International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Risk Inference-Based Privacy Preservation Model for Cyber-Physical Systems

[1]Manas Kumar Yogi, [2]Dr. A. S. N. Chakravarthy

Submitted: 03/02/2024 **Revised**: 11/03/2024 **Accepted**: 17/03/2024

Abstract: The Risk Inference-Based Privacy Preservation Model for Cyber-Physical Systems (CPS) addresses the critical need for safeguarding privacy in the evolving landscape of interconnected physical and digital environments. This model, aptly named RIP2 (Risk Inference for Privacy-Preserving CPS), integrates advanced risk assessment techniques with robust privacy-preserving mechanisms to create a dynamic and adaptive framework. The model begins with a comprehensive risk assessment module that identifies potential threats, values privacy-sensitive assets, and assesses vulnerabilities within the CPS architecture. A privacy risk inference engine dynamically analyses contextual data, user behavior, and continuously evolving risk factors to assess the current privacy risk level. Privacy-preserving mechanisms, including differential privacy, encryption, and anonymization, are adaptively applied based on the inferred risk level, ensuring a tailored and effective approach to privacy preservation. Users are empowered to define their privacy preferences, and the model incorporates dynamic privacy policies that automatically adjust based on the risk assessment. Furthermore, the model incorporates incident response and continuous learning mechanisms to respond promptly to privacy incidents and improve the overall resilience of the system. The RIP2 Model aims to strike a balance between the seamless functionality of CPS and the paramount importance of preserving individual privacy in an interconnected and data-driven world.

Keywords*-Risk, Privacy, Sensitivity, Cyber-Physical system*

1. Introduction

Privacy preservation in a Cyber-Physical System (CPS) is motivated by various factors, all of which revolve around the need to protect individuals and entities from potential privacy violations and associated risks [1]. Here are some key motivations:

Sensitivity of Personal Data:

In a CPS, personal data is often collected and processed to enable various functionalities. This data could include information about individuals' behavior, preferences, and activities. Privacy preservation is motivated by the recognition that this sensitive personal data should be handled with care to prevent unauthorized access or misuse [2].

Legal and Regulatory Compliance:

Many regions and industries have strict data protection laws and regulations that mandate the protection of individuals' privacy [3]. Adhering to these legal requirements is not only a legal obligation but also a motivation for organizations and developers to implement robust privacy preservation mechanisms in CPS to avoid legal consequences.

User Trust and Acceptance:

Users are more likely to trust and engage with CPS systems if they are confident that their privacy is being respected. Maintaining user trust is crucial for the successful adoption and operation of CPS applications. A lack of privacy preservation measures can lead to user concerns and reluctance to participate.

Prevention of Identity Theft and Fraud:

CPS often involves the collection and processing of personal information, making it a potential target for malicious actors seeking to engage in identity theft or fraudulent activities [4].

Minimization of Discrimination and Profiling:

The use of personal data in CPS systems can inadvertently lead to discriminatory practices or profiling. Privacy preservation aims to prevent the unfair treatment of individuals based on their personal characteristics, ensuring that the system does not contribute to bias or discrimination [5].

Individual Autonomy and Control:

Privacy preservation recognizes the importance of individual autonomy and control over one's personal information. By implementing mechanisms that allow users to define and control their privacy preferences, CPS systems empower individuals to make informed decisions about the extent to which their data is shared and used.

[1]*Assistant Professor, CSE Department, Pragati Engineering College (A), Surampalem*
[2]*Professor, CSE Department, JNTUK, Kakinada, A.P., India*
Corresponding Author name: Manas Kumar Yogi
Corresponding Author Email: manas.yogi@gmail.com

Mitigation of Social Stigma:

Certain applications of CPS, such as healthcare monitoring or behavior tracking, may carry a risk of social stigma if not handled with sensitivity. Privacy preservation helps mitigate potential negative social consequences by ensuring that individuals' personal information is not disclosed without their consent [6].

Corporate and Organizational Reputations:

Organizations that prioritize and effectively implement privacy preservation measures enhance their reputations. Public awareness and concern about privacy have increased, and organizations that demonstrate a commitment to protecting privacy are likely to be viewed more favourably by the public and stakeholders.

2. Related Work

From past few years due to the awareness of users involved in a smart ecosystem, privacy concerns are being addressed with the help of various adaptive models for personalized privacy. Below Table 1 shows an overview of risk-based privacy models in Cyber-Physical Systems (CPS), including their main themes of working, benefits, and limitations:

Table 1. Popular Privacy models in CPS and their Benefits, Limitations

Reference No.	Privacy Model	Main Theme of Working	Benefits	Limitations
Proposed Model	RIP2 Model	Integrates risk assessment with adaptive privacy-preserving mechanisms.	- Dynamic risk assessment - Adaptive privacy measures - User-defined preferences	- Complexity in implementation
				- Continuous monitoring overhead
7	PPTAP Model	Privacy preservation through dynamic sensitivity and adaptive policies.	- Homomorphic encryption - User-defined privacy levels	- Complexity in parameter tuning
			- Learning from incidents	- Potential computational overhead
8	DSAP Model	Leverages dynamic sensitivity for adaptive privacy in data analysis.	- Dynamic sensitivity estimation	- Challenge in parameter tuning
			- Privacy amplification	- Balancing privacy-utility trade-off
			- Learning from user behavior	
9	Adaptive DP Framework	Utilizes adaptive differential privacy for dynamic privacy protection.	- Continuous adjustment of privacy parameters	- Determining optimal adaptability parameters
			- Sensitivity adaptation	- Potential utility loss
10	Context-Aware Privacy Mechanism	Adapts privacy measures based on contextual analysis and user behavior.	- Contextual awareness	- Dependence on accurate context analysis
			- User behavior modeling	- Potential user resistance
			- Customizable privacy settings	
11	Dynamic Privacy Policies (DPP)	Implements dynamic policies for real-time adaptation to privacy risks.	- Real-time policy adjustments	- Potential complexity in policy management
			- User privacy preferences	- Resource consumption
			- Incident response planning	

These models showcase different approaches to address privacy concerns in CPS, each with its unique working theme, benefits, and limitations. The choice of a particular model depends on the specific requirements, context, and trade-offs preferred in a given CPS environment.

3. RIP2 Model

A Risk Inference-Based Privacy Preservation Model for Cyber-Physical Systems (CPS) involves combining risk assessment techniques with privacy-preserving mechanisms. This model is called the “RIP2 Model" (Risk Inference for Privacy-Preserving CPS).

Components of the RIP2 Model:

1. Risk Assessment Module:

- Threat Modeling: Identify potential privacy threats and risks in the CPS environment. This includes understanding possible attack vectors, vulnerabilities, and the potential impact of privacy breaches [12].

- Asset Valuation: Assign values to the privacy-sensitive assets within the CPS. This could include personal data, system configurations, or any information that, if compromised, could lead to privacy violations.

- Vulnerability Assessment: Evaluate the vulnerabilities in the CPS architecture that could be exploited to compromise privacy. This involves assessing the security measures in place and identifying potential weak points.

2. Privacy Risk Inference Engine:

- Contextual Analysis: Analyse the context in which data is generated, transmitted, and processed within the CPS. Consider factors such as the sensitivity of the data, user preferences, and regulatory requirements.

- Dynamic Risk Assessment: Implement a dynamic risk assessment mechanism that continuously monitors the CPS environment for changes in risk factors. This ensures that the privacy preservation model can adapt to evolving threats and vulnerabilities [13].

- User Behavior Modeling: Incorporate models that predict user behavior and preferences, allowing the system to anticipate privacy concerns and adjust privacy measures accordingly.

3. Privacy-Preserving Mechanisms:

- Differential Privacy: Integrate differential privacy techniques to protect individual privacy while allowing for meaningful data analysis. This includes adding controlled noise to data or query results to prevent the identification of specific individuals.

- Anonymization Techniques: Apply advanced anonymization techniques to protect the identities of users and entities within the CPS. This could involve data anonymization, such as replacing personally identifiable information with pseudonyms.

4. Adaptive Privacy Policies:

- User-Defined Privacy Preferences: This approach advocates that the users can define their privacy choices depending on their comfort levels and the context of their interactions with the CPS. This empowers individuals to have control over the extent to which their data is shared or used.

- Dynamic Privacy Policies: Develop a system that can dynamically adjust privacy policies based on the risk inference engine's assessments. For example, if the risk level increases, the system could automatically enhance privacy measures.

Workflow:

1. Continuous Risk Monitoring:

- The RIP2 Model continuously monitors the CPS environment for changes in risk factors, including new threats, vulnerabilities, and changes in user behavior.

2. Dynamic Risk Assessment:

- The risk inference engine dynamically assesses the privacy risk level based on contextual analysis, user behavior modeling, and the current state of the CPS.

3. Adaptive Privacy Measures:

- Privacy-preserving mechanisms, like encryption, and anonymization, are adaptively applied based on the inferred privacy risk. Stronger measures are activated when the risk level is higher.

4. User Interaction and Preferences:

- Users interact with the CPS while having the ability to define their privacy preferences. These preferences are taken into account when applying privacy-preserving mechanisms.

5. Incident Response and Learning:

- In the event of a privacy incident, the incident response plan is activated. The continuous learning mechanism analyses the incident to improve the risk inference model and enhance privacy measures for future interactions.

The RIP2 Model aims to create a holistic approach to privacy preservation in CPS by integrating dynamic risk assessment, privacy-preserving mechanisms, user preferences, and continuous learning from incidents.

Creating a complete mathematical model for a "Risk Inference-Based Privacy Preservation Model for Cyber-Physical Systems (CPS)" involves formalizing the key components such as risk assessment, inference, and privacy-preserving mechanisms. Below is a simplified representation:

Let:

- R be the set of risk factors in the CPS environment.

- A be the set of privacy-sensitive assets.

- V be the vulnerability matrix indicating the vulnerabilities of the CPS.

- D be the data set collected by the CPS.

- P be the set of privacy-preserving mechanisms.

The Risk Inference-Based Privacy Preservation Model (RIP2 Model) can be mathematically represented as:

1. Risk Assessment:

- The risk assessment function Risk Assessment maps the current state of the CPS to a risk level:

RiskLevel=RiskAssessment(R,A,V) (1)

2. Privacy Risk Inference:

- The privacy risk inference function PrivacyInference dynamically assesses the privacy risk based on contextual analysis, user behavior, and risk factors:

PrivacyRisk=PrivacyInference(D,RiskLevel) (2)

3. Privacy-Preserving Mechanisms:

- The privacy-preserving mechanisms are applied based on the inferred privacy risk and the set of selected mechanisms:

PrivacyPreservation=ApplyPrivacyMechanisms(D,PrivacyRisk,P) (3)

4. User-Defined Privacy Preferences:

- Users can define their privacy preferences, influencing the privacy-preserving mechanisms applied:

UserPrivacyPreferences=GetUserPrivacyPreferences() (4)

5. Dynamic Privacy Policies:

- Dynamic privacy policies adjust based on the risk inference and user-defined preferences: DynamicPrivacyPolicies=AdjustPrivacyPolicies(RiskLevel,UserPrivacyPreferences) (5)

The overall mathematical representation of the RIP2 Model is a combination of these components:

CPSModel(D,R,A,V,P)=ApplyPrivacyMechanisms(D,PrivacyInference(D,RiskAssessment(R,A,V)),AdjustPrivacyPolicies(RiskAssessment(R,A,V),GetUserPrivacyPreferences())) (6)

The above formulation in Equation 6 provides a high-level mathematical representation of the RIP2 Model, incorporating risk assessment, privacy risk inference, user-defined preferences, and dynamic privacy policies. Depending on the specific algorithms and mechanisms used in each function, the model can be further refined and expanded.

4. Experimental Results

For implementing the RIP2 model, python 3.4 language is used in Anaconda3, Jupyter Notebook. The dataset used to carry out the implementation of the proposed model is obtained from the Behavioral Risk Factor Surveillance System (BRFSS) [21]. This dataset helped in creating a framework which identified trends, determinants of health conditions among group of persons residing in a locality under surveillance. The dataset includes 126,464 rows, 25 columns with attributes like year, location, age, topic, category, question etc.

1. Privacy Risk Assessment over Time:

In below, figure 1 shows how the privacy risk changes over time based on the proposed model. This eventually helps in illustrating the effectiveness of the approach in mitigating risks. It can be observed that the proposed method has the lowest privacy risk over long duration of time. This reduction in the degree of privacy risk implies the effectiveness of the RIP2 approach.

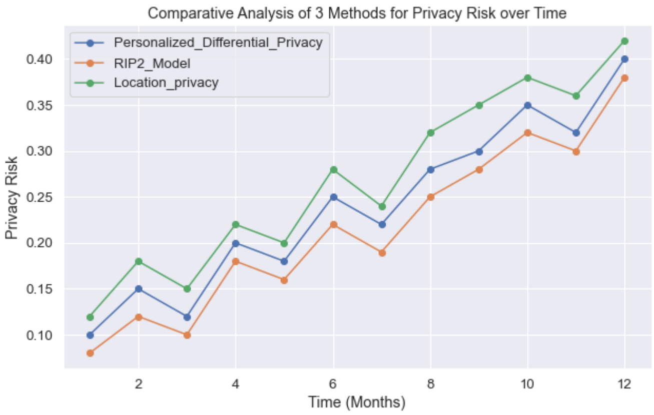

Fig 1.Comparative analysis of popular methods

2. Comparison of Privacy Preservation Models:

In figure 2, the bar charts compare the proposed model's performance with existing privacy preservation models. This includes metrics like accuracy, precision, recall, and F1 score. The RIP2 model performs at a greater level with respect to aspect of all the performance metrics.

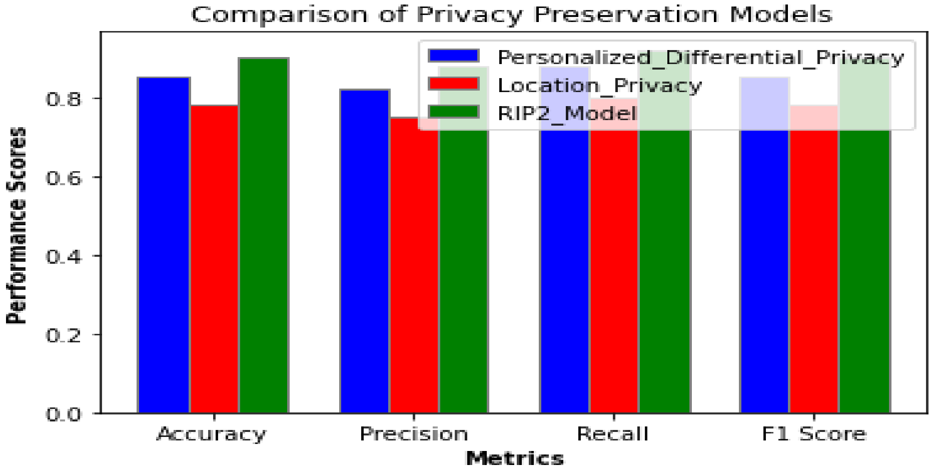

Fig 2.Comparision of Privacy preservation models

3. Sensitivity Analysis:

In below, figure 3 the series of bar charts demonstrates how sensitive the model is to different privacy parameters which are considered critical to privacy preservation in a CPS ecosystem. This could help in understanding which factors have the most significant impact on privacy preservation.

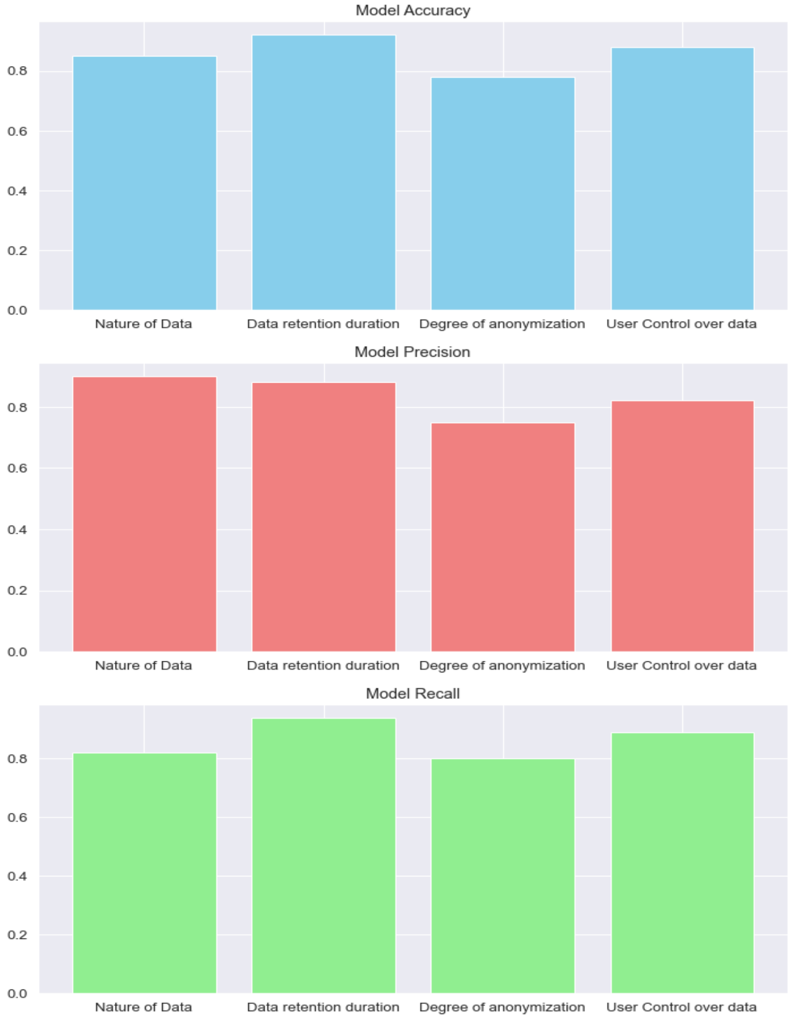

Fig 3.Model Accuracy, Model Precision, Model Recall for various CPS parameters

4. Privacy Risk Heatmaps:

Figure 4 shows the heatmap for the risk of privacy across various CPS components. It has to be noted that each of the components which are involved in playing a role in CPS environment may or may not contain sensitive user data. Hence the privacy risk is not uniform in all the components. It has to be observed that the privacy risk in user interface is the highest and then in sensors. In storage and control systems the privacy risk is low to moderate due to the fact that they are hardware and other peripheral devices which are difficult to manipulate and are less vulnerable in the whole CPS environment.

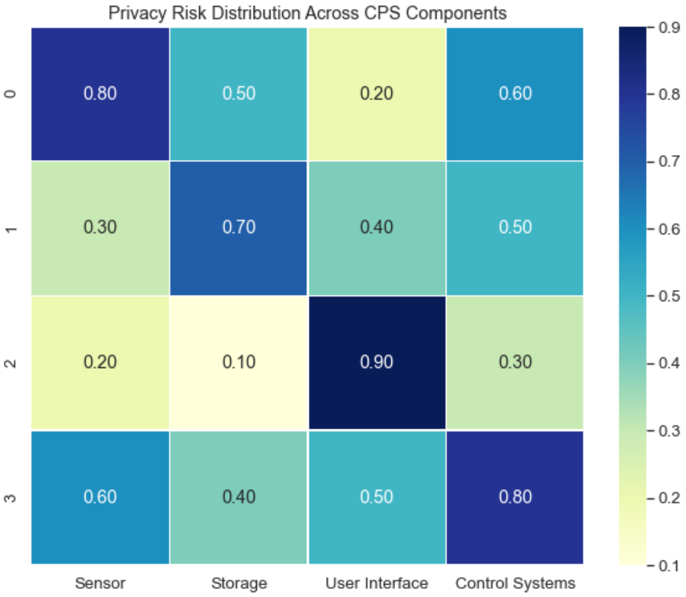

Fig 4. Heatmap for Privacy risk distribution across CPS components

5. Future Directions

The future directions for the development and enhancement of Risk Inference-Based Privacy Preservation Models for Cyber-Physical Systems (CPS) involve addressing emerging challenges, leveraging evolving technologies, and advancing the sophistication of privacy preservation strategies. Several key directions pave the way for the continuous improvement and effectiveness of these models [15]:

1. Amalgamation of cutting edge technologies like Artificial Intelligence (AI) and Machine Learning (ML):

Future models can benefit from integrating AI and ML algorithms to enhance the accuracy of risk inference and dynamic adaptation mechanisms. Advanced analytics and predictive modeling can better anticipate evolving privacy risks, leading to more proactive and precise privacy preservation.

2. Federated Learning in Decentralized CPS Architectures:

As CPS architectures evolve toward decentralization, incorporating federated learning techniques can be instrumental. With the help of federated learning, models can be trained across decentralized devices without sharing raw data, improving the model's adaptability while preserving privacy at the edge [16].

3. Quantum-Safe Cryptography:

With the advent of quantum computing, the security landscape is expected to undergo significant changes. Future privacy preservation models for CPS should explore quantum-safe cryptography to ensure long-term security against potential threats posed by quantum computers [17].

4. User-Centric Privacy Dashboards:

Enhancing the transparency of privacy preservation models is crucial. Future models can incorporate user-centric privacy dashboards, providing individuals with instantaneous understanding of how their data is being utilized, the current privacy risk level, and the impact of privacy-preserving measures.

5. Blockchain for Transparent and Immutable Privacy Records:

Integrating Blockchain technology can contribute to creating transparent and immutable records of privacy-related activities [18]. This can enhance accountability, traceability, and auditability in privacy preservation efforts within CPS, fostering trust among users and stakeholders.

6. Privacy-Preserving Edge Computing:

As edge computing becomes more prevalent in CPS, future models should focus on privacy-preserving techniques at the edge. This involves processing and analyzing data locally on edge devices while preserving individual privacy, reducing the need for transmitting sensitive data to centralized servers.

7. Standardization and Regulatory Compliance:

Collaborative efforts should be made to establish industry standards and regulatory frameworks for privacy preservation in CPS. Future directions should involve active participation in standardization processes, ensuring that privacy models align with legal and ethical guidelines [19].

8. Human-Centric Design and Usability:

Prioritizing human-centric design principles and usability in privacy preservation models is essential for user acceptance. Future models should focus on enhancing the user experience, making privacy preferences more intuitive, and ensuring that individuals can easily comprehend and control their privacy settings.

9. Continuous Learning and Adaptation:

Building on the concept of continuous learning, future models should implement more sophisticated learning mechanisms. These mechanisms can involve not only learning from privacy incidents but also incorporating insights from behavioural psychology to better predict and respond to user preferences.

10. Cross-Domain Collaboration:

The future of privacy preservation in CPS requires cross-domain collaboration. Collaborative efforts between academia, industry, policymakers, and users can foster a multidisciplinary approach, ensuring that the models are robust, ethical, and aligned with societal expectations [20].

In navigating these future directions, the goal is to create resilient, user-centric, and adaptive Risk Inference-Based Privacy Preservation Models that not only mitigate risks but also contribute to a trustworthy and responsible CPS ecosystem.

6. Conclusion

The development and implementation of a Risk Inference-Based Privacy Preservation Model for Cyber-Physical Systems (CPS) mark a significant stride toward reconciling the intricate balance between seamless functionality and the paramount importance of safeguarding individual privacy in today's interconnected world. The RIP2 Model, with its dynamic integration of risk assessment, privacy inference, and adaptive privacy-preserving mechanisms, represents a robust model for facing privacy changes in cyber-physical systems.The model's core strength lies in its ability to dynamically adapt to the ever-changing landscape of risks within the CPS. By incorporating advanced risk assessment techniques, the RIP2 Model not only identifies potential threats and vulnerabilities but also continually evaluates and infers privacy risks based on contextual analysis and user behavior. This adaptability allows the model to respond promptly to emerging threats, providing a robust defense against potential privacy breaches. Furthermore, the RIP2 Model introduces a user-centric approach to privacy preservation. Empowering users to define their privacy preferences fosters a sense of control and trust in CPS interactions. The model accommodates these preferences, allowing individuals to tailor their privacy levels based on their comfort and contextual requirements. This user-centricity not only enhances individual autonomy but also contributes to the overall acceptance and adoption of CPS applications. The incorporation of dynamic privacy policies ensures that the model remains resilient in the face of evolving risks and user expectations. The ability to adjust privacy measures in real-time based on risk assessments and user-defined preferences positions the RIP2 Model as a forward-looking solution that anticipates and adapts to the changing dynamics of privacy in CPS. However, it is essential to acknowledge the challenges inherent in implementing such a sophisticated model. The complexity of continuous risk monitoring, parameter tuning, and potential resource overhead must be carefully managed. Striking the right balance between privacy and utility, especially in scenarios with stringent computational requirements, remains an on-going challenge. In essence, the Risk Inference-Based Privacy Preservation Model for Cyber-Physical Systems embodies a holistic and adaptive paradigm that not only mitigates privacy risks but also lays the groundwork for a more secure, trustworthy, and user-centric CPS ecosystem. As privacy concerns continue to evolve, the RIP2 Model stands as a testament to the commitment to preserving individual privacy in the age of interconnected and data-driven technologies.

References

[1] Davis, John S., and Osonde Osoba. "Improving privacy preservation policy in the modern information age." Health and Technology 9 (2019): 65-75.

[2] Wang, Shengling, et al. "Privacy preservation in location-based services." IEEE Communications Magazine 56.3 (2018): 134-140.

[3] Ara, Anees. "Privacy preservation in cloud based cyber physical systems." Journal of Computational and Theoretical Nanoscience 16.10 (2019): 4320-4327.

[4] Pan, Miao, et al. Big data privacy preservation for cyber-physical systems. Springer International Publishing, 2019.

[5] Chong, Michelle S., Henrik Sandberg, and André MH Teixeira. "A tutorial introduction to security

and privacy for cyber-physical systems." 2019 18th European Control Conference (ECC). IEEE, 2019.

[6] Keshk, Marwa, et al. "Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems." IEEE Access 9 (2021): 55077-55097.

[7] Liang, Xueping, et al. "A reliable data provenance and privacy preservation architecture for business-driven cyber-physical systems using blockchain." International Journal of Information Security and Privacy (IJISP) 12.4 (2018): 68-81.

[8] Feng, Jun, et al. "Privacy-preserving computation in cyber-physical-social systems: A survey of the state-of-the-art and perspectives." Information Sciences 527 (2020): 341-355.

[9] Sharma, Tanusree, John C. Bambenek, and Masooda Bashir. "Preserving privacy in cyber-physical-social systems: An anonymity and access control approach." ISSN 1613-0073 (2020).

[10] Sangogboye, Fisayo Caleb, et al. "A framework for privacy-preserving data publishing with enhanced utility for cyber-physical systems." ACM Transactions on Sensor Networks (TOSN) 14.3-4 (2018): 1-22.

[11] Hassan, Muneeb Ul, Mubashir Husain Rehmani, and Jinjun Chen. "Differential privacy techniques for cyber physical systems: a survey." IEEE Communications Surveys & Tutorials 22.1 (2019): 746-789.

[12] Fink, Glenn A., et al. "Security and privacy in cyber-physical systems." Cyber-physical systems. Academic Press, 2017. 129-141.

[13] Zhao, Yaliang, et al. "Privacy-preserving clustering for big data in cyber-physical-social systems: Survey and perspectives." Information Sciences 515 (2020): 132-155.

[14] Gifty, R., R. Bharathi, and P. Krishnakumar. "Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection." Neural Computing and Applications 31.Suppl 1 (2019): 23-34.

[15] Basak, Santanu, Kakali Chatterjee, and Ashish Singh. "DPPT: A differential privacy preservation technique for cyber–physical system." Computers and Electrical Engineering 109 (2023): 108661.

[16] Bhattacharjee, Arpan. Integrity and privacy protection for cyber-physical systems (cps). Diss. University of Nevada, Reno, 2021.

[17] 17.Usha, L. Josephine, and J. Jesu Vedha Nayahi. "Security and Privacy in Big Data Cyber-Physical Systems." Cybersecurity and Privacy in Cyber Physical Systems. CRC Press, 2019. 217-249.

[18] Bhattacharjee, Arpan, et al. "Vulnerability characterization and privacy quantification for cyber-physical systems." 2021 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics). IEEE, 2021.

[19] Lu, Yang, and Minghui Zhu. "A control-theoretic perspective on cyber-physical privacy: Where data privacy meets dynamic systems." Annual Reviews in Control 47 (2019): 423-440.

[20] Kaushik, Keshav. "Exposing Security and Privacy Issues on Cyber-Physical Systems." Cyber-Physical Systems: Foundations and Techniques (2022): 273-288.

[21] https://data.world/cdc/behavioral-risk-factor-hrqol