International Journal of Innovative Research and Scientific Studies, 8(3) 2025, pages: 899-908

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Ensuring the ethical application of user data in IoE-Driven E-commerce: A systematic review with proposed framework

Yin Lei Yee Myint[1], Rajermani Thinakaran[2*], Hushalictmy Paliyanny[3], Kaung Khant Yan Naing[4], Saule Kumargazhanova[5]

[1]*Faculty of Business and Communication, INTI International University, Malaysia.*
[2,3]*Faculty of Data Science and Information Technology, INTI International University, Malaysia.*
[4]*Department of Electronic Engineering, Yangon Technological University, Myanmar.*
[5]*School of Information Technology and Artificial Intelligence, D. Serikbayev East Kazakhstan Technical University, Ust-Kamenogorsk, Kazakhstan.*

Corresponding author: Rajermani Thinakaran (*Email: rajermani.thina@newinti.edu.my*)

Abstract

The purpose of the study is to propose a framework to ensure the ethical application of user data on the Internet of Everything (IoE) commercial platforms by investigating the ethical application of user data on IoE-driven e-commerce platforms, focusing on privacy challenges, regulatory impacts, and innovative privacy-preserving techniques. A systematic literature review (SLR) methodology was employed to analyze existing research on privacy challenges, regulatory frameworks, and technological solutions within IoE-driven e-commerce. The study synthesizes findings from 22 scholarly articles across multiple databases and proposes an Integrated Privacy-Compliance-Innovation (IPCI) Framework to harmonize ethical data use, regulatory compliance, and innovation. The research identifies three critical aspects of privacy in IoE-enabled e-commerce: (1) challenges arising from the integration of IoE technologies, such as data fragmentation and consent complexity; (2) regulatory measures like the General Data Protection Regulation (GDPR) that enforce stricter data protection standards that may hinder innovation; and (3) privacy-preserving approaches, including encryption protocols, blockchain-based systems, and privacy-by-design principles. The IPCI Framework integrates these elements into a cohesive model to address multifaceted privacy concerns while fostering technological innovation. The findings provide actionable insights for policymakers, researchers, and practitioners aiming to enhance trust and compliance in e-commerce ecosystems. The IPCI framework serves as a practical tool for organizations to implement robust privacy measures without compromising innovation. Future empirical testing of the framework across diverse e-commerce settings is recommended to validate its effectiveness. This study establishes a solid base that supports the alignment of innovation methods with user privacy standards in emerging e-commerce systems.

Keywords: Data privacy, E-commerce, Ethical user data, Internet of Everything (IoE), Privacy challenges, Process innovation, Regulatory compliance.

DOI: 10.53894/ijirss.v8i3.6662
Funding: This study received no specific financial support.
History: Received: 6 March 2025 / **Revised:** 7 April 2025 / **Accepted:** 9 April 2025 / **Published:** 2 May 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

The rapid growth of e-commerce has fundamentally transformed the global retail landscape, with the Internet of Everything (IoE) taking digital platforms to unprecedented levels of connectivity and service customization [1]. IoE-enhanced e-commerce systems can provide better customer experiences, more efficient processes, and innovative results by integrating connected devices, real-time analytics, and advanced data processing [2]. These products can be sophisticated recommendation engines, pricing strategies, or even AR-based shopping effects [3]. Yet, with an extensive collection of user data comes increased scrutiny over ethical data usage, namely privacy practices that safeguard consumer data and ensure appropriate use of said data [4].

However, this quest for innovation and seamless user engagement also raises pressing concerns regarding the ethical application of user data. E-commerce platforms often rely on continuous data collection, ranging from personal profiles and purchasing histories to geolocation and biometric metrics, to tailor product recommendations, dynamic pricing, and targeted advertising [5]. While these data-driven strategies can deliver significant competitive advantages and improved customer experiences, they also introduce critical privacy challenges. In this regard, academic literature emphasizes the importance of privacy for sustainable innovation in digital markets [6]. On the one hand, strong privacy practices can reinforce data protection, maximize regulatory compliance, and maintain user dignity, most importantly ensuring ethical use of consumer data [6].

While the dynamics of how privacy and innovation intersect in IoE-enabled e-commerce settings have gained attention, there is still no comprehensive synthesis of how these factors influence the sector's development. Most studies concern technical architecture or isolative privacy frameworks, providing partial perspectives of the relevant ecosystem [7, 8]. In filling this gap, this Systematic Literature Review (SLR) focuses on privacy measures of the ethical usage of user data and innovation outcomes in IoE-enhanced e-commerce, impacting the effectiveness and acceptance of new data-driven solutions.

Extending this focus, the current SLR seeks to explore and synthesize the knowledge base Varsha et al. [9] that explains the effect of privacy measures under the ethical usage of user data on innovation outcomes in the IoE-enabled e-commerce context while underpinning some of the international data privacy laws. Specifically, this review questions four primary aspects of this phenomenon: 1) the key privacy-related challenges that emerge from integrating IoE technologies to drive innovation in e-commerce; 2) current regulations addressing these privacy challenges in IoE-driven e-commerce; 3) the privacy solutions effectively addressing these challenges to enhance IoE adoption in e-commerce platforms; and 4) a framework on directions for future research to focus on balancing ethical data use, user trust, and sustained innovation in the context of IoE-powered e-commerce. Approaching these questions in parallel, the review aspires to bridge the disparate research and practice silos regarding the balance between privacy protection, consumer confidence, and technology advancement, and to enable the pursuit of responsible and long-term forward-looking approaches in a global economy in which the ethics of data and potential for innovation are more intertwined than previously.

The paper is organized as follows: Section 2 summarizes the literature landscape related to privacy and innovation outcomes in IoE-driven e-commerce. Section 3 details the methodology employed in the systematic review. Section 4 provides a discussion of the findings, and Section 5 notes limitations and avenues for future inquiry. Finally, the concluding section synthesizes the overall contributions and emphasizes the study's relevance to researchers, practitioners, and policymakers seeking to harmonize innovation and user privacy in next-generation e-commerce ecosystems.

2. Literature Landscape

This literature landscape explains how regulatory structures influence organization-level innovation capabilities. Businesses need to establish complex methods that comply with changing data protection policies simultaneously while fostering innovative utilization of data [10]. Literature establishes privacy and innovation as core elements that facilitate IoE adoption within e-commerce operations.

2.1. Internet of Everything (IoE)

IoE advances Internet of Things (IoT) technology by linking all internet-connected components, including physical objects, with digital processes as well as data and human users [11]. The linked system delivers enhanced choices, automated operations, and better productivity throughout multiple industry sectors [12]. IoE functions using four basic pillars, including people together with things and data, as well as processes [13]. People use connected devices, including wearables and

smartphones, to both collect data that shapes system operations and utilize these devices to engage with IoE systems [2]. Things that include actuators together with sensors make up the fundamental basis of IoE through their ability to generate real-time data while connecting to physical objects [2]. The study Kumar et al. [2] discussed that the collected data undergoes analysis to optimize processes and improve decision-making, through which devices and individuals establish strategic interactions for value maximization.

Several key technologies support the accomplishment of the IoE vision, especially Artificial Intelligence (AI) within IoE create improvements that include predictive analytics along with autonomous decisions and customized services for end users [14]. IoE implementations transform operations into various domains of application.

2.2. IoE Adoption in E-Commerce

The escalated interconnectivity of IoE enables real-time analytics, hyper-personalized consumer experiences, and frictionless exchange of data in e-commerce settings [15]. Studies on IoT were mainly focused on sensor networks and device interoperability, whereas with IoE, the literature shifts to interlinked ecosystems that combine digital platforms, data-driven services, and machine learning to provide e-commerce solutions [16]. According to researchers, the successful integration of IoE into business enterprises requires companies to modify their operational processes, from optimizing supply chains to creating effective omnichannel marketing strategies that can effectively utilize continuous data flows [17, 18].

2.3. Privacy as an Ethical Imperative

Data privacy stands as the fundamental ethical concern that appears throughout the analyzed literature. The ability to track user activities through detailed information creates competitive opportunities, but privacy infringements combined with unapproved data exchange continue to be major issues [19]. Among current academic studies about IoE deployment in e-commerce, there exist three recognized standard systems that include privacy-by-design concepts along with encryption protocols and General Data Protection Regulation (GDPR) requirements [20, 21]. AngloTel incurred increased complexity and expenses when putting privacy safeguards into practice, which subsequently caused some firms to minimize their investment in protective measures [22]. Community members emphasize privacy as the essential foundation for lasting IoE adoption, which fosters trust and stability [23].

2.4. Innovation as a Competitive Edge

Innovation is one of the top benefits of IoE adoption is innovation. Real-time data collection can also facilitate advanced personalization, more efficient logistics, and better-informed strategic decisions [24]. If used well, businesses that are interfacing with IoE innovation will be able to quickly prototype new services or features. Langley et al. [1] think of voice-enabled shopping assistants or AI-assisted inventory management. These innovations have broadened consumer choice, increased market dynamics, and fostered continuous experimentation, Raji et al. [25] as numerous studies demonstrate. However, there is a growing awareness that innovation needs to be tempered with privacy obligations to maintain consumer goodwill and regulatory compliance[26].

3. Methodology

In this section, the SLR protocol is adopted to analyze how e-commerce platforms use IoE technologies and ethically apply user data. The research adheres to accepted protocols for conducting SLRs in technology and information systems research and follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework for transparent reporting [27]. It forms a comprehensive and substantive overview for policymakers and future scholars of the topic. According to the purpose of this review, the following research questions were identified:

RQ1: What are the key privacy-related challenges that arise from integrating IoE technologies to drive innovation in e-commerce?

RQ2: How do current regulations address these privacy challenges in IoE-driven e-commerce?

RQ3: What are the solutions to resolve privacy challenges, considering regulatory compliance, to enhance IoE adoption and data-driven innovation in e-commerce?

3.1. Study Selection and Eligibility Criteria

Articles were searched and selected from five scholarly literature databases: Google Scholar, MDPI, IGI Global, Springer Nature, and Science Direct. The following keywords were used for the literature search.

- e-commerce: “e-commerce” OR “electronic commerce”
- IoE: “IoE” OR “Internet of Everything”
- Privacy: “privacy” OR “data privacy” OR “privacy challenges” OR “privacy concerns”
- Regulatory: “privacy regulatory” OR “data protection”
- Innovation: “innovation” OR “privacy-by-design”

The only papers are selected from the most relevant sources in conference proceedings, reviews, and journal articles. However, books, chapters, dissertations, and reports have been excluded so that the results in each database are readable and can be filtered in a short time. Moreover, the eligibility criteria were independently applied to all reports as a way of minimizing the risk of selection bias, as described in Table 1. Finally, a total of 22 articles were included in the final review of this study. Each of the selected articles was then read in detail to extract the relevant data to answer the research questions.

The synthesized findings were then the answer to each research question. The PRISMA flow diagram for the systematic review and results is shown in Figure 1.

Table 1.
Inclusion and Exclusion Criteria for Literature Review.

Inclusion Criteria	Exclusion Criteria
Articles must be written in English.	Articles are written in other languages.
Articles are published from 2019 to 2024.	Articles were published before 2019 and after 2024.
Articles published in conferences and journals.	Articles are published on news websites, magazines, and other unreliable sources.
Articles focus on the e-commerce industry.	Articles focus on FMCG, Healthcare, Tourism, and other industries.
Articles dedicated to privacy challenges, regulations, and solutions for IoE-driven e-commerce.	Articles dedicated to consumer behavior, customer trust, digital marketing, and platform features of e-commerce.

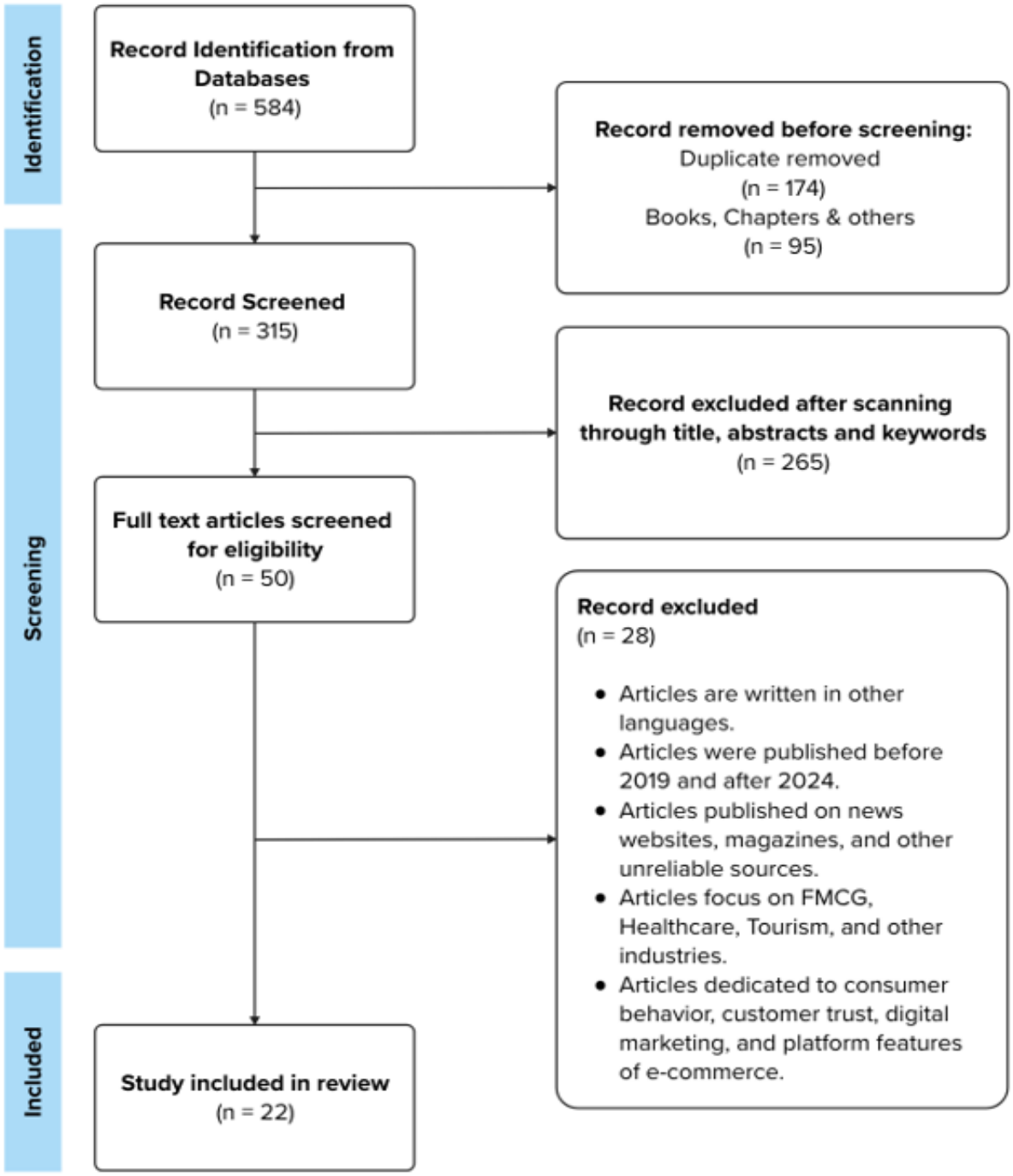

Figure 1.
PRISMA Flow Diagram for SLR.

Table 2 provides a summary illustration for a breakdown of databases by year and the eligible components; privacy challenges, regulations, and solutions, discussed by the studies.

Table 2.
Summary of Eligible Studies from SLR.

Database	Year	Study	Privacy		
			Challenges	Regulations	Solutions
Google Scholar	2024	Jia [28]	Yes	No	No
		Singla [26]	Yes	Yes	Yes
		Yao and Tarofder [29]	Yes	No	Yes
	2023	Arora [30]	Yes	Yes	Yes
		Bashir, et al. [31]	Yes	Yes	Yes
		Nalla and Reddy [32]	Yes	No	Yes
		Noninska and Romansky [33]	Yes	Yes	Yes
		Youssef and Hossam [34]	Yes	No	Yes
	2022	Lu, et al. [35]	Yes	No	Yes
		Nuredini, et al. [36]	Yes	Yes	Yes
		Saberi and Sadeghi [37]	Yes	Yes	Yes
		William [38]	Yes	No	Yes
	2020	Imtiaz, et al. [39]	Yes	No	Yes
MDPI	2024	Morić, et al. [40]	Yes	Yes	Yes
	2023	Saeed [41]	Yes	No	No
	2019	Sun, et al. [42]	Yes	No	No
Spring Nature	2022	Ahi, et al. [43]	Yes	Yes	Yes
	2021	Chawla and Kumar [44]	Yes	Yes	Yes
	2019	Bandara, et al. [45]	Yes	No	No
Science Direct	2023	Bartol, et al. [46]	Yes	No	No
		Haddara, et al. [47]	Yes	Yes	Yes
IGI Global	2023	Picoto, et al. [48]	Yes	No	Yes

4. Discussion

The session uses three main research questions to examine privacy obstacles as well as privacy laws and approaches that resolve user privacy concerns. The discussion introduces the IPCI Framework as the last component. The session utilizes earlier findings on research questions to construct a comprehensive knowledge framework that explains e-commerce system operations between digital innovation and privacy protection abilities.

RQ1: What are the key privacy-related challenges that arise from integrating IoE technologies to drive innovation in e-commerce?

IoT technologies integrated with e-commerce operations create substantial traditional privacy issues, which stem from increasing voluminous data and system fragmentation, and vast network connections. The study by Bandara et al. [45] developed a comprehensive privacy risk categorization system that examines data obtaining and customer approval measures for data saving. As IoE device numbers increase, a severe challenge has emerged for managing large data quantities because these unbroken streams now contain behavioral patterns, geolocation data, and biometric information. A primary issue arises from weak privacy protections because this leads to problems in notifying patients about data collection activities and the effectiveness of data minimization protocols [45].

IoE faces technical issues because devices with dissimilar security protocols expose numerous points at which data can be stolen [48]. IoE creates multiple vulnerabilities to data because of the merged operation of AI with cloud computing systems [34]. The research of Imtiaz et al. [39] and Sun et al. [42] demonstrates that important consumer trust for e-commerce growth suffers due to unclarified data processing standards and complex consent procedures.

Several studies Yao and Tarofder [29] and William [38], show that privacy issues affect digital marketing operations and general consumer defense in web-based businesses, while the study by Noninska and Romansky [33] discusses privacy management in an environment of quick business digitization. Digital transformation is identified as a privacy trap because the pursuit of innovation frequently results in poor privacy security measures [35]. It points out that e-commerce expansion leads to greater risks of both unauthorized data access and possible harm to user privacy [30].

These different studies demonstrate that the main obstacles in e-commerce powered by IoE exist between data governance, consent visibility, and declining consumer confidence. The multiple challenges combine with creating an urgent requirement for structured solutions that will be addressed through the regulatory, technical, and user-centric measures featured in the IPCI Framework.

RQ2: How do current regulations address these privacy challenges in IoE-driven e-commerce?

Current regulatory platforms determine the methods used to handle various privacy difficulties within IoE-driven e-commerce activities. GDPR stands as the most impactful regulation of the present time because it mandates users to grant explicit consent and limits data collection while enabling them to request the complete removal of their data. GDPR forces corporations to change their data management systems through strict legal requirements [40].

Consumer privacy regulations at times restrict analytic data scope, making it harder to achieve personalized innovation [47]. Different regions show substantial variations in their data protection models throughout their regions [38]. Markets with strict compliance requirements face opposition between strong customer safety and technological innovation speed up as increased administrative burdens reduce new technology adoption rates.

The international e-commerce regulations receive special attention as per the studies [37, 43]. Diverse cultural and legal entities oppose the process of harmonization because they hold different perspectives on privacy protection. The degree to which e-commerce marketing privacy concerns differ from jurisdictions maintaining contrasting regulatory approaches toward marketing innovations via their administrative frameworks [29].

Consumer protection laws in global markets constitute an important factor that affects the operation of e-business organizations [31]. The rules support both regulatory compliance and stimulate organizations to adopt advanced methods in data protection, together with risk management practices. The constantly shifting technological environment of IoE systems requires that privacy regulations stay up to date, even though GDPR functions as the baseline standard. ITPCI advances an adaptable framework because its goal follows the need to regulate electronic transactions against advancing technology.

RQ3: What are the solutions to resolve privacy challenges, considering regulatory compliance, to enhance IoE adoption and data-driven innovation in e-commerce?

Proactively designed systems that utilize advanced technology help organizations successfully defend privacy against new e-commerce developments in IoE. The study by Nalla and Reddy [32] recommends using databases that intertwine present-day encryption and anonymization methods. Data protection systems give real-time security while analytics operate without damaging user privacy rights.

The foundation of excellent privacy solutions involves privacy by design. The research by Bartol et al. [46] shows that system developers should integrate privacy features during initial system designs because this proactive approach minimizes vulnerabilities that build user trust. The data shows increased e-commerce platform trust of users when they receive transparent communication about privacy settings, according to Saeed [41].

Voluntary data publishers now have access to the dynamic data publishing model suggested by Jia [28], which dynamically adjusts privacy management for changing data patterns. Blockchain-based data management secures cloud infrastructure and edge computing systems and develops decentralized protection architectures that complement one another [49].

System design with incorporated regulatory requirements helps organizations achieve operational efficiency and maintain their compliance [44]. The development of systemic weaknesses arises from neglecting privacy by design principles throughout system implementation [30, 35]. Current research demonstrates that establishing secure privacy solutions demands a combination of technological defensive elements with government regulations and end-user protections in design processes. Integration between strategies led to the development of the IPCI framework, which establishes a unified framework between innovation advancement and privacy protection.

4.1. Proposing the Integrated Privacy-Compliance-Innovation (IPCI) Framework

IPCI framework integrates the enforcement of privacy law with technology of security and practices of human design to apply procedural risk management protocols across the continuum of different privacy issues being manifested in IoE-based e-commerce systems. Based on the findings obtained from the systematic literature review, CS forms an archetype of the foundational architecture in the supportive pillar of the framework and may also act as a means for the data collector to define the amount of data to be collected per use case, augmented by dynamic audit processes. Apart from the anonymization and the features of the blockchain, modern security measures also include high-end encryption protocols and safe edge processing solutions.

The IPCI Framework allows developers to adopt privacy concepts upfront through its development phase focus, communication protocols, and end-user controls. Privacy continuous monitoring systems play an important role in risk assessment in real-time, providing an update of all the privacy-protecting mechanisms being applied in the system.

Such an IoE-based e-commerce innovation of various policies in terms of privacy and compliance technology is the IPCI framework, which spans the entire spectrum of simultaneous privacy processing and compliance regulation. It consists of four interdependent layers of operation that aid in the retention of privacy aspects in various digital exchanges while allowing for the flexibility that functionality requires.

Regulatory and Policy Compliance Layer works on such data processing processes that comply with GDPR compliance rules or other data protection policies. Further, the base system architecture at this layer introduces security measures that serve as a robust legal basis for the system and impede any regulatory risks while simultaneously boosting user confidence.

Additional layers of security to protect data integrity are layers provided by the Technical Safeguards and Infrastructure Layer. Its security framework merges state-of-the-art encryption methods, data masking protocols, and blockchain-based decentralized technologies. The enforced measures ensure that any sensitive IoE device data is safe and compliant with the laws referring to what data is being processed and why, during the exponentially growing volume of accumulating information. The on-campus or remote and distributed locations of such organizations are protected against such data without an unfavorable effect on its speed and velocity at the cloud and edge computing frameworks.

A user-centric approach with privacy by design to implement protection is built right from the system's inception. The proactive and visible structure holds commons; for whitewashing and barrier practices, and it communicates with its users about privacy settings tightened to a string as an attachment to the communicative systems where everything outland goes. Having a platform that is easy for everyone to use ensures higher customer trust and confidence, which is a key precondition for long-term e-commerce success.

Finally, the Dynamic Risk Assessment and Innovation Support Layer makes sure the structure can be modified to ensure the organization can adapt to current risks and trends. However, continuous monitoring, real-time risk assessments, and agile feedback loops enable live feedback adaptive implementation of privacy controls. This is an essential part of the framework, allowing it to keep up with the fast pace of innovation while continuing to be used as an effective tool for privacy protection, adapting to new IoE technologies, and changing regulatory conditions.

The IPCI Framework presents an all-encompassing solution that aligns authoritative data practices with technological progress, establishing a precedent for secure, compliant, and innovative digital commerce.

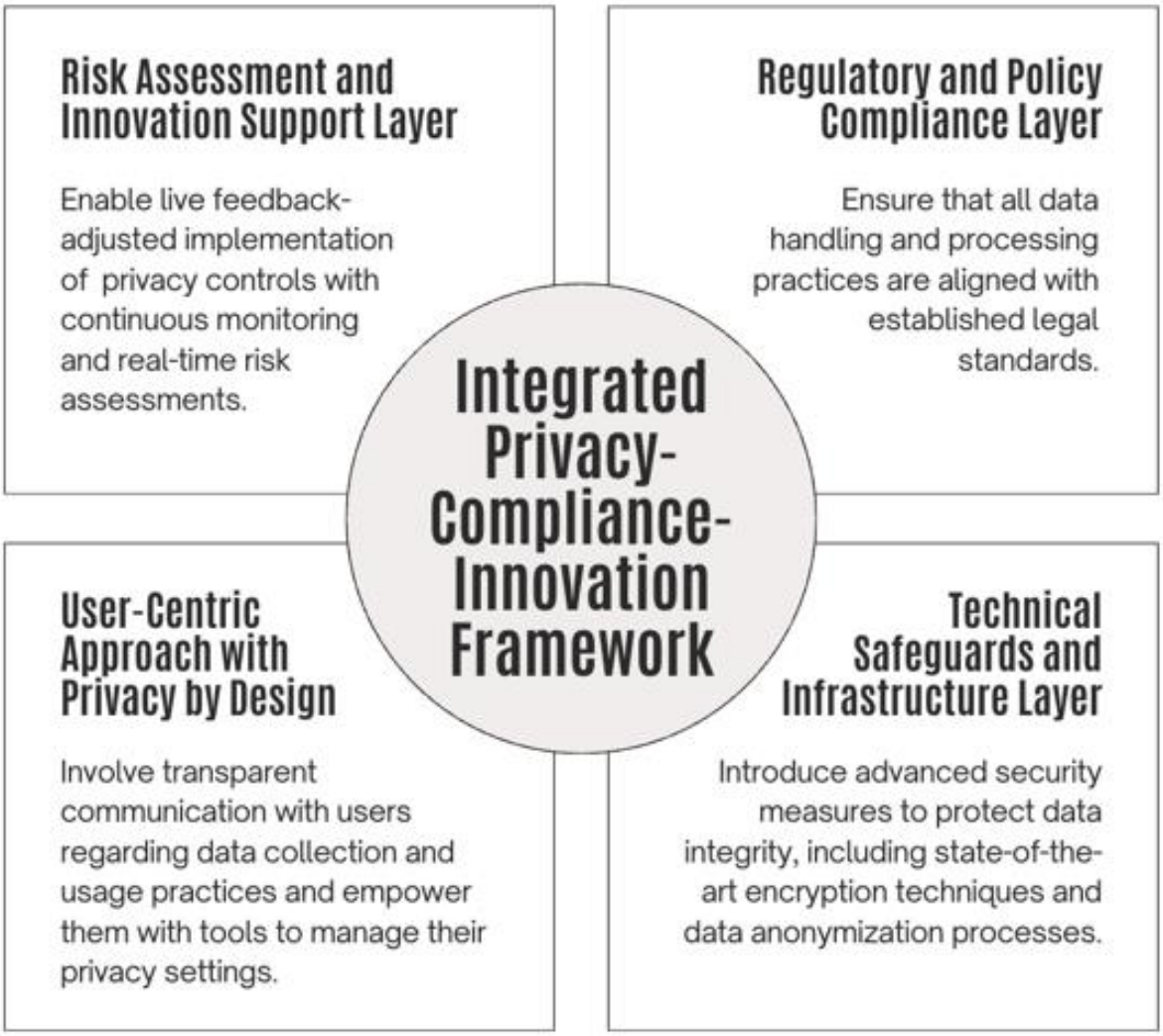

Figure 2.
Proposed Framework of Integrated Privacy-Compliance-Innovation (IPCI).

5. Future Studies

The proposed IPCI Framework provides a wide-ranging system to unite privacy protection with innovative elements of IoE-driven e-commerce yet operates under some limitations. The IPCI Framework experiences limitations because both GDPR and various other conventions require functioning within rapidly shifting legal frameworks of developing economies. Even though several studies Nuredini et al. [36] and Morić et al. [40], focus on regulated areas, the proposed framework requires tailoring to function properly in emerging markets with their specific legal frameworks. IoE's accelerated technological evolution continuously makes technical security methods such as encryption and blockchain with secure cloud solutions obsolete since emerging vulnerabilities and technologies appear [32, 49]. The effectiveness of the framework requires continuous updates through a regular cycle to protect organizations from predicted cyber threats.

One substantial drawback occurs when implementing the various parts of this framework into real-world operational environments because it proves complicated to merge all components effectively. Minimal coordination is necessary between regulatory bodies and business stakeholders, as well as technology developers, to implement the multi-dimensional IPCI Framework successfully. Bartol et al. [46] and Saeed [41], together with other researchers, have exposed difficulties in

implementing “privacy-by-design” and managing user transparency without compromising functionality or system speed. The implementation of risk assessment and feedback loops poses challenges to legacy systems because such systems are not optimized for real-time monitoring or agile adaptation [28, 48].

Identifying many potential research directions exists. The empirical testing of the IPCI Framework should focus on validating it through different e-commerce settings. When applying the framework to new regulatory contexts, future research should use case analyses and pilot implementations, which enable scientists to check its real-world applicability and improve its structure. The research could compare regional regulatory frameworks to determine their impact on IPCI Framework performance while using comparative findings from the studies by Bashir et al. [31] and Nuredini et al. [36]. Observing the potential benefits of applying emerging technology elements to risk assessment through AI or quantum-resistant encryption technology would improve the technical safeguards level of the framework.

Researchers should study the combined impact of social aspects along with technological components that determine performance in user-based privacy systems. Research should study consumer behavior changes related to enhanced privacy [39, 42]. Research across legal domains and technical expertise, and business domains creates better tools that enable researchers to develop appropriate solutions for balancing innovation and strong privacy defenses. The combined strategy forms the foundations to develop adaptive privacy solutions suitable for IoE-driven e-commerce as it advances at a fast pace.

6. Conclusion

This study analyzed ethical user data applications in IoE-driven e-commerce by examining the main privacy challenges, regulatory effects, and the impact of solutions on innovation. The review introduced an IPCI Framework to address the current difficulties. The framework interweaves regulatory compliance, technical safeguards, privacy-by-design principles, and dynamic risk assessment into a cohesive model. The IPCI Framework combines system architecture integration with advanced security technologies to provide institutions with a system for reducing privacy risks while promoting e-commerce innovation.

Even though the IPCI Framework delivers an all-encompassing solution, it operates with specific constraints. The framework depends on conventional regulatory frameworks, which limit its adoption within emerging markets, yet the quick expansion of IoT technologies requires that its technological safeguards be frequently updated. The successful implementation of the IPCI Framework's multiple components depends on extensive stakeholder coordination, which poses operational difficulties for future research to solve.

Future studies must confirm the IPCI Framework through real-world tests in other e-commerce businesses and involve updating the risk assessment to include artificial intelligence and quantum-resistant encryption in an evaluation. Further interdisciplinary research focusing on consumer behavior and the social implications of such privacy enhancements would be helpful for a holistic understanding of the field. Utilization of the existing literature in creating the IPCI Framework shows strong evidence for addressing certain user data ethics challenges in IoE-enabled e-commerce systems. It comes to terms with present-day privacy battles and establishes a foundational infrastructure for an established digital economic system that balances sustainability and moral standards.

References

[1] D. J. Langley, J. Van Doorn, I. C. Ng, S. Stieglitz, A. Lazovik, and A. Boonstra, "The internet of everything: Smart things and their impact on business models," *Journal of Business Research*, vol. 122, pp. 853-863, 2021. https://doi.org/10.1016/j.jbusres.2019.12.035

[2] R. Kumar, S. Narayanan, and G. Kaur, "Future of internet of everything (IOE)," *International Research Journal of Computer Science*, vol. 8, no. 4, pp. 84–92, 2021. https://doi.org/10.26562/irjcs.2021.v0804.003

[3] R. Zimmermann *et al.*, "Enhancing brick-and-mortar store shopping experience with an augmented reality shopping assistant application using personalized recommendations and explainable artificial intelligence," *Journal of Research in Interactive Marketing*, vol. 17, no. 2, pp. 273-298, 2023. https://doi.org/10.1108/jrim-09-2021-0237

[4] N. Radwan, "Big data ethics," Zenodo," *ERN European Organization for Nuclear Research*, 2021. https://doi.org/10.5281/zenodo.4533717

[5] T. T. Tin, "Factors influencing consumer behavior in Malaysia E-Commerce for online shopping," *Pakistan Journal of Life and Social Sciences*, vol. 22, no. 2, 2024. https://doi.org/10.57239/pjlss-2024-22.2.001164

[6] J. R. Saura, D. Ribeiro-Soriano, and D. Palacios-Marqués, "From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets," *International Journal of Information Management*, vol. 60, p. 102331, 2021. https://doi.org/10.1016/j.ijinfomgt.2021.102331

[7] Y. Shen, M. Miettinen, P. Moen, and L. Kutvonen, "Privacy preservation approach in service ecosystems," presented at the In 2011 IEEE 15th International Enterprise Distributed Object Computing Conference Workshops (pp. 283-292). IEEE, 2011.

[8] G. D. Skinner and E. Chang, "An environmentally adaptive conceptual framework for addressing information privacy issues in digital ecosystems," presented at the Inaugural IEEE-IES Digital EcoSystems and Technologies Conference, pp. 302–307. https://doi.org/10.1109/dest.2007.371988, 2007.

[9] P. Varsha, A. Chakraborty, and A. K. Kar, "How to undertake an impactful literature review: Understanding review approaches and guidelines for high-impact systematic literature reviews," *South Asian Journal of Business and Management Cases*, vol. 13, no. 1, pp. 18-35, 2024. https://doi.org/10.1177/22779779241227654

[10] N. Martin, C. Matt, C. Niebel, and K. Blind, "How data protection regulation affects startup innovation," *Information Systems Frontiers*, vol. 21, no. 6, pp. 1307-1324, 2019. https://doi.org/10.1007/s10796-019-09974-2

[11] D. Vaya and T. Hadpawat, "Internet of everything (IoE): A new era of IoT," in *In ICCCE 2019: Proceedings of the 2nd International Conference on Communications and Cyber Physical Engineering (pp. 1-6). Singapore: Springer Singapore*, 2019.

[12] J. Fiaidhi and S. Mohammed, "Internet of everything as a platform for extreme automation," *IT Professional*, vol. 21, no. 1, pp. 21-25, 2019. https://doi.org/10.1109/mitp.2018.2876534

[13] M. Sajid, A. Harris, and S. Habib, "Internet of everything: Applications, and security challenges," presented at the International Conference on Innovative Computing (ICIC), pp. 1–9. https://doi.org/10.1109/icic53490.2021.9691507, 2021.
[14] N. Tang, "Leveraging Big Data and AI for Enhanced Business Decision-Making: Strategies, Challenges, and Future Directions," *Journal of Applied Economics and Policy Studies*, vol. 11, pp. 25-29, 2024.
[15] T. M. Le and S.-Y. Liaw, "Effects of pros and cons of applying big data analytics to consumers' responses in an e-commerce context," *Sustainability*, vol. 9, no. 5, p. 798, 2017. https://doi.org/10.3390/su9050798
[16] F. Aulkemeier, M.-E. Iacob, and J. van Hillegersberg, "Platform-based collaboration in digital ecosystems," *Electronic Markets*, vol. 29, no. 4, pp. 597-608, 2019. https://doi.org/10.1007/s12525-019-00341-2
[17] R. N. Akram, H.-H. Chen, J. Lopez, D. Sauveron, and L. T. Yang, "Security, privacy and trust of user-centric solutions," *Future Generation Computer Systems*, vol. 80, pp. 417-420, 2018. https://doi.org/10.1016/j.future.2017.11.026
[18] S. Pimsakul, P. Samaranayake, and T. Laosirihongthong, "Prioritizing enabling factors of IoT adoption for sustainability in supply chain management," *Sustainability*, vol. 13, no. 22, p. 12890, 2021. https://doi.org/10.3390/su132212890
[19] A. Hagiu and J. Wright, "Data-enabled learning, network effects, and competitive advantage," *The RAND Journal of Economics*, vol. 54, no. 4, pp. 638-667, 2023. https://doi.org/10.1111/1756-2171.12453
[20] M. Barati and O. Rana, "Tracking GDPR compliance in cloud-based service delivery," *IEEE Transactions on Services Computing*, vol. 15, no. 3, pp. 1498-1511, 2020. https://doi.org/10.1109/tsc.2020.2999559
[21] A. D. Kounoudes and G. M. Kapitsaki, "A mapping of IoT user-centric privacy preserving approaches to the GDPR," *Internet of Things*, vol. 11, p. 100179, 2020. https://doi.org/10.1016/j.iot.2020.100179
[22] A. Selzer, D. Woods, and R. Bohme, "An economic analysis of appropriateness under article 32 gdpr," *Eur. Data Prot. L. Rev.*, vol. 7, p. 456, 2021. https://doi.org/10.21552/edpl/2021/3/15
[23] M. Petrescu, A. Krishen, and M. Bui, "The internet of everything: Implications of marketing analytics from a consumer policy perspective," *Journal of Consumer Marketing*, vol. 37, no. 6, pp. 675-686, 2020. https://doi.org/10.1108/jcm-02-2019-3080
[24] Z. Wen, "Research on big data technology leading smart marketing development of logistics industry," presented at the International Conference on Economy Development and Social Sciences Research (EDSSR 2020). https://doi.org/10.25236/edssr.2020.025, 2020.
[25] M. A. Raji, H. B. Olodo, T. T. Oke, W. A. Addy, O. C. Ofodile, and A. T. Oyewole, "E-commerce and consumer behavior: A review of AI-powered personalization and market trends," *GSC Advanced Research and Reviews*, vol. 18, no. 3, pp. 066-077, 2024. https://doi.org/10.30574/gscarr.2024.18.3.0090
[26] A. Singla, "The evolving landscape of privacy law: Balancing digital innovation and individual rights," *Indian Journal of Law*, vol. 2, no. 1, pp. 1–6, 2024. https://doi.org/10.36676/ijl.v2.i1.01
[27] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *bmj*, vol. 372, 2021. https://doi.org/10.1136/bmj.n71
[28] J. Jia, "A Consumer Data Privacy Protection Model Based on Non-Parametric Statistics for Dynamic Data Publishing in e-Commerce Platforms," *HighTech and Innovation Journal*, vol. 5, no. 2, pp. 410-419, 2024. https://doi.org/10.28991/hij-2024-05-02-013
[29] H. Yao and A. K. Tarofder, "Privacy concerns in E-commerce marketing: A systematic literature review study," *International Journal of Global Economics and Management*, vol. 2, no. 3, pp. 64–75, 2024. https://doi.org/10.62051/ijgem.v2n3.07
[30] D. Arora, "Data privacy issues with e-commerce," *International Journal of Social Science and Economic Research*, vol. 8, pp. 1167-1174, 2023. https://doi.org/10.46609/ijsser.2023.v08i05.020
[31] S. Bashir, A. S. Khan, and F. S. Khan, "Impact of online consumer protection laws on e-commerce in global market," *Pakistan Journal of Social Research*, vol. 5, no. 02, pp. 93-99, 2023. https://doi.org/10.52567/pjsr.v5i02.1112
[32] L. N. Nalla and V. M. Reddy, "Data privacy and security in e-commerce: Modern database solutions," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 3, pp. 248-263, 2023. https://doi.org/10.13140/RG.2.2.16554.63682
[33] I. Noninska and R. Romansky, "Features of e-business and e-commerce with a reflection on privacy in the digital age," *International Journal on Information Technologies & Security*, vol. 15, no. 3, 2023.
[34] H. Youssef and A. Hossam, "Privacy issues in AI and cloud computing in e-commerce setting: A review," *International Journal of Responsible Artificial Intelligence*, vol. 13, no. 7, pp. 37-46, 2023.
[35] C.-H. Lu, Y.-H. Chen, and P.-T. Jan, "The privacy trap of digital transformation: The existence and the implication," *Journal of Internet Technology*, vol. 23, no. 1, pp. 63-71, 2022. https://doi.org/10.53106/160792642022012301006
[36] B. Nuredini, J. Xhafaj, and V. Paukovska Dodevska, "A comparative overview of data protection in e-commerce in the european union, the united states of america, the republic of north macedonia, and albania: Models and specifics," *Studia Iuridica Lublinensia*, vol. 31, no. 3, pp. 61-84, 2022. https://doi.org/10.17951/sil.2022.31.3.61-84
[37] R. Saberi and S. Sadeghi, "The future of global e-commerce regulation: Legal challenges in ensuring fair competition, consumer rights, and data protection," Retrieved: https://www.jlsda.com/index.php/lsda/article/view/5. [Accessed 2022.
[38] A. William, "Data Privacy Analysis on E-commerce Application," *International Journal of Technology and Management*, vol. 7, no. 2, pp. 1-29, 2022.
[39] S. Imtiaz, S. H. Ali, and D. J. Kim, "E-commerce growth in Pakistan: Privacy, security, and trust as potential issues," *Culinary Science & Hospitality Research*, vol. 26, no. 2, pp. 10-18, 2020. https://doi.org/10.20878/cshr.2020.26.2.002
[40] Z. Morić, V. Dakic, D. Djekic, and D. Regvart, "Protection of personal data in the context of e-commerce," *Journal of Cybersecurity and Privacy*, vol. 4, no. 3, pp. 731-761, 2024.
[41] S. Saeed, "A customer-centric view of E-commerce security and privacy," *Applied Sciences*, vol. 13, no. 2, p. 1020, 2023. https://doi.org/10.3390/app13021020
[42] Y. Sun, S. Fang, and Y. Hwang, "Investigating privacy and information disclosure behavior in social electronic commerce," *Sustainability*, vol. 11, no. 12, p. 3311, 2019. https://doi.org/10.3390/su11123311
[43] A. A. Ahi, N. Sinkovics, and R. R. Sinkovics, "E-commerce policy and the global economy: a path to more inclusive development?," *Management International Review*, vol. 63, no. 1, pp. 27-56, 2023. https://doi.org/10.1007/s11575-022-00490-1
[44] N. Chawla and B. Kumar, "E-commerce and consumer protection in India: The emerging trend," *Journal of Business Ethics*, vol. 180, no. 2, pp. 581-604, 2022. https://doi.org/10.1007/s10551-021-04884-3

[45] R. Bandara, M. Fernando, and S. Akter, "Privacy concerns in E-commerce: A taxonomy and a future research agenda," *Electronic Markets*, vol. 30, no. 3, pp. 629-647, 2020. https://doi.org/10.1007/s12525-019-00375-6

[46] J. Bartol, V. Vehovar, M. Bosnjak, and A. Petrovčič, "Privacy concerns and self-efficacy in e-commerce: Testing an extended APCO model in a prototypical EU country," *Electronic Commerce Research and Applications*, vol. 60, p. 101289, 2023. https://doi.org/10.1016/j.elerap.2023.101289

[47] M. Haddara, A. Salazar, and M. Langseth, "Exploring the impact of GDPR on big data analytics operations in the E-commerce industry," *Procedia Computer Science*, vol. 219, pp. 767-777, 2023. https://doi.org/10.1016/j.procs.2023.01.350

[48] W. N. Picoto, J. C. Abreu, and P. Martins, "Integrating the Internet of Things into e-commerce: The role of trust, privacy, and data confidentiality concerns in consumer adoption," *International Journal of E-Business Research*, vol. 19, no. 1, pp. 1-18, 2023. https://doi.org/10.4018/ijebr.321647

[49] N. Singh, Y. Do, Y. Yu, I. Fouad, J. Kim, and H. Kim, "Crumbled cookies: Exploring e-commerce websites' cookie policies with data protection regulations," *ACM Transactions on the Web*, vol. 19, no. 1, pp. 1-24, 2025. https://doi.org/10.1145/3708515