.3

INFORMATION SCIENCE AND TECHNOLOGY FOUNDATION

REVIEW PAPER

Navigating the Concept of Privacy, Consent and Cyber-Physical Systems

A. Sogbesan[1*], U.M. Mbanaso[2], S. Bassey[3] and G. Aimufua[4]

[1]*PhD Candidate: Centre for Cyberspace, Nasarawa State University, Keffi, Nasarawa State, Nigeria*
[2]*Professor of Computing and Cybersecurity, former Executive Director: Centre for Cyberspace, Nasarawa State University, Keffi, Nasarawa State, Nigeria*
[3]*Fellow: Centre for Cyberspace, Nasarawa State University, Keffi, Nasarawa State, Nigeria*
[4]*Professor of Computer Science and Deputy Director: Centre for Cyberspace, Nasarawa State University, Keffi, Nasarawa State, Nigeria*

**Corresponding author: tolasogbesan@ieee.org*

Received: 07 Apr., 2024 **Revised:** 25 May, 2024 **Accepted:** 02 June., 2024

ABSTRACT

Cyber-physical systems (CPS) are characterised by integrating physical and computational components, which use embedded systems and internetwork connectivity. These systems operate in real-time, facilitating interaction and control of physical elements to address problem-solving scenarios. Cyber-physical systems (CPS) operate in digital and physical realms, so their actions, such as those in smart homes or medical devices, can significantly affect individuals' privacy. For instance, they may automatically adjust home settings based on user behaviour or monitor vital signs in real-time. Consequently, CPS can potentially infringe upon an individual's private spaces, such as homes, personal vehicles, or workplaces, through pervasive sensing and actuation, thereby constraining personal autonomy. As they increasingly permeate our daily lives, empowering individuals to manage their data privacy and safeguarding against potential threats becomes paramount. This article introduces a novel Privacy Consent Management Architecture (PCMA) to address these concerns. We discuss the architecture's components, functionality, and benefits, demonstrating its effectiveness in safeguarding privacy and security in CPS. The PCMA is a symmetric system that allows transaction parties to balance the sharing of privacy data and benefits of the transaction to the privacy data owner through a policy-based negotiating framework. The enforcement of privacy data consent enables users to manage their privacy data actively and, importantly, fosters trust, a critical factor in complex CPS environments. The PCMA introduces a dynamic architecture for privacy management, offering the potential to manage and strengthen privacy and security in CPS environments, giving hope for a more secure future.

Keywords: Private data, data privacy, personally identifiable information (PII), cyber-physical systems, General Data Protection Regulation (GDPR), data leaks, user consent, Internet of Things (IoT)

How to cite this article: Sogbesan, A., Mbanaso, U.M., Bassey, S. and Aimufua, G. (2024). Navigating the Concept of Privacy, Consent and Cyber-Physical Systems. *IJISC.,* **11**(01): 13-27.

Source of Support: None; **Conflict of Interest:** None

The convergence of physical and digital realms in Cyber-Physical Systems (CPS) has ushered in a new era of innovation and efficiency. Cyber-physical systems (CPS) seamlessly integrate computational systems, such as software, data, and algorithms, with physical systems, including mechanical, electrical, or biological elements. This integration harnesses embedded technology and internet connectivity to enable real-time operation, where computational algorithms interact with and control physical components to achieve specific objectives. This is often accomplished by leveraging sensors, actuators, and control systems to ensure efficient and reliable performance.

Integrating these systems is crucial in various applications, such as smart grids, autonomous vehicles, and healthcare. By incorporating advanced technologies like artificial intelligence and machine learning, they facilitate improved efficiency and automation[1][2][3][5].

However, this innovative CPS raises privacy, security, safety, and trust (PSST) issues and has posed challenges to ensuring PSST, as these systems are susceptible to cyber threats that can potentially disrupt essential services[2][4]. In some cases, CPS design introduces complexities involving advanced networking and computing abstractions that account for computational and physical dynamics, highlighting the intricacy of continually addressing PSST to support the benefits of this modern technology[4][5].

Thus, ensuring PSST in CPS is a critical requirement that must be continuously addressed due to the dynamic nature of the CPS environments. However, existing solutions focus on static access control and encryption, neglecting explicit user consent and data minimisation.

Establishing a robust and reliable architecture for managing privacy consent has become increasingly crucial in today's digital landscape. The PCMA addresses these limitations, providing CPS with a strong approach to simultaneously solve PSST by leveraging a symmetric and dynamic policy-based PSST negotiating engine to guarantee the appropriate, proportionate and responsible use of privacy data. Through expressed policy content, individuals can take complete control over their personally identifiable information (PII) within the CPS environments.

By enshrining transparency and control, PCMA aims to foster trust and reduce the risks related to data breaches and misuse[6]. This research delves into PCMA's critical role in safeguarding PSST in CPS. It investigates the unique PSST challenges posed by CPS's interconnected nature and explores innovative approaches to resolving them.

The goal is to implement a privacy consent framework that empowers users to enable informed data decisions while ensuring that CPS operators comply with ethical and legal obligations on data protection. Integrating PCMA into CPS can lead to a more safe and privacy-focused digital future.

Implementing the above mentioned principles aims to enrich the user experience by promoting transparency, enabling greater control, and ensuring adherence to privacy regulations. The architecture empowers users to oversee and control their data proactively, essential for navigating complex CPS environments. In this way, PCMA provides CPS users with a way to understand how their data is used, thereby fostering trust and promoting engagement with the system[7]. Thus, by providing an Application Programming Interface (API), PCMA can help CPS product developers create compliant and transparent systems that enhance user confidence[11].

PCMA addresses the asymmetry in privacy management by allowing users to weigh service benefits against data access demands, promoting a more balanced approach to consent management[10]. Furthermore, PCMA addresses personal data privacy protection in an open architecture, ensuring compliance with

GDPR, the California Consumer Privacy Act (CCPA), the Gramm—Leach—Bliley Act (GLBA), and the Personal Information Protection and Electronic Documents Act.

(PIPEDA) regulations and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The dynamic PCMA policy framework obtains users' consent before data processing and sharing[11]. Thus, PCMA can facilitate the secure exchange of sensitive information, reducing privacy risks related to data sharing in CPS transactions[8].

By enabling users to make knowledgeable choices regarding their data and providing mechanisms for transparency and accountability, PCMA ensures explicit user consent, data minimisation, and granular access control, providing robust data privacy for CPS users.

While PCMA significantly improves user experience by enhancing control and compliance, it may also introduce complexity that could overwhelm less tech-savvy users. Balancing usability with robust privacy features remains a challenge in PCMA-CPS integration.

Background and Related Works

The applications of privacy-enhancing technologies (PETs) to improve Cyber-Physical Systems (CPS) security and privacy are vast and promising. CPS is essentially based on IoT and introduces unstructured multiple data points that require critical investigation of PETs that can facilitate PSST safeguards. For instance, Federated Learning (FL) can leverage PETs to secure sensitive data during collaborative training, mitigating privacy threats[12].

Thus, integrating PETs in FL enhances computational and communication performance, making it a viable option for CPS applications. Techniques like secure multi-party computation and homomorphic encryption ensure data confidentiality in distributed environments, which can be crucial for CPS[13]. This is defined as Verifiable Privacy-Preserving Computing. Furthermore, using zero-knowledge proofs can enhance the verifiability of computations, ensuring both privacy and correctness in data handling[13].

From regulatory and developmental perspectives, current advancements in PETs highlight their role in improving data governance and compliance with privacy regulations[14]. Encouraging software developers to integrate PETs into applications can significantly reduce privacy threats in CPS[15].

In contrast, challenges such as increased development costs and the complexity of integrating PETs into modern systems may hinder their widespread adoption in CPS, necessitating further research and innovation in the field[15][16].

The Government Privacy Instructions Corpus, or GPI Corpus, introduces about 1,043 privacy laws, regulations, and guidelines spanning about 182 jurisdictions[18] to enable a comprehensive quantitative and qualitative evaluation of global privacy legal issues. This demonstrates the international significance of privacy laws, with a notable surge in legislation addressing various personal data concerns. For instance, the NIST Privacy Framework and other regional regulatory laws share common goals in protecting individuals' privacy but differ in scope and approach[6][17].

Existing frameworks introduced by various regional and national bodies aim to establish guidelines and principles governing decisions, actions, and other activities related to collecting, processing, and sharing personal information.

The massive intrusion of privacy necessitates treating privacy data, whether directly or indirectly identifiable to an individual, with a focus on safeguarding privacy.

By ensuring the privacy of Personally Identifiable Information (PII), consumers are expected to develop greater trust and confidence, thereby fostering healthier transactions and competition, ultimately leading to increased utilisation of digital systems[10].

When establishing parameters and limitations for the gathering, handling, and utilising PII, a balance can be achieved between legally sharing information and safeguarding privacy rights. This will enable stakeholders to adhere to these regulatory principles, which serve as the foundation for addressing privacy-related data management concerns.

Following a comprehensive review of these privacy directives and principles, it is crucial to place them in the context of this work. Notably, it is essential to emphasise that service providers collecting, utilising, or retaining data for PII transactions must adhere to fundamental privacy standards.

Therefore, the PCMA complements existing privacy frameworks and laws by providing a structured approach to consent management, enhancing operational efficiency, scalability, transparency, and accountability.

Privacy Concerns in CPS

Due to the integration of digital and physical processes, CPS faces significant challenges regarding user privacy and trust. As CPS becomes more prevalent in healthcare, transportation, industry, smart homes, and other areas, the risks associated with data sensitivity, user surveillance and tracking, and potential privacy abuses, misuses, or breaches can escalate.

The complex environment and dynamic operation of CPS introduce numerous privacy challenges:

1. *Communication Network Security:* CPS depends on communication between physical and computational components, implying that cyber adversaries (or malicious parties) could intercept sensitive information if the communication channels are not secured appropriately. Similarly, pervasive data collection from multiple sensors can be continuous on data about users, environments, or physical processes.

   This data may include PII (e.g., location, health data, behaviour patterns) that can lead to privacy breaches. CPS provides an opportunity for increased surveillance in smart environments (e.g., smart homes and cities), implying that CPS can enable continuous monitoring of individuals, leading to concerns about constant surveillance without consent.

2. *Unauthorized Data Access:* Most environments may need more protection mechanisms. Sensitive data collected by CPS (such as medical records in healthcare systems or location data in autonomous vehicles) may not be adequately protected.

   Moreover, unauthorised access to the data can result due to flawed encryption, vulnerability landscapes, or poor security practices. Third-party sharing of data generated by CPS may be shared with third parties, often without users being aware or giving consent. This can happen when companies use the data for analytics, marketing, or other purposes, exposing users to further privacy risks.

3. *Location and Identity Tracking:* CPS can potentially expose users' location, which can inadvertently be used to track them. For example, transportation systems (e.g., smart traffic, smart vehicles, etc.) and personal systems such as wearables can show users' real-time location and identity, thereby raising privacy risks such as unlawful tracking or profiling[24][25].
4. *Inference Attacks:* Attacks such as sensitive inference can be initiated by malicious parties analysing raw data that may seem non-sensitive but aggregating it to infer personal, sensitive information, including health conditions, habits, or practices. Such aggregation may expose a user's behavioural pattern of interactions with the CPS.
5. *Lack of Transparency and Control:* Users are mainly left in the dark about what data CPS collects and stores and for what reasons it is used. This occurs primarily due to the lack of a policy-oriented protection framework; most users may not be aware of the data exposed by CPS. Furthermore, it may be difficult to erase or fully anonymise the data after it is collected, particularly when it is shared with multiple repositories.
6. *Physical Privacy Concerns:* CPS operates in the digital and physical realms. Transactions such as in smart homes or medical devices can impact users' privacy directly. An example is the potential to automatically update home settings based on user behaviour or monitor vital signs in real time. In addition, CPS can intrude into customarily private spaces, resulting in pervasive sensing and actuation, which invades an individual's privacy. This can exacerbate unhindered access to private data without consent recourse to permission[20].

However, the advent of emerging technologies that may accelerate CPS innovations, such as Blockchain Technology, can enhance data integrity and privacy through decentralised data sharing. Proposed blockchain-assisted schemes, which allow deniable authentication[19], introduce privacy concerns.

Similarly, the Energy-Saving and Privacy Data Sharing (ESPPDS) scheme offers a privacy-preserving approach tailored for resource-constrained healthcare devices that claim to ensure efficient data sharing without compromising user privacy[21] and lack real-time users' consent.

Moreover, advancements in technologies that protect privacy, including differential privacy and homomorphic encryption, promise to enhance user trust and safeguard personal data in CPS[20][26], which lacks transparency in users' consent. The PCMA addresses most of these gaps by providing a policy-based symmetrical architecture that allows the negotiation of the release of privacy data and service benefits to users dynamically before data is shared.

Privacy Consent Management Architecture (PCMA)

The PCMA provides an adaptable framework to streamline consent-related processes while complying with data governance regulations. Implementing this universal model can allow organisations to meet specific consent management requirements while maintaining consistency with data governance policies.

The PCMA design addresses issues such as user fatigue, lack of clarity, and complexities in handling detailed consent choices. Its symmetry allows for a seamless protocol for negotiating service benefits against proportionate and appropriate release of privacy data.

The PCMA features a centralised consent management mechanism that stores and manages individuals' privacy preferences and consent decisions in a policy. It allows users to easily access and adjust their

consent policy configurations, giving them significant control over their data. Implementing a symmetric design in the architecture is essential for achieving consistent usability across various domains and scenarios.

This approach facilitates a standardised methodology that can be applied universally, enhancing the user experience and ensuring that consent management processes are efficient and effective. Establishing a symmetric design ensures that the underlying mechanisms for obtaining and managing consent remain consistent, thereby reducing the cognitive load on the architecture. The architecture's set policy governance drives this repeatability. The privacy ecosystem can be simple yet intricate, as shown in Fig. 1, representing typical interaction characterisation. It visually demonstrates the challenges of managing privacy data in multiple transactions.

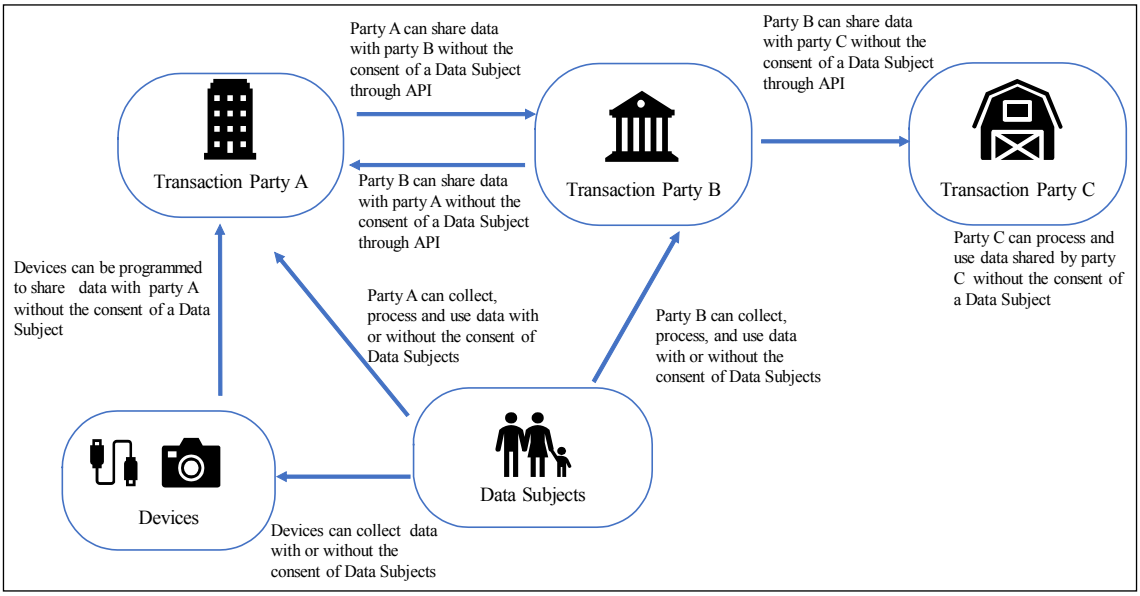

Fig. 1: Privacy ecosystem relationship

Thus, the symmetric presentation makes the architecture adaptable, effectively complies with regulations, fulfils compliance obligations, and establishes trust in a decentralised environment. A thorough auditing mechanism tracks and records all consent-associated actions, such as consent requests, changes, and withdrawals, to ensure accountability and compliance with privacy regulations.

The PCMA also includes a user-friendly interface that simplifies user engagement with the consent management system. It provides precise and concise information about the intentions for which their data will be used, empowering individuals to make informed decisions about their consent.

Organisations can efficiently manage and honour individuals' privacy preferences by deploying a symmetric centralised consent management system, comprehensive auditing mechanisms, and user-friendly interfaces. These systems promote transparency and accountability in handling privacy consent inquiries.

PCMA Components and Workflow

The effectiveness of data transmission from data owners to service providers relies heavily on three critical elements known as the three Ts: transparency, the type of data involved, and the level of Trust established[37]. These components, when integrated, form a pivotal factor, denoted as the transfer of personal data, which holds considerable importance in the quest for customer data that can be leveraged to achieve a competitive edge and success in the market. Managing data user privacy by transferring personally identifiable information (PII) to service providers is as crucial and essential as a transaction requiring data transfers.

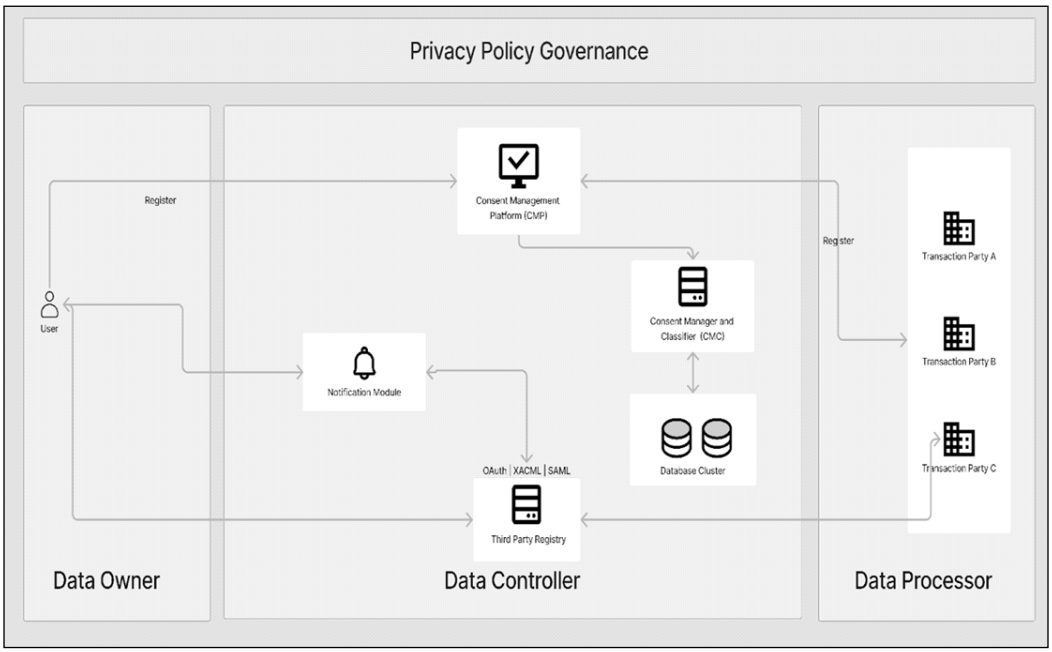

Fig. 2: PCMA Sequence Diagram of Workflow (***Source:*** Author)

Fig. 2 depicts the Architecture and the data flow within its components. Each uses OAuth 2.0, XAMCL, and SAML for symmetric repeatability. The basic architecture and underlying workflow are also shown.

(a) Basic Data Request

Data Owners (DO) and Transaction Parties (TP) - Service Providers register on the PCMA: Within the PCMA context, registering Data Owners and Transaction Parties is essential for establishing a structured environment where data can be effectively managed and utilised. Data Owners provide ample information and their PIIs.

1. Data Owners (DO) and Transaction Parties (TP) - Service Providers register on the PCMA: Within the PCMA context, registering Data Owners and Transaction Parties is essential for establishing a structured environment where data can be effectively managed and utilised. Data Owners provide ample information and their PIIs. On the other hand, transaction parties, which encompass various

service providers, consume the information determined by the data controllers. This involves the data they control, including its nature, usage rights, and relevant compliance requirements. It also demonstrates the capability to handle transactions securely and efficiently, fostering trust among all stakeholders involved in the data exchange process and interacting with any registered TP using OAuth2.0 to get an access token to access the services on the TP. Data Owners engage with any registered Third Party (TP) through the OAuth 2.0 protocol, which facilitates the secure exchange of access tokens. This interaction is crucial as it allows Data Owners to authenticate themselves and authorise the TP to access specific services on their behalf. The OAuth 2.0 framework enhances security by ensuring that sensitive information is not directly shared with the TP—still, an access token grants limited permissions for service access.

2. Mapping data owners to transaction parties involves establishing a secure and reliable connection between entities. XACML provides a standardised language for expressing access control policies, while SAML enables the exchange of authentication and authorisation data between different security domains. By leveraging these technologies, the PCMA ensures that Data Owners can securely share their information with Transaction Parties while maintaining control over who has access to what data.
3. The Data Owner receives an update concerning the status of their data transfer, which is communicated through a notification. This update is designed to provide the DO with insights into the ongoing transfer activities, including any potential delays or issues that may arise. The notification is vital in ensuring transparency and optimising the data transfer process by informing the DO.

(b) Escalated Data Request

1. When a Service Provider (SP) requires additional data, such as the user's PII, it will only be accessible after consent is granted. The first step is for the SP to send a request on the PCMA, which triggers a notification to the User with a prompt to approve or decline the request for additional data. This process ensures that the data owner has the necessary control over the release of their data. By sending the request to PCMA, the system can access the required information and promptly facilitate the transaction completion.
2. If the Data Owner approves, a view-only page of the requested PII is shared with the requesting Transaction Party. Both the screenshot and copy feature are disabled, which prevents any unauthorised storage by Service Providers. The approval has a time limit and will be revoked after 15 minutes. This process ensures that the Third Party has only temporary access to the requested PII while the PCMA helps maintain security and control over the Data Owners' PII.
3. If the Data Owner declines the request, the subsequent action involves forwarding the response to the Transaction Party. This procedural step ensures that the Transaction Party remains informed of the Data Owner's decision, thereby maintaining transparency in the communication process. The implications of such a refusal can be significant, as it may affect the ongoing transactions or agreements between the involved parties.

(c)Data Leak Check

This involves a process of web crawling that systematically navigates through various online resources to detect and extract sensitive information that may have been inadvertently exposed through unauthorised third-party transfers. This technique employs automated bots or spiders that traverse the internet, indexing content from websites, forums, and databases to uncover instances where users' PII may be publicly accessible. The data leak check process is critical in protecting the privacy and security of personally identifiable information belonging to the data owner information. By proactively initiating a request to search for their PII on the Internet, the data owner is committed to ensuring their sensitive information stays safeguarded from unauthorized access. Following the completion of the investigation, the results are promptly relayed to the data owner, allowing them to carefully examine the findings and take any necessary actions to address potential vulnerabilities. The feature is not activated on the PCMA.

(d) The PCMA Components

The identified critical building blocks established in the literature and highlighted in section 4.1 earlier are presented in the Architecture workflow as follows:

1. **Consent Management Platform (CMP):** The CMP is the primary interface for regulating user consent and supervising data transmission. It operates as a hub that interfaces with diverse applications and services to acquire personally identifiable information (PII). Through its integration with these applications, the CMP guarantees the acquisition and observance of user consent across the data-gathering procedure. By establishing connections with multiple applications, the CMP ensures the proper acquisition and adherence to user consent, thereby ensuring conformity with data protection regulations. This centralised approach streamlines the control of user consent and data transmission, thereby augmenting transparency and liability within the procedure in a controlled and transparent manner.
2. **Database Cluster (DC):** A database cluster represents a sophisticated infrastructure facilitating the seamless integration of diverse databases into a unified entity. By allocating tasks across various nodes, a database cluster can manage large data volumes effectively while delivering prompt responses. The interconnected structure of the cluster enables data replication, guaranteeing that all nodes possess an updated database replica. This duplication not only improves data accessibility but also ensures fault tolerance, ensuring that the failure of one node does not result in data loss or system interruptions. In essence, a database cluster serves as a robust solution for organisations seeking advanced data management capabilities and the capacity to expand their operations in alignment with increasing data requirements.
3. **Consent Manager and Classifier (CMC):** Users can provide detailed consent for disclosing personally identifiable information (PII). This denotes their ability to precisely specify which data points are permissible for sharing, identify the third parties with whom the data can be shared, and define the purposes for which the data may be utilised. Moreover, the system classifies PII into various levels of sensitivity, distinguishing between data of lower sensitivity, such as a name and susceptible information like a Social Security Number (US), National Insurance (UK), National Identity Number (Nigeria), etc. Based on the sensitivity level of the data, stricter consent requirements could be essential to guarantee the protection and confidentiality of the

user's information. This approach allows users to safeguard their privacy, assists organisations in adhering to data protection regulations, and fosters trust with users by showing a commitment to protecting their personal information.

4. **Third-Party Registry:** The primary function of this secure registry is to maintain a comprehensive record of approved third parties, guaranteeing the confidentiality and privacy of user data. This registry acts as a trusted source of information, providing insights into the purpose behind data collection activities conducted by these authorised entities. Additionally, it serves as a repository for privacy policies, outlining the measures and practices implemented by these third parties to ensure the protection of user information. Organizations can effectively oversee and manage third-party activities by maintaining this registry, ensuring compliance with privacy regulations and promoting a secure data ecosystem.
5. **Notification Module (NM):** This module ensures that users can stay informed about the progress of their consent and take appropriate actions based on the provided information. Whether the consent is accepted or rejected, the notification service ensures that users are promptly notified, enabling them to stay informed and make informed decisions regarding their consent status. Its configuration includes:

   - **Informative Message**: The user receives a clear and concise notification detailing:
     - The type of PII being transferred (e.g., name and email address).
     - The identity of the third-party recipient.
     - The purpose for data transfer is specified by the application/service.
   - **Consent Options:** The notification provides clear options for users to:
     - **Review Consen**t: Users can access and review the specific consent they provided for the data transfer.
     - **Modify Consent:** Users can modify their consent for future PII transfers to this third party (e.g., revoke or limit).
     - **Object to Transfer:** Users can object to the specific PII transfer.

6. **Audit Trail:** The platform has been designed to maintain a comprehensive log of each occasion when a user grants consent, any transmission of personally identifiable information (PII), and all messages dispatched to users. An audit trail function is essential in fostering users' trust and confidence, given that its scrupulous monitoring mechanism advances openness and accountability in managing user data. By retaining elaborate documentation of user consent activities, PII transfers, and notifications, the system can present a coherent outline of how user data is supervised and protected, ultimately bolstering the overall credibility of the platform.

The PCMA Policy Framework

The PCMA Policy Framework is a crucial element of the architecture. It offers a mechanism for dynamic privacy management through a policy construct. The policy offers flexible and robust symmetrical constructs configurable and grounded in two key concepts: *Capabilities and Requirements*[10]. This policy architecture enables each party to articulate and precisely describe its capabilities – the services

it provides, the requirements involved, and the credentials necessary to access these capabilities, along with any further obligations or constraints. To facilitate the dynamic sharing of personal data among transaction parties, they should outline their access policy rules in the Requirements and Capabilities sections of the policy architecture. Fig. 3 depicts the framing of the policy architecture, illustrating its symmetric attributes.

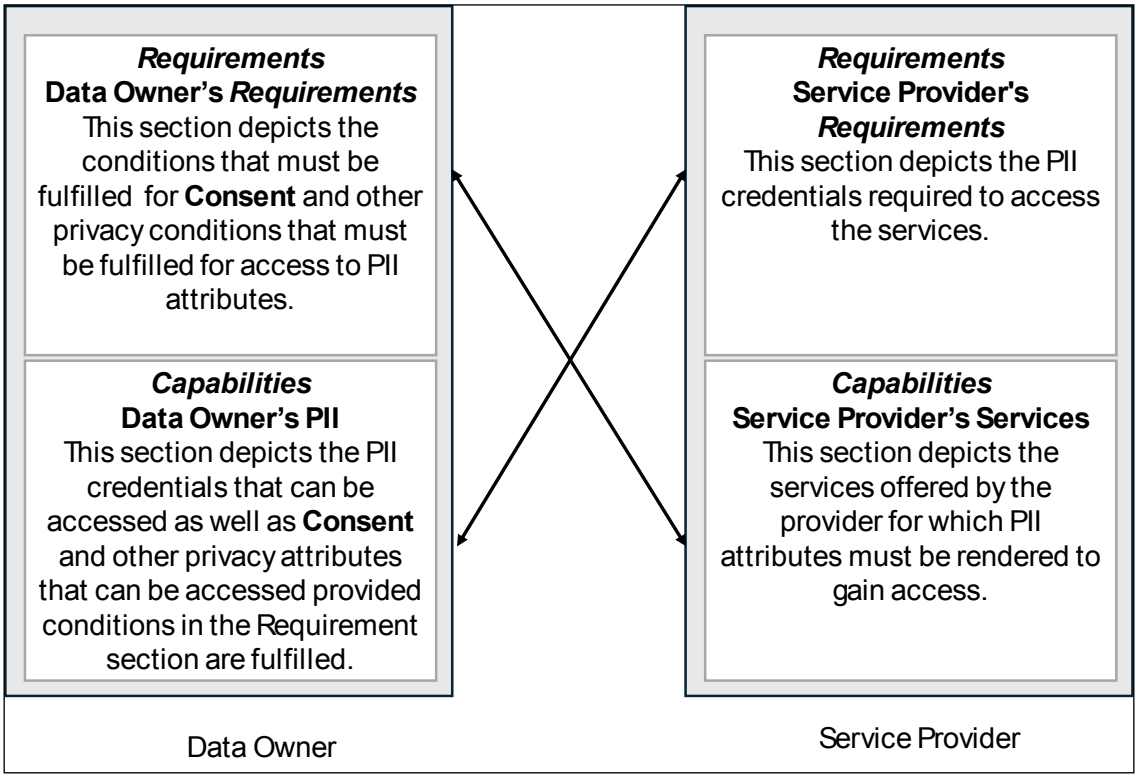

Fig. 3: Privacy Policy Architecture

Advantages and Limitations of PCMA to CPS Users

(a) Advantages

The PCMA's conceptualisation is characterised by various components, such as the Data owners, specifics of personal data, context handler, consent manager, notice service, and data manager. The data owners bestow consent upon a service provider using the dynamic policy construct, specifying crucial elements of lawful consent.

When consent is required for personal data gathering and utilisation, the data owner must be capable of validating the Data controllers' compliance. The policy explicitly expresses a service provider's requirements to address the consent conditions. Through the policy, the Data owner can express restraint to retract their consent at any given time, as stipulated by (GDPR).

Thus, PCMA dynamically offers effective privacy consent management in Cyber-Physical Systems (CPS), primarily enhancing user control, security, and compliance with regulations.

PCMA allows users to manage their data, reducing unauthorised access and misuse of PII. Another paramount advantage of heightened user control is the capacity to determine how data is accessed and used, thus nurturing a feeling of ownership over personal information[27]. On the other hand, transparency in data usage allows users to make informed decisions, which is crucial in highly secure settings where sensitive information is involved[28].

Another incentive is the improved security measures through dynamic policy negotiation and enforcement and automated consent directives, ensuring that data is only shared with authorised parties[27]. The PCMA achieves this by providing timed users' PII on the platform, which cannot be copied or screenshotted. Additionally, regulatory compliance is a vital benefit CPS users can take from adopting PCMA. This is evident in enforcing organisations' compliance with regulations like GDPR, NDPR, etc, which mandate user consent for data processing[29].

LIMITATIONS

Implementing robust privacy consent management in Cyber-Physical Systems (CPS) poses several technical challenges owing to its inherent complexity and dynamic nature. The challenges associated with Cyber-Physical Systems (CPS) can be categorised into several key areas. First, there is the issue of heterogeneity and integration, as CPS often consist of diverse components and technologies. This diversity complicates establishing a unified consent management framework that can accommodate different data types and processing methods[30].

Integrating IoT devices also adds complexity, as each device may have different privacy requirements and capabilities[31]. In the earlier section, compliance with regulation was identified as a critical benefit for PCMA privacy enhancement on CPS; however, research shows that **a**dhering to privacy regulations like GDPR necessitates transparent consent processes, often inadequately supported by existing systems[32].

Furthermore**,** regulatory guidelines' ambiguity complicates the identification of appropriate technical measures for compliance, leading to inconsistent implementations[34]. This ambiguity extends to the Security and Transparency case, where ensuring user consent's integrity and non-deniability is crucial yet challenging due to the potential misuse of data and the need for robust security measures[32]. Thus, CPS's dynamic behaviour requires real-time consent management solutions that adapt to changing contexts and user preferences[31].

CONCLUSION

Privacy consent architecture can be customized to suit any CPS environment and context, effectively meeting users' specific needs. On the technical side, the PCMA is robust and efficient, effectively tackling most privacy issues related to it CPS. Thus, PCMA offers a comprehensive privacy and security solution for CPS, addressing consent, data minimisation, access control, and data protection. Its implementation ensures the safeguarding of sensitive information, fostering trust in CPS.

This research has delved into the intricate relationship between CPS and PCMA, exploring the unique challenges posed by CPS and the potential solutions offered by PCMA. Key findings include:

- **The need for context-specific PCMA:** CPS' unique characteristics require tailored PCMA approaches to address specific vulnerabilities and challenges.
- **The importance of user education:** It is crucial to empower users with knowledge about their privacy rights and the implications of consent decisions.
- **The role of technology:** Advancements in technology enhance trust in the adoption of CPS and address emerging threats.
- **The need for collaboration:** Stakeholders across industries, governments, and academia must collaborate to develop and implement compelling user privacy consent controls in CPS.

In conclusion, navigating the intersection of privacy, consent, and CPS requires a multifaceted approach. By adopting PCMA, organisations can foster trust, empower users, and mitigate data collection and usage risks in the digital age.

As CPS continues to evolve, ongoing research and development in Privacy-Enhancing Technologies, like the PCMA, will ensure that privacy and security remain at the forefront of technological innovation.

REFERENCES

1. Ruben, Eduardo, Montano, Claure., Julie, B., Heynssens., Ian, Burke., Mahafujul, Alam and Bertrand, Cambou. 2024. Enhancing cyber-physical systems (CPS) robustness through sensor-pair health indicators. doi: 10.1117/12.3012525
2. Sindhu, Rajendran., Sri, Ram, Chandra, Murthy, P.., Sreenivasulu, Reddy, Reddy, L., N., Ramavenkateswaran. 2024. Cyber-Physical System: Advances and Applications in Cyber Security. doi: 10.2174/9789815223286124010007
3. Rahul, Umesh, Mhapsekar., Muhammad, Iftikhar, Umrani., Mohd, Faizan., Omer, Ali., Lizy, Abraham. 2024. Building Trust in AI-Driven Decision Making for Cyber-Physical Systems (CPS): A Comprehensive Review. Doi: 10.48550/arxiv.2405.06347
4. Husnara, Khan and Daljeet, Kaur. 2024. Cyber-physical systems. doi: 10.58532/nbennurch188
5. Rudresha, S.J., Gopinath, Harsha, R., Kiran, Kumar, G.R., Shruthi, S., Kalpana. 2024. A cyber-physical systems perspective on smart grids. doi: 10.58532/v3bgai10p1ch4
6. Sogbesan, Abdulfattah Adetola, 2024, Privacy Consent Management Architecture (PCMA) for Personal Identifiable Information. PhD Thesis, Nasarawa State University.
7. Thomas, Ernst, Jost., Christian, Stary., Richard, Heininger. 2023. Towards User-Centered Privacy Adaptation Management: Insights From Privacy Research and a System-of-Systems Architecture. doi: 10.1109/cbi58679.2023.10187468
8. Balambiga, Ayappane., Rohith, Vaidyanathan., Srinath, Srinivasa., Jayati, Deshmukh. 2023. Extensible Consent Management Architectures for Data Trusts. arXiv.org, doi: 10.48550/arxiv.2309.16789
9. Thomas, Jost., Christian, Stary. 2022. A Single Point of Contact for Privacy Management in Cyber-Physical Systems. doi: 10.1007/978-3-031-19704-8_8

10. Uche, Mbannaso., Adetola, Sogbesan. 2022. The conceptualisation of a Configurable Consent Architecture for Personal Data Release. doi: 10.1109/nigercon54645.2022.9803088

11. Neda, Peyrone., Duangdao, Wichadakul. 2022. Formal models for consent-based privacy. Journal of logical and algebraic methods in programming, doi: 10.1016/j.jlamp.2022.100789

12. Jaime, Loureiro-Acuña., Xavier, Martínez-Luaña., Héctor, Padín-Torrente., Gonzalo, Jiménez-Balsa., Carlos, García-Pagán., Ines, Ortega-Fernandez. 2024. Enhancing Privacy in Federated Learning: A Practical Assessment of Combined PETs in a Cross-Silo Setting. doi: 10.1145/3658664.3659661

13. Tariq, Bontekoe., Dimka, Karastoyanova., Fatih, Turkmen. 2023. Verifiable Privacy-Preserving Computing. arXiv.org, doi: 10.48550/arxiv.2309.08248

14. OECD, 2023. "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en.

15. Maisha, Boteju., Thilina, Ranbaduge., Dinusha, Vatsalan., Nalin, Asanka, Gamagedara, Arachchilage. 2023. SoK: Demystifying Privacy Enhancing Technologies Through the Lens of Software Developers. arXiv.org, doi: 10.48550/arxiv.2401.00879

16. Elisa, Bertino., Ravi, Sandhu., Bhavani, Thuraisingham., Indrakshi, Ray., Wei, Li., Maanak, Gupta., Sudip, Mittal. 2022. Security and Privacy for Emerging IoT and CPS Domains. doi: 10.1145/3508398.3519314

17. Seyed, Ramin, Ghorashi., Tanveer, Zia., Michael, Bewong., Yinhao, Jiang. 2023. An Analytical Review of Industrial Privacy Frameworks and Regulations for Organisational Data Sharing. Applied Sciences, doi: 10.3390/app132312727

18. Gupta, S., Poplavska, E., O'Toole, N., Arora, S., Norton, T., Sadeh, N., & Wilson, S. 2022. Creation and analysis of an international corpus of privacy laws. *arXiv preprint arXiv:2206.14169*.

19. Yang, Xu., Ziyu, Peng., Cheng, Zhang., Gaocai, Wang., Huiling, Wang., Hongbo, Jiang., Yaoxue, Zhang. 2024. Enhancing privacy in cyber-physical systems: An efficient blockchain-assisted data-sharing scheme with deniability. *Journal of Systems Architecture,* doi: 10.1016/j.sysarc.2024.103132

20. Manvendra, Sharma. 2024. Enhancing Security and Privacy in Cyber-Physical Systems: Challenges and Solutions. doi: 10.1109/ccwc60891.2024.10427691

21. Yangyang, Bao., Weidong, Qiu., Xiaochun, Cheng. 2022. Privacy-preserving and fine-grained data sharing for resource-constrained healthcare CPS devices. Expert Systems, doi: 10.1111/exsy.13220

22. Anand, K., Bapatla., Saraju, P., Mohanty., Elias, Kougianos. 2023. 4. FortiRx 2.0: Smart Privacy-Preserved Demand Forecasting of Prescription Drugs in Healthcare-CPS. doi: 10.1109/ocit59427.2023.10430944

23. Pradeep, Kumar, Roy., Sunil, Kumar, Singh. 2022. Privacy preserving monitoring protocol for Cyber-Physical System. Computers & Electrical Engineering, doi: 10.1016/j.compeleceng.2022.108232

24. Yinhao, Jiang., Mir, Ali, Rezazadeh, Baee., Leonie, Simpson., Praveen, Gauravaram., Josef, Pieprzyk., Tanveer, A., Zia., Zhen, Zhao., Zung, Le. 2024. Pervasive User Data Collection from Cyberspace: Privacy Concerns and Countermeasures. doi: 10.3390/cryptography8010005

25. Soumya, Samarpita., Rajeeb, Kumar, Mishra., Rabinarayan, Satpathy., Bibudhendu, Pati. 2023. Security Issues and Privacy Challenges of Cyber-Physical System in Smart Healthcare Applications. Transactions on Computer Systems and Networks, doi: 10.1007/978-981-99-4518-4_5

26. Book Chapter 2022. Challenges in the Taxonomy of Cyber-Physical Security and Trust. Cyber-Physical Systems, 1st Edition, doi: 10.1201/9781003220664-5

27. Lelethu, Zazaza., Lelethu, Zazaza., Hein, S., Venter., George, Sibiya. 2018. The current state of electronic consent systems in e-Health for privacy preservation. doi: 10.1007/978-3-030-11407-7_6

28. Lelethu, Zazaza., Lelethu, Zazaza., Hein, S., Venter., George, Sibiya. 2019. A Conceptual Model for Consent Management in South African e-Health Systems for Privacy Preservation. doi: 10.1007/978-3-030-43276-8_6

29. Michael, A., Gailloux., Lauren, Ricardo, Aubyn, St., King. 2020. Private information disclosure consent management system.

30. Muhammad, Irfan, Khalid., Mansoor, Ahmed., Markus, Helfert., Jungsuk, Kim. 2023. Privacy-First Paradigm for Dynamic Consent Management Systems: Empowering Data Subjects through Decentralized Data Controllers and Privacy-Preserving Techniques. Electronics, doi: 10.3390/electronics12244973

31. Thomas, Jost., Christian, Stary. 2022. A Single Point of Contact for Privacy Management in Cyber-Physical Systems. doi: 10.1007/978-3-031-19704-8_8

32. Elisa, Bertino., Ravi, Sandhu., Bhavani, Thuraisingham., Indrakshi, Ray., Wei, Li., Maanak, Gupta., Sudip, Mittal. 2022. Security and Privacy for Emerging IoT and CPS Domains. doi: 10.1145/3508398.3519314

33. Ram, Govind, Singh., Sushmita, Ruj. 2023. Encoding of security properties for transparent consent data processing. doi: 10.1109/GCON58516.2023.10183463

34. Christoph, Hohmann., Tim, Posselt. 2019. Design challenges for CPS-based service systems in industrial production and logistics. *International Journal of Computer Integrated Manufacturing,* doi: 10.1080/0951192X.2018.1552795

35. Klymenko, O., Meisenbacher, S. and Matthes, F. 2023. Identifying practical challenges in the implementation of technical measures for data privacy compliance. arXiv preprint arXiv:2306.15497.

36. Mazurek, G. and Małagocka, K. 2019. What if you ask, and they say yes? Consumers' willingness to disclose personal data is stronger than you think, *Business Horizons,* **62**(6): 751-759.