Research Paper

Privacy elasticity: building resilient data protection for cyber physical systems

Manas Kumar Yogi[1*], Dr. A. S. N. Chakravarthy[2]
[1*]Research Scholar, Department of Computer Science and Engineering, JNTUK Kakinada, A. P., India.
[2]Professor, Department of Computer Science and Engineering, JNTUK Kakinada, A.P., India.

Article Info

Article History:
Received: 29 January 2025
Revised: 07 April 2025
Accepted: 14 April 2025
Published: 30 June 2025

Keywords:
Cyber-Physical
Privacy
Attack
Access
Security

ABSTRACT

In an increasingly interconnected world, cyber-physical systems play a pivotal role in our daily lives, spanning industries from healthcare to transportation and smart cities.With the growing use of smart devices, the privacy concerns are also increasing manifold.This research work depicts novel viewpoints on recommendations for privacy aspects within the eco-systems of cyber-physical systems, aiming to address these critical challenges. The developing nature of privacy design puts impact on non-static authorization, facilitating fine-grained access control depending on real-time situations. End-to-end security ensures data protection throughout its lifecycle, while robust enrolment and authentication APIs enhance identity verification. Distributed authorization and decentralized authentication mechanisms offer a diversified security approach, reducing the reliance on centralized systems. Interoperable privacy profiles establish consistency and compatibility in multi-system interactions, promoting a high level of privacy assurance. Abstraction of a secure environment protects the underlying physical parts, working as a defense against possible security threats. Such innovative solutions are crucial to maintain the confidentiality of sensitive data and ensure the security of cyber-physical systems. With the rapid development of technology, these privacy design guidelines should be realized and adopted in practice so as to protect both people and organizations, and to maximize the potential of cyber-physical systems and minimize the risk associated with them. This investigation highlights that privacy design is a dynamic and moving target in the rapidly changing technology landscape.

Corresponding Author:
Manas Kumar Yogi
Research Scholar, Department of Computer Science and Engineering, JNTUK Kakinada, A. P., India.
Email: manas.yogi@gmail.com

1. INTRODUCTION

In the age of digital transformation, where the physical and digital worlds converge, cyber-physical systems (CPS) have become integral to our daily lives. Such systems comprising sensors, actuators, connectivity, and computational capabilities are critical to diverse applications ranging from healthcare, smart cities, and manufacturing, to transportation [1]. With the continued development of CPS, maintaining privacy for all parties in CPS (including users) is becoming increasingly important. We address in this paper the importance of secure data for the CPS environment and for the importance of preserving privacy of sensitive data and personal information in a data driven inter connected world.

Siginifacnt security and privacy technologies for modern Cyber-Physical Systems (CPS) in healthcare [2], [3]. Post-quantum cryptography employs lattice-based and homomorphic encryption to protect against quantum attacks, with platforms like Microsoft Azure enabling encrypted data analysis without decryption.

Zero-Trust Architecture uses continuous authentication and behavioral analysis to reduce unauthorized access by 60%, as demonstrated by Google's BeyondCorp system. Federated Learning enables decentralized model training while maintaining data locality, with platforms like Owkin achieving 95% precision in cancer detection while ensuring GDPR compliance through differential privacy. Secure Hardware Enclaves like Intel SGX create isolated computing environments, reducing attack vectors by 70% for real-time medical data processing.

Blockchain technology through Hyperledger Fabric provides tamper-proof audit trails for HIPAA compliance. Edge-based anonymization applies k-anonymity and differential privacy at collection points to prevent re-identification.

Adaptive privacy policies enable emergency access through context-aware systems like EPIC, balancing privacy with urgent medical needs. Cyber-physical systems are defined by the tight connection between physical processes and computing systems. They provide an opportunity for real-time data acquisition, processing, and control, which translates into efficient automation and alos making informed decisions.Due to the heterogeneous nature of data in the CPS ecosystem, privacy of sensitive data is difficult to be maintained.The sensors collect huge amount of private data and therefor the possibility of leakage of data is also proportional to the amount of data collected. Ensuring privacy preservation for each of these entities is essential [4].

1. Personal Data Protection: Users' personal data, such as health information, location data, and lifestyle choices, are often collected and processed within CPS. Ensuring their privacy is critical to protect against identity theft and misuse of personal information.
2. People gain autonomy through privacy because they preserve control over their data. The right of control over data collection as well as data sharing and usage must belong to users.
3. Trust levels among users protect privacy which leads to their acceptance of CPS technologies because they feel secure using them.

Importance for Stakeholders [5]

1. These organizations consist of both device manufacturers together with service providers who bear the responsibility for data collection as well as management. Privacy protection stands as an absolute necessity because it keeps the trust of customers while fulfilling data protection regulations.
2. The enforcement of privacy principles depends on regulatory bodies acting under their official authority. These entities must supervise CPS providers so they follow legal guidelines as well as protect both user privacy and their information.

3. The job of Cybersecurity experts as security professionals involves protecting CPS infrastructure against potential attacks. Privacy assurance stands as an essential concern in cybersecurity because system breaches result in both data breaches and system vulnerabilities.
4. CPS protection of privacy extends beyond personal users and reaches across society at every level. The consequences of privacy violations spread beyond personal losses because they impact settled communities as well as infrastructure systems and public trust networks.

Privacy Preservation Strategies

Several methods should be used to solve privacy issues and protect the privacy of CPS ecosystem stakeholders and users [6], [7].

1. The system collects only essential data needed for functions so as to limit exposure of sensitive material.
2. The system must employ advanced encryption techniques which will protect data moving through the network along with protecting stored data from unauthorized access.
3. When possible researchers and data scientists must anonymize their data records through Anonymization and Pseudonymization techniques to keep individual identities protected yet allow data analysis to proceed.
4. You should establish detailed protocols for access authorization alongside secure authentication procedures to limit the access rights of unauthorized personnel who want to view sensitive files.
5. Privacy by Design: Incorporate privacy considerations into the design and development of CPS from the outset, rather than as an afterthought.
6. Organizations should perform Privacy Impact Assessments to detect privacy-related challenges in CPS developments along with methods to handle these issues.

Benefits of Privacy Preservation

The protection of privacy throughout the CPS environment yields several advantageous consequences [7].

1. The protection of user privacy stimulates higher adoption rates from users for CPS technologies.
2. Privacy protection in data allows organizations to fulfill their legal requirements thus protecting them from non-compliance penalties and punitive actions.
3. Data breaches become less likely when robust privacy measures are established thus businesses avoid substantial financial costs together with damage to their reputation.
4. The practice of privacy preservation reflects both ethical principles that protect individual rights to data privacy and security.
5. Organizations committed to privacy foster innovation across the CPS domain through trust and service and technology development.

2. RELATED WORK

In below table, Table 1 summarizes privacy-aware design aspects for a cyber-physical system (CPS), along with their benefits and limitations [8], [9].

These design aspects are essential for ensuring privacy in a cyber-physical system. The benefits they offer include enhanced security, user trust, compliance with regulations, and ethical considerations.

Table 1. Taxanomy of Privacy Aware Design Aspects

Sr. No.	Privacy-Aware Design Aspects	Benefits	Limitations
1	Data Minimization	Data collection is limited to sensitive information which decreases both data breach risks	The CPS becomes less functional and less useful when data accessibility is restricted because it

		and improper entry points.	reduces available analytics capacities.
2	Encryption	The encryption system defends data while it moves between systems and while data remains stored on servers thus maintaining privacy.	Packing data with encryption causes systems to operate at reduced speed.The management of encryption keys along with certificates proves to be a complicated process.
3	Access Control	Makes sure that only valid users or devices can access private data and perform specific actions, safeguarding against unauthorized access.	Access control policy management and managing the user/device permissions can be difficult and may lead to administrative challenges.
4	Anonymization/Pseudonymization	Data analysis and utility capabilities exist within an information security system that protects user identities along with sensitive information.	Performing complete anonymization on data can harm its functionality for particular applications without easy methods to find the right balance between privacy and useful data.
5	Privacy by Design	The initial system design integrates privacy elements to establish privacy as an essential operational element.	The establishment of this design requires supplemental resources and expert knowledge for both phases. Implementing privacy solutions to existing systems proves to be more difficult than integrating them during new system development.
6	Privacy Impact Assessments	CPS projects benefit from this method which identifies privacy risks along with related solutions for strengthened protection of personal information.	The operationalization of assessments demands extensive time commitments from a potentially technical staff.
7	Consent Mechanisms	The approach allows users to gain insight into data collection practices which results in better trust as well as enhanced transparency.	Managing user consent together with obtaining their agreement requires complicated operational procedures that might decrease user interface quality.
8	Privacy Policies and Education	The system explicitly shows its data protection measures and communicates user rights as well as stakeholder responsibilities through informational material.	Users face difficulties understanding lengthy and complex policies because of their complexity. Organizations might need to dedicate additional resources when ensuring user compliance and running educational programs.

Role of Privacy-Preserving Design Aspects for Cyber-Physical Systems (CPS) in Medical IoT

Medical IoT Cyber-Physical Systems require sophisticated privacy mechanisms to protect sensitive health data while maintaining real-time operational capabilities. Seven key approaches address these challenges [10], [11], [12].

Post-Quantum Cryptography: replaces vulnerable AES encryption with lattice-based and homomorphic systems, enabling encrypted data analysis without decryption through platforms like Microsoft Azure Confidential Computing.
Zero-Trust Architecture: employs continuous authentication and behavioral analysis to combat insider threats, with Google's BeyondCorp reducing unauthorized access by 60%.
Federated Learning: allows decentralized model training while keeping data local, with Owkin achieving 95% cancer detection accuracy through differential privacy protection.
Secure Hardware Enclaves: like Intel SGX create isolated computing environments, reducing attack vectors by 70% for real-time ECG analysis.
Blockchain Technology: via Hyperledger Fabric ensures tamper-proof audit trails for HIPAA compliance through smart contracts.
Edge-Based Anonymization: applies k-anonymity and differential privacy at collection points to prevent subject re-identification.
Adaptive Privacy Policies: enable emergency access through context-aware systems, balancing privacy with critical medical needs.

3. METHODOLOGY

3.1. Dynamic Authorization

A dynamic authorization system for cyber-physical systems requires ten structured components to execute context-aware access control policies [13], [14].

The Policy Engine serves as the core evaluation system, conducting real-time policy assessments and making flexible adjustments based on current operational conditions. Context Awareness components continuously collect environmental data, user interactions, and device status through secure transmission protocols. A centralized Policy Repository stores all access control policies organized by resource types, user roles, locations, and attributes. Real-time Evaluation performs continuous checks between access requests, applicable policies, and current situational context, triggering re-evaluation when conditions change. Machine Learning and AI algorithms support unbiased decision-making, enable dynamic policy adjustments, and monitor emerging privacy threats. Comprehensive Logging and Auditing maintains detailed records of access requests, evaluations, and authorization decisions for regular performance verification [15].

User and Device Authentication integrates multi-factor authentication mechanisms to ensure legitimate access requests. Response Mechanisms handle both approval and denial processes, including alarm activation and user notifications. Fine-Grained Control enables administrators to define specific resource and action permissions based on current scenarios [16]. Finally, Redundancy and Fail-Safe Measures prevent unauthorized access during system outages or security failures, ensuring continuous protection of critical cyber-physical system resources. In Table 2, the various design principles with ther inherent merits are represented along with an example and degree of privacy achieved [17], [18], [19].

Table 2. Privacy Design Aspects with their Merits

Aspect	Merit	Suitable Example	Degree of Privacy
Policy Engine	Supports flexible, real-time decisions for access control based on dynamic conditions.	An e-healthcare system dynamically changing the access to patient records during emergencies.	High
Context Awareness	Improves decision accuracy by considering real-time environmental data.	A smart home not allowing door access when suspicious activity is detected.	Medium
Policy Repository	Centralized management of policies for consistency and	A cloud-based repository saving role-based access	High

	easy updates.	policies for a corporate network.	
Real-time Evaluation	Makes sure that access decisions adapt to changing conditions in real time.	Revoking permissions to access the secure facility when an employee badge is reported lost.	High
Machine Learning & AI	Enhances threat prediction and adaptive policy adjustments.	Detecting abnormal access patterns and blocking potential intrusions.	Medium
Logging and Auditing	Provides accountability and helps detect security breaches.	Recording all access attempts to a financial database for compliance audits.	High
User/Device Authentication	Prevents unauthorized access through strong identity verification.	Biometric + OTP authentication for accessing a military control system.	High
Response Mechanisms	Ensures appropriate actions (e.g., alerts) when access is granted/denied.	Locking down a server room and alerting security upon unauthorized entry.	High
Fine-Grained Control	Allows precise access restrictions (e.g., time-bound or action-specific).	A factory worker only accessing machinery relevant to their current shift.	High
Redundancy & Fail-Safe	Prevents unauthorized access during system failures.	Backup authentication servers taking over if the primary system fails.	High

Privacy Considerations

High Privacy: Ensures strict access control, minimal exposure of sensitive data (e.g., authentication logs, policy enforcement) [20].

Medium Privacy: Involves some data collection (e.g., behavioral patterns) but with safeguards.

Low Privacy: Rare in this system, as most components are designed to enhance security and privacy.

The proposed design ensures secure, adaptive, and privacy-preserving access control in cyber-physical systems.

3.2. End to End Security

Providing end to end security for cyber physical systems requires maintaining protection throughout the system including sensor devices and actuators plus entire central control and management components [21].

3.3. Enrolment and Authentication APIs

API enrollment and authentication in cyber-physical systems involves defining access permissions for edge devices and users. The process includes secure registration with user credentials and device identifiers, implementing multi-factor authentication (MFA) for users and certificate/key verification for devices [22]. Token management reduces re-authentication through periodic refresh cycles. Complete activity logging ensures security and regulatory compliance. The system supports complex password policies, SSO integration with external providers like OAuth, regular security assessments, and comprehensive documentation for best practices guidance [23].

3.4. Distributed Authorization

Distributed authorization in cyber-physical systems enhances cybersecurity by distributing decision-making authority across system components to reduce unauthorized access risks. The framework utilizes Role-Based Access Control (RBAC) to establish distinct permission levels for users, devices, and components based on their functions [24]. Individual devices maintain autonomous policy control through central servers or blockchain ledgers, enabling local verification of access requests and real-time authorization decisions without central authority dependence. The system incorporates backup mechanisms for critical security functions, secure encrypted connections between components, and authentication systems to prevent cyber attacks while maintaining compliance with industry standards and legal requirements for CPS authorization functions [25].

3.5. Interoperable Privacy Profiles

Privacy profiles across various components and systems inside a cyber-physical system must have an interoperable mechanism designed for them to establish standardized and consistent privacy practices [26]. This mechanism presents a standardized framework to manage privacy-related items according to Figure 1.

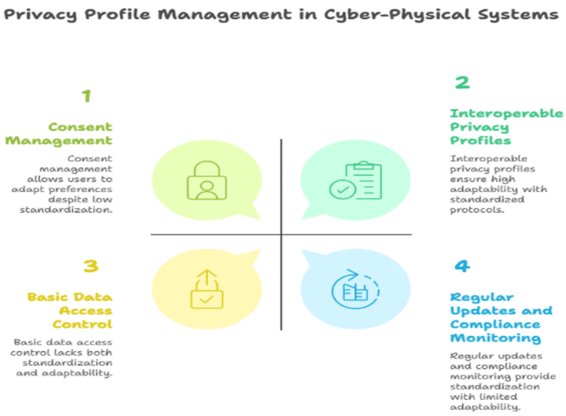

Figure 1. Privacy Profile Management in CPS

Interoperable privacy profiles in cyber-physical systems provide standardized privacy protection through role-specific settings and automated configuration during device onboarding. The framework includes profile repositories, granular consent management, mandatory encryption protocols, and access control policies [27]. It incorporates compliance monitoring, regulatory versioning, third-party integration, and privacy-by-design principles, ensuring comprehensive user-centric protection while maintaining system interoperability [28].

4. RESULTS AND DISCUSSION

The dataset is designed to simulate the impact of privacy profiles on various aspects of cyber-physical systems (CPS), covering privacy adoption, and enforcement, compliance, and security incidents. Table 3 shows the key attributes used in the dataset which can be applied for the proposed privacy design principles.

Table 3. Dataset Attributes

Attribute Name	Functionality	Values
Component_ID	Unique identifier for CPS components	Alphanumeric ID (e.g., CPS001, USR045)
Component_Type	Specifies the type of CPS component	User, Device, Sensor, Actuator, Third-Party Service
Privacy_Profile_Applied	Indicates if a privacy profile is applied	1 = Yes, 0 = No

Privacy_Profile_Adoption_Rate (%)	Percentage of system components with applied privacy profiles	0% – 100%
Data_Sharing_Volume (MB)	Volume of data shared before and after privacy profile enforcement	0 – 1000 MB (or more, depending on system size)
Consent_Type	Specifies the user consent preference	Full,Partial, None
Unauthorized_Access_Attempts	Number of unauthorized access attempts detected	Integer (e.g., 5, 20, 45)
Privacy_Enforcement_Rate (%)	Effectiveness of privacy profile enforcement over time	0% – 100%
Encryption_Type	Encryption or anonymization method used	AES, Homomorphic, Differential Privacy
Privacy_Score (0-100)	Privacy protection effectiveness score	0 – 100
Compatibility_Score (%)	Compatibility level of privacy policies across CPS components	Fully Compatible, Partially Compatible, Incompatible
Privacy_Profile_Updates	Number of privacy profile updates over time	Integer (e.g., 2, 5, 10)
Time_Period (Weeks/Months)	Time intervals used for tracking trends	Days, Weeks, Months, Years
Privacy_Violations	Number of privacy violations detected per time period	Integer (e.g., 10, 25, 50)
Third_Party_Integration	Integration level with third-party privacy standards	Fully Integrated, Partially Integrated, Not Integrated
Security_Incidents	Number of security incidents before and after privacy-by-design	Integer (e.g., 5, 18, 45)

The below results demonstrate the impact and effectiveness of interoperable privacy profiles in a cyber-physical system (CPS).

1. Privacy Profile Adoption Across System Components

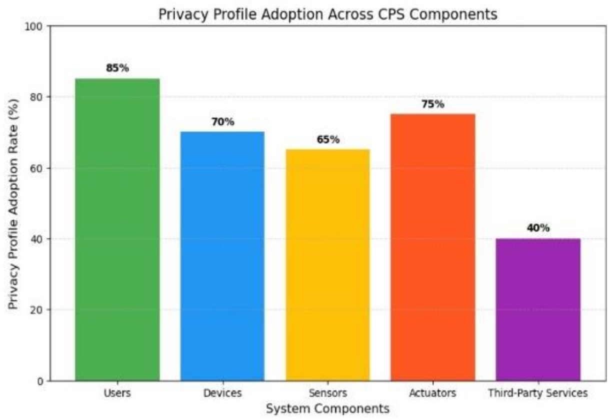

Figure 2. Privacy Profile Adoption Across CPS Components

The bar chart in Figure 2 illustrates the privacy profile adoption rates across various CPS components. The graph reveals that users have the highest adoption rate at 85%, indicating strong privacy enforcement. Devices, Sensors, and Actuators show moderate adoption rates (70%, 65%, and 75%, respectively), highlighting reasonable privacy compliance. Third-Party Services have the lowest adoption rate at 40%, potentially indicating a privacy vulnerability or lack of enforcement in external integrations.

2. Impact of Privacy Profiles on Data Sharing Reduction

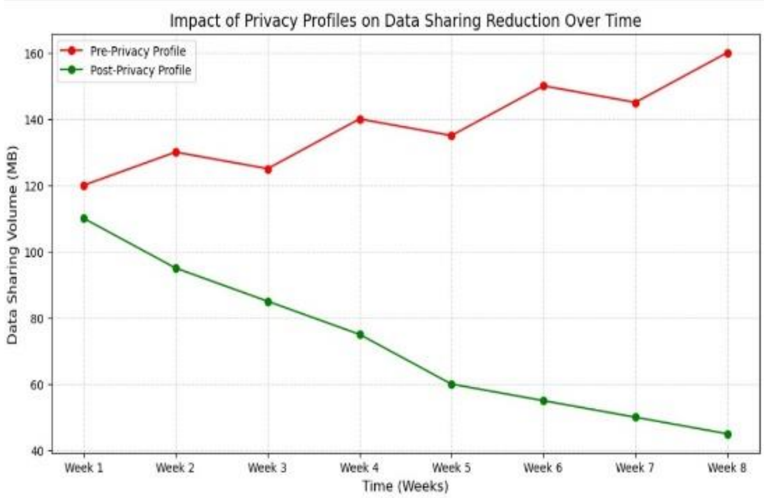

Figure 3. Impact of Privacy Profiles on Data Sharing Over Time

The line chart in Figure 3 shows that pre-privacy profile implementation, data sharing volume increased to 160 MB by Week 8, indicating excessive exchange. Post-implementation, it significantly dropped to 45 MB, reflecting improved privacy enforcement, data minimization, and consistent protection.

3. Consent Preference Distribution

The pie chart in Figure 4 illustrates the distribution of user privacy preferences through consent management. The chart shows 45% of users prefer partial consent, indicating a desire for granular privacy control. 35% grant full consent, suggesting trust or low privacy awareness, while 20% deny consent, reflecting privacy concerns. This highlights the need for flexible privacy settings [29].

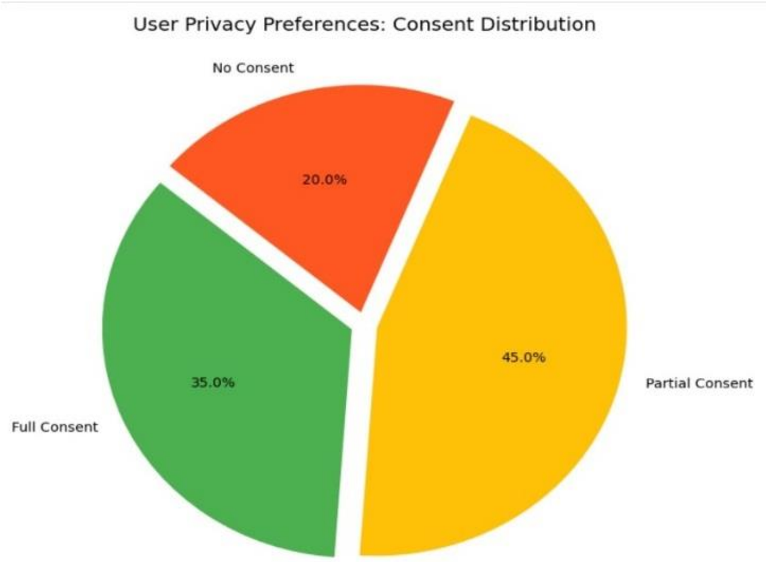

Figure 4. User Privacy Preferences

4. Privacy Profile Enforcement vs. Unauthorized Access Attempts

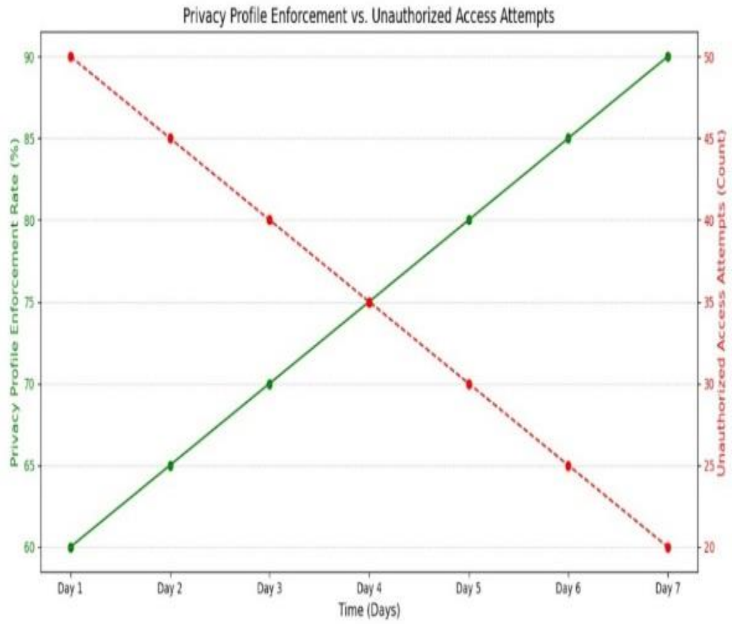

Figure 5. Relation between Privacy Profile Enforcement and Unauthorized Access

The line chart in Figure 5 shows that as privacy profile enforcement increases from 60% to 90%, unauthorized access attempts drop from 50 to 20, demonstrating that stronger privacy measures reduce breaches, enhancing overall system security and access control effectiveness.

5. Privacy Profile Versioning and Update Frequency

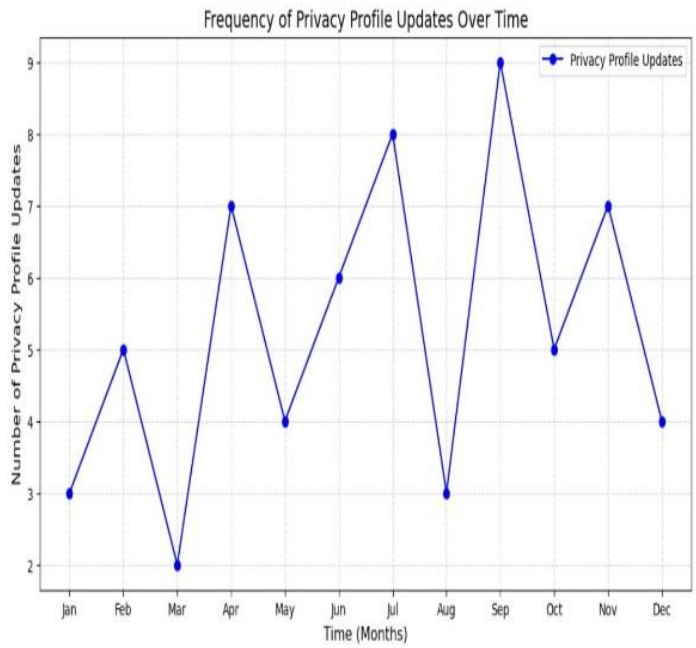

Figure 6. Frequency of Privacy Profile Updates over Time

The line chart in Figure 6 shows frequent privacy profile updates in July (8) and September (9), reflecting proactive compliance. Low updates in March (2) and August (3) suggest gaps, risking out-dated privacy settings and potential vulnerabilities.

6. Compliance Monitoring: Privacy Violations over Time

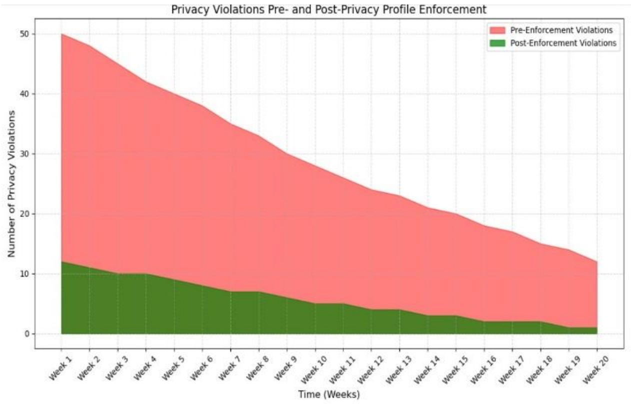

Figure 7. Privacy Violations Profile Enforcements

The area chart in Figure 7 shows that pre-enforcement, privacy violations gradually drop from 50 to 12 by Week 20. Post-enforcement, incidents significantly decrease to 1, highlighting enhanced compliance, stronger privacy controls, and improved system security.

7. Privacy by Design Impact on Security Incidents

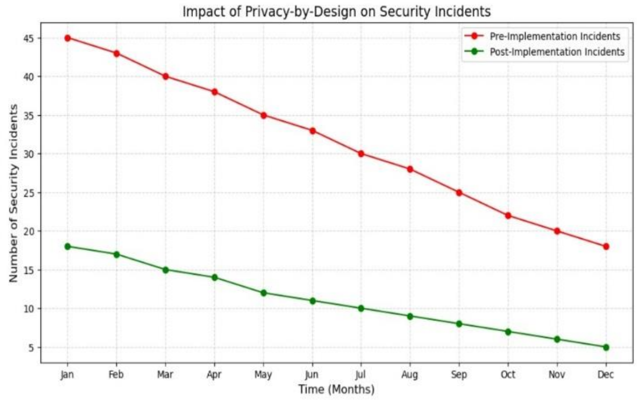

Figure 8. Impact of Privacy by Design on Security Incidents

The line chart in Figure 8 shows that pre-implementation, security incidents drop slowly from 45 to 18. Post-implementation, incidents significantly decline from 18 to 5, highlighting enhanced privacy controls, stronger compliance, and improved protection against security threats [30].

Future Directions

Privacy design research in cyber-physical systems faces six critical challenges [31], [32]. Contextual Privacy Preservation requires developing adaptive recommendations that protect sensitive information in dynamic, context-aware environments. Decentralized Systems demand consistent privacy enforcement across distributed components with effective policy management.

IoT and Sensor Privacy addresses protection of vast data streams from numerous connected devices while preserving user privacy. Interoperability and Standardization focuses on creating harmonized privacy practices that work seamlessly across diverse platforms and devices.

Regulatory Compliance ensures adherence to privacy regulations like GDPR and CCPA while maintaining system functionality. Scalability and Real-time Processing explores maintaining privacy protection as systems expand and handle high-speed data flows. Addressing these challenges is essential for developing effective privacy design recommendations that protect user data, ensure regulatory compliance, and accommodate the unique characteristics of cyber-physical systems' complex, evolving nature.

5. CONCLUSION

This study explores privacy design recommendations for cyber-physical systems, which integrate digital and physical worlds. Traditional security approaches are insufficient for these dynamic systems that require real-time protection of sensitive data and operational integrity.Key recommendations include: dynamic authorization for real-time access control that adapts to changing contexts; end-to-end security protecting data throughout its lifecycle; robust enrollment and authentication APIs for identity verification; distributed authorization to reduce central authority vulnerabilities; decentralized authentication using blockchain technology; interoperable privacy profiles for seamless system integration; and secure environment abstraction to shield physical components.These novel perspectives address the evolving threat landscape and emphasize continuous adaptation and innovation. They provide a foundational framework for building resilient cyber-physical ecosystems that safeguard data, users, and critical infrastructure, serving as a roadmap for secure digital-physical integration as technology advances.

Acknowledgments

We sincerely thank the Department of Computer Science & Engineering for providing the resources and guidance to conduct this research. Our gratitude extends to faculty members, and institutional support for their invaluable feedback.

Funding Information

Authors state no funding involved.

Author Contributions Statement

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Manas Kumar Yogi	✓	✓	✓	✓	✓	✓		✓	✓	✓				
Dr. A. S. N. Chakravarthy		✓				✓			✓	✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

Conflict of Interest Statement

Authors state no conflict of interest.

Informed Consent

We have obtained informed consent from all individuals included in this study.

Ethical Approval

The research related to human use has been complied with all the relevant national regulations and institutional policies in accordance with the tenets of the Helsinki Declaration and has been approved by the authors' institutional review board or equivalent committee.

Data Availability

The data that support the findings of this study are available on request from the corresponding author, Manas Kumar Yogi. The data, which contain information that could compromise the privacy of research participants, are not publicly available due to certain restrictions. Derived data supporting the findings of this study are available from the corresponding author Manas Kumar Yogi on request.

REFERENCES

[1] Song, H., et al. Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications. John Wiley & Sons, 2017. doi.org/10.1002/9781119226079

[2] Darwish, A., and A. E. Hassanien. 'Cyber Physical Systems Design, Methodology, and Integration: The Current Status and Future Outlook'. J. Ambient Intell. Humaniz. Comput, vol. 9, 2018, pp. 1541-1556. doi.org/10.1007/s12652-017-0575-4

[3] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: a survey," IEEE Commun. Surv. Tutorials, vol. 22, no. 1, pp. 746-789, 2019. doi.org/10.1109/COMST.2019.2944748

[4] Seshia, S. A. 'Design Automation of Cyber-Physical Systems: Challenges, Advances, and Opportunities'. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst, vol. 36, no. 9, 2016, pp. 1421-1434. doi.org/10.1109/TCAD.2016.2633961

[5] F. Li et al., "Privacy-aware secure anonymous communication protocol in CPSS cloud computing," IEEE Access, vol. 8, pp. 62660-62669, 2020. doi.org/10.1109/ACCESS.2020.2982961

[6] Habibzadeh, H. 'A Survey on Cybersecurity, Data Privacy, and Policy Issues in Cyber-Physical System Deployments in Smart Cities'. Sustain. Cities Soc, vol. 50, 2019. doi.org/10.1016/j.scs.2019.101660

[7] Yogi, M. K., et al. 'Investigation of Holistic Approaches for Privacy Aware Design of Cyber-Physical Systems'. Cyber-Physical Systems: Foundations and Techniques, 2022, pp. 257-271. doi.org/10.1002/9781119836636.ch11

[8] Seshia, S. A. 'Design Automation of Cyber-Physical Systems: Challenges, Advances, and Opportunities'. IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst, vol. 36, no. 9, 2016, pp. 1421-1434. doi.org/10.1109/TCAD.2016.2633961

[9] Ma, L. 'Security and Privacy for Smart Cyber-Physical Systems'. Secur. Commun. Netw, vol. 2019, 2019. doi.org/10.1155/2019/7045862

[10] M. S. Chong, H. Sandberg, and A. M. H. Teixeira, "A tutorial introduction to security and privacy for cyber-physical systems," in Proc. 2019 18th Eur. Control Conf. (ECC), 2019. doi.org/10.23919/ECC.2019.8795652

[11] Nazarenko, A. A., and G. A. Safdar. 'Survey on Security and Privacy Issues in Cyber Physical Systems'. AIMS Electron. Electr. Eng, vol. 3, no. 2, 2019, pp. 111-143. doi.org/10.3934/ElectrEng.2019.2.111

[12] Lu, Y., and M. Zhu. 'A Control-Theoretic Perspective on Cyber-Physical Privacy: Where Data Privacy Meets Dynamic Systems'. Annu. Rev. Control, vol. 47, 2019, pp. 423-440. doi.org/10.1016/j.arcontrol.2019.04.010

[13] J.-P. A. Yaacoub et al., "Cyber-physical systems security: Limitations, issues and future trends," Microprocess. Microsyst., vol. 77, p. 103201, 2020. doi.org/10.1016/j.micpro.2020.103201

[14] Gupta, R. 'Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges'. IEEE Access, vol. 8, 2020, pp. 24746-24772. doi.org/10.1109/ACCESS.2020.2970576

[15] G. P. Pinto et al., "A systematic review on privacy-aware IoT personal data stores," Sensors, vol. 24, no. 7, p. 2197, 2024. doi.org/10.3390/s24072197

[16] Coiduras-Sanagustín, A., et al. 'Understanding Perspectives on Personal Data Privacy in Internet of Things (IoT): A Systematic Literature Review (SLR)'. Heliyon, 2024. doi.org/10.2139/ssrn.4631186

[17] Harinath, D. 'Enhanced Data Security and Privacy in IoT Devices Using Blockchain Technology and Quantum Cryptography'. J. Syst. Eng. Electron, vol. 34, no. 6, 2024.

[18] Alqahtani, A. S. 'Homomorphic Encryption Algorithm Providing Security and Privacy for IoT with Optical Fiber Communication'. Opt. Quantum Electron, vol. 56, no. 3, 2024. doi.org/10.1007/s11082-023-06098-5

[19] Makina, H., et al. 'Survey on Security and Privacy in Internet of Things-Based eHealth Applications: Challenges, Architectures, and Future Directions'. Secur. Privacy, vol. 7, no. 2, 2024. doi.org/10.1002/spy2.346
[20] C. Zhonghua, S. B. Goyal, and A. S. Rajawat, "Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing," J. Supercomput., vol. 80, no. 2, pp. 1396-1425, 2024. doi.org/10.1007/s11227-023-05517-4
[21] Sun, P. 'A Survey of IoT Privacy Security: Architecture, Technology, Challenges, and Trends'. IEEE Internet Things J, 2024. doi.org/10.1109/JIOT.2024.3372518
[22] Dhinakaran, D. Privacy-Preserving Data in IoT-Based Cloud Systems: A Comprehensive Survey with AI Integration. 2024.
[23] Marengo, A. 'Navigating the Nexus of AI and IoT: A Comprehensive Review of Data Analytics and Privacy Paradigms'. Internet Things, 2024. doi.org/10.1016/j.iot.2024.101318
[24] Wang, R. 'RPIFL: Reliable and Privacy-Preserving Federated Learning for the Internet of Things'. J. Netw. Comput. Appl, vol. 221, 2024. doi.org/10.1016/j.jnca.2023.103768
[25] Aouedi, O. 'A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions'. IEEE Commun. Surv. Tutorials, 2024. doi.org/10.1109/COMST.2024.3430368
[26] M. Adam et al., "A survey on security, privacy, trust, and architectural challenges in IoT systems," IEEE Access, 2024. doi.org/10.1109/ACCESS.2024.3382709
[27] Magara, T., and Y. Zhou. 'Internet of Things (IoT) of Smart Homes: Privacy and Security'. J. Electr. Comput. Eng, vol. 2024, no. 1, 2024. doi.org/10.1155/2024/7716956
[28] M. Rahaman et al., "Privacy-centric AI and IoT solutions for smart rural farm monitoring and control," Sensors, vol. 24, no. 13, p. 4157, 2024. doi.org/10.3390/s24134157
[29] Rai, H. M. 'Enhancing Data Security and Privacy in Energy Applications: Integrating IoT and Blockchain Technologies'. Heliyon, vol. 10, no. 19, 2024. doi.org/10.1016/j.heliyon.2024.e38917
[30] L. P. Rachakonda, M. Siddula, and V. Sathya, "A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in next-generation networks (5G/6G/beyond)," High-Confid. Comput., p. 100220, 2024. doi.org/10.1016/j.hcc.2024.100220
[31] O. Popoola et al., "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions," Blockchain: Res. Appl., vol. 5, no. 2, p. 100178, 2024. doi.org/10.1016/j.bcra.2023.100178
[32] Eghmazi, A. 'Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy'. IoT, vol. 5, no. 1, 2024, pp. 20-34. doi.org/10.3390/iot5010002

How to Cite: Manas Kumar Yogi, Dr. A. S. N. Chakravarthy. (2025). Privacy elasticity: building resilient data protection for cyber physical systems. Journal of Electronics, Computer Networking and Applied Mathematics (JECNAM), 5(1), 1-15. https://doi.org/10.55529/jecnam.51.1.15

BIOGRAPHIES OF AUTHORS

	**Manas Kumar Yogi** currently a research scholar in CSE department of JNTUK Kakinada. He has published more than 270 Papers in various reputed journals, conferences. His research interest is cyber security, soft computing, and Cyber Physical systems. He is also credited with publishing 2 patents in IoT domain and 6 book chapters in reputed publication houses. He can be contacted at Email: manas.yogi@gmail.com

	**Dr. A. S. N. Chakravarthy** currently working as Professor in CSE Department of JNTUK Kakinada. He has published over 160 papers in various International and National journals .He has published 6 patents, authored 5 Books. He is currently guiding many research scholars in the area of cyber security, data mining, image processing, and soft computing. He can be contacted at Email: chakravarthy.cse@jntukucev.ac.in