RESEARCH-ARTICLE

SoK: Privacy, Security, and Ethical Considerations in Vehicular Data Monetization

ERFAN BAHRAMI, Sharif University of Technology, Tehran, Tehran, Iran

AHMED ABDULLAHI, Manchester Metropolitan University, Manchester, Greater Manchester, U.K.

TOOSKA DARGAHI, Manchester Metropolitan University, Manchester, Greater Manchester, U.K.

Open Access Support provided by:

Manchester Metropolitan University

Sharif University of Technology

Published: 25 August 2025

Citation in BibTeX format

BSCI '25: 7th ACM International Symposium on Blockchain and Secure Critical Infrastructure
August 25 - 29, 2025
Hanoi, Vietnam

Conference Sponsors:
SIGSAC

https://doi.org/10.1145/3709016.3737800
ISBN: 9798400714122

SoK: Privacy, Security, and Ethical Considerations in Vehicular Data Monetization

Erfan Bahrami*
erfan.bahrami98@sharif.edu
Sharif University of Technology
Tehran, Iran

Ahmed Danladi Abdullahi*
a.abdullahi@mmu.ac.uk
Manchester Metropolitan University
Manchester, United Kingdom

Tooska Dargahi
t.dargahi@mmu.ac.uk
Manchester Metropolitan University
Manchester, United Kingdom

Abstract

Vehicular data monetization is expected to revolutionize the automotive industry by unlocking the immense value generated by connected vehicles. However, this shift also raises significant challenges around privacy, security, and ethical governance of such data. This paper examines over 100 scholarly and industry contributions to explore how emerging technologies, such as blockchain and edge computing, are shaping this space and their impact on data breaches, re-identification attacks, and vague data ownership. Detailed discussion of privacy-preserving mechanisms and comprehensive threat models is presented in the paper to highlight the limitations of the existing practices. Beyond the technical aspects, the ethical and legal challenges, such as consent management and fair compensation for data sharing, have been discussed as well. Findings of this study offer a comprehensive overview of the current landscape and underline the need for interdisciplinary collaboration to build secure, efficient, and ethically grounded vehicular data marketplaces.

Keywords

Data Marketplace, Privacy, Cybersecurity, Blockchain, Monetization

ACM Reference Format:
Erfan Bahrami, Ahmed Danladi Abdullahi, and Tooska Dargahi. 2025. SoK: Privacy, Security, and Ethical Considerations in Vehicular Data Monetization. In *The 7th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI '25), August 25–29, 2025, Hanoi, Vietnam.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3709016.3737800

1 Introduction

The exponential growth of connected vehicles presents a transformative opportunity for data monetization in the automotive industry. Modern vehicles, equipped with up to 200 sensors and generating more than 100 data points per second, are projected to be more than $1.2 billion by 2035, which will be a penetration of 65% of the total vehicle, generating between 1.4 and 4 terabytes of data per day [1–3]. These data span technical diagnostics, driving behavior, location history, and user preferences, fueling a global vehicle data market projected to be worth between $80 billion and $800 billion by 2030 [4]. However, data monetization raises challenges related to ownership, privacy, security, and fair value distribution.

A fundamental issue is the ambiguity in data ownership, as vehicle manufacturers, drivers, dealerships, and service providers compete for control over data generated during vehicle operation [5]. This uncertainty extends to storage, processing, and monetization rights, with manufacturers leveraging technological infrastructure while consumers generate valuable behavioral insights. The lack of transparent compensation mechanisms exacerbates the issue, as data is sold to insurers, advertisers, and third parties without clear consumer benefits. Automakers and data aggregators collect extensive information, including GPS location, fuel consumption, and driver biometrics [6, 7]. This often occurs without explicit user consent, and unclear agreements limit consumers' control over their data [8]. Furthermore, imbalanced revenue-sharing models favor manufacturers and data aggregators, leaving vehicle owners with little to no compensation [9, 10].

The security and privacy risks in vehicular data marketplaces are significant, with threats such as identity theft, real-time tracking, and cyberattacks [8, 11, 12]. Regulatory inconsistencies between regions further complicate data protection, while the EU GDPR imposes strict controls, other jurisdictions adopt more flexible frameworks [7]. While blockchain, federated learning, and anonymization have been proposed to mitigate these risks, their real-world adoption remains limited by technical constraints and lack of standardization [13]. Despite ongoing research on vehicular data marketplaces and regulatory frameworks, no comprehensive study systematically addresses the interplay of privacy preservation, security measures, and ethical considerations in data monetization platforms.

This research gap has resulted in suboptimal solutions that fail to capture the full complexity of these challenges. Therefore, this paper systematizes the knowledge of vehicular data marketplaces with a focus on privacy, security, and ethical considerations of both academically proposed frameworks and industry-adopted solutions. The main contributions of this study are as follows:

(1) This is the first comprehensive systematization of knowledge in vehicular data monetization, analyzing 104 papers across security, privacy, and ethical domains.
(2) A detailed discussion of privacy-preserving mechanisms, which are used on such platforms, is presented, along with an evaluation of their effectiveness and critical limitations.
(3) A comprehensive threat model is designed to map various attack vectors and their impacts on marketplace operations

*Both authors contributed equally to this research

BSCI '25, August 25–29, 2025, Hanoi, Vietnam

ACM ISBN 979-8-4007-1412-2/2025/08
https://doi.org/10.1145/3709016.3737800

and monetization risks. This model serves as a foundation for future security analysis in this domain.
(4) Ethical and regulatory landscape of vehicular data monetization has been discussed, and significant gaps between theoretical frameworks and practical implementations have been identified.

This systematization of knowledge (SoK) provides researchers and practitioners with a comprehensive framework for understanding and addressing the challenges in vehicular data monetization, particularly in developing vehicular data marketplaces that respect users' privacy, ensure fair revenue sharing, and maintain the integrity of the data exchanges while highlighting areas requiring further investigation. The rest of the paper is organized as follows: Section 2 discusses related work on this topic. Section 3 presents our methodology. Sections 4, 5, and 6 provide an in-depth analysis of privacy and data governance, security strategies, and ethical and regulatory aspects of vehicular data monetization, respectively. Section 7 reviews enabling technologies, and finally, sections 8 and 9 outline future research directions and conclude the paper.

2 Related Work

Research on vehicular data monetization has grown considerably in recent years. However, most existing studies focus on specific aspects of the problem, such as data analytics, privacy-preserving technologies, or platform business models. These works often overlook the complex interplay of technical feasibility, ethical governance, and domain specific challenges that characterize real-world vehicular data marketplaces. Unlike static contexts, such as enterprise cloud systems, vehicle generated data is continuous, highly contextual, and distributed across multiple stakeholders with competing interests. This environment introduces different difficulties in enforcing user consent, maintaining data integrity, securing real-time exchanges, and ensuring fair compensation. Although previous contributions offer valuable information, they lack a comprehensive framework that addresses these concerns in an integrated manner.

Firouzi et al. [14] conduct a survey and propose a reference architecture integrating multi-party computation and privacy-preserving machine learning for health data monetization ecosystems. Although effective for regulated environments with static trust relationships, their approach does not address the dynamic and decentralized nature of vehicular data flows or the economic governance layers required for commercial marketplaces. Sterk et al. [15] present an empirical taxonomy based on a structured review and data-driven analysis of connected car business models through a four-perspective framework. Their strategic-level synthesis, however, does not engage with privacy risks, cybersecurity infrastructure, or regulatory compliance—elements essential for secure and ethically aligned data marketplaces. George et al. [16] review privacy-preserving techniques and introduce a conceptual framework for data sharing between organizations using differential privacy and secure multiparty analytics. Although the study offers a foundational understanding, it lacks specificity regarding data types, consent modalities, and real-time constraints critical to vehicular applications. Ofulue et al. [17] conduct a systematic literature review synthesizing a holistic framework for data monetization models. Though effective in mapping diverse strategies, their high-level perspective does not address architectural trade-offs, threat models, or enforcement mechanisms for user data rights—key challenges in vehicular data ecosystems. Kumar et al. [18] review data analytics approaches and prognostic models for connected vehicles, identifying commercial opportunities in predictive maintenance and fleet optimization. Their survey emphasizes operational efficiency, but does not delve into privacy concerns or data governance architectures vital for secure data monetization. Zhang et al. [19] conduct a review of game-theoretic methods for analyzing data monetization in competitive environments. While insightful for strategic modeling, the study abstracts away from practical implementation concerns, including data sensitivity, reidentification risks, and mechanisms for user consent. Sterk et al. [20] extend their prior empirical review by developing a comprehensive taxonomy and cluster analysis of data-driven business models in connected cars. Despite its breadth across ten dimensions and seven archetypes, the framework does not explore privacy and security implications across varying business configurations.

In contrast to these works, this study addresses critical gaps in existing research by providing the first comprehensive systematization of knowledge specifically focused on vehicular data monetization. Our analysis synthesizes 104 academic and industrial sources across security architectures, privacy preserving mechanisms, ethical governance models, and regulatory compliance frameworks. This integrated approach enables identification of fundamental limitations in current approaches, systematic comparison of mechanisms across technical and ethical dimensions, and development of a comprehensive threat model tailored to vehicular data marketplaces. The resulting analysis provides a structured foundation for both researchers and practitioners, establishing a solid framework for future research directions and practical implementation strategies that can support the development of trustworthy and equitable data marketplaces specifically designed for the automotive domain. Table 1 presents a comparison of existing SoK articles and survey articles on the subject, highlighting the unique contribution of this study.

3 Methodology

The adopted methodology in this paper consists of the following key steps:

- **Literature search and query terms:** We conducted a systematic literature search in December 2024 across major computer science, security, and blockchain-related academic venues to identify relevant works on security, privacy, and ethical considerations in vehicle data monetization. Our initial search queries included variations and combinations of key terms related to data monetization security, vehicle data marketplaces, blockchain data trading, privacy-preserving data sharing, data marketplace ethics, connected vehicle data privacy, data trading security, and vehicular data ethics. The academic venues searched included IEEE Transactions, ACM Digital Library, NDSS, IEEE S&P, Usenix Security, and Science Library. We additionally examined the top 200 Google Scholar results for "secure vehicular data monetization" and "privacy-preserving vehicle data marketplace". After establishing this initial set of works through database searches,

Table 1: Comparison with existing SoK and survey articles on the topic.

Work	Methodology	Scope	P[1]	S	E	M	Notable contribution
Firouzi *et al.* [14] (2022)	Conceptual review	IoT-based health data ecosystems	●	◐	◐	●	AI and privacy-aware architecture using multi-party computation and privacy-preserving machine learning in healthcare
Sterk *et al.* [15] (2022)	Taxonomy analysis	Data-driven business models in connected cars	○	○	○	●	Four-perspective taxonomy for connected car data-driven business models
George *et al.* [16] (2022)	Conceptual framework	Privacy-preserving data sharing platforms	●	◐	◐	●	Privacy-preserving technologies for secure, cross-organizational data sharing and monetization
Ofulue *et al.* [17] (2022)	Systematic literature review	Data monetization models	○	○	○	●	Holistic framework categorizing trends and managerial implications with research agenda
Kumar *et al.* [18] (2023)	Industry analysis	Vehicle telematics data	○	◐	○	●	connected vehicle data analytics, health prognostics, and monetization opportunities
Zhang *et al.* [19] (2023)	Game-theoretic modeling	Firm-level data monetization strategies	◐	◐	○	●	Direct and indirect data monetization strategies in competitive markets
Sterk *et al.* [20] (2024)	Taxonomy analysis	Data-driven business models in connected cars	◐	○	○	●	10-dimension taxonomy and seven business model archetypes for the connected car domain
This work	Systematic literature review	Vehicular data monetization	●	●	●	●	First comprehensive SoK on privacy, security, and ethics in vehicular data monetization with threat model.

[1] Dimensions are abbreviated as follows: P for privacy, S for security, E for ethical considerations, and M for monetization. In addition, Filled circles ● indicates full coverage, half-filled circles ◐ partial or limited coverage, and empty circles ○ no coverage.

we employed snowball sampling by examining the references of identified papers to discover additional relevant works. We also reviewed documentation and white papers from major automotive and technology companies implementing data marketplaces, including initiatives from BMW, Tesla, Volkswagen, and relevant blockchain platforms [21–23].

- **Paper selection criteria:** We examined the papers manually to assess both their relevance for inclusion and to extract key information about approaches, technical mechanisms, privacy guarantees, and limitations. To be included for analysis, works needed to contain substantial discussion or implementation of security, privacy, or ethical considerations in data monetization systems. The papers needed to address marketplace architectures, privacy-preserving mechanisms, security protocols, or ethical frameworks. Additionally, works had to be applicable to vehicular or IoT data trading contexts and provide technical details beyond high-level descriptions. Only papers published in peer-reviewed venues or as technical reports from recognized institutions were included. Generic papers on blockchain or data privacy without specific application to data marketplaces were excluded, as were papers focusing solely on vehicular networks without data monetization aspects.
- **Results:** Our search yielded 104 relevant papers spanning security architectures, privacy-preserving protocols, ethical frameworks, and data marketplace implementations. The identified works are analyzed in detail in Table 2, with their distribution by category and publication year shown in Figure 1.

For the remainder of this work, we systematically examine our findings across the key aspects of secure and ethical data monetization by analyzing current state-of-the-art approaches, identifying limitations and gaps, and suggesting future research directions. Table 3 shows the details of all the feature analysis of the selected literature for this paper.

4 Privacy and Data Governance

Privacy-preserving architectures in vehicular data monetization face systematic implementation challenges that reveal gaps between theoretical capabilities and practical deployment requirements. As connected vehicles generate massive amounts of personal and sensitive data, the need for robust privacy frameworks is more pressing than ever [20]. Current architectures rely on cryptographic techniques, anonymization strategies, and privacy-by-design frameworks to safeguard users' information [64]. However, despite these advancements, significant gaps remain in the transparency and efficacy of these mechanisms. Cryptographic protocols deployed in vehicular systems reveal systematic trade-offs between security guarantees and operational requirements. Techniques such as homomorphic encryption [6], zero-knowledge proofs [113], and blockchain-based [10, 84] privacy layers offer promising solutions

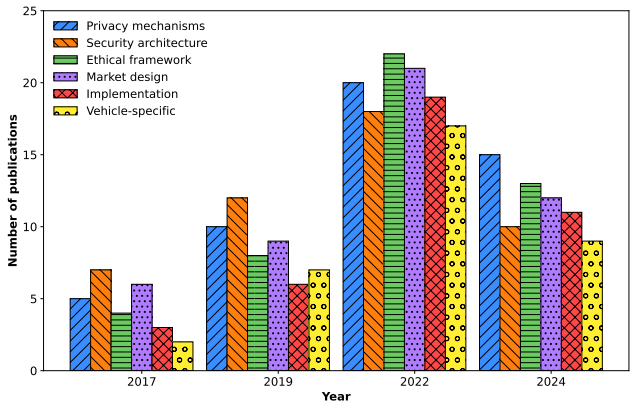

Figure 1: Publication distribution by year and core aspects.

Table 2: Literature search results for data monetization under privacy, security, and ethical considerations.

Core aspect	Summary of focus	Sub-categories	Relevant literature[1]
Privacy mechanisms	Focuses on protecting user privacy in vehicular data collection and monetization. Includes data anonymization, access control, and ownership rights.	Data anonymization	[24], [25], [26], [27],[28] ,[12], [29], [30], [31], [32], [33], [34], [35], [36]
		Access control	[37], [38], [39], [40], [41], [42], [43], [44], [45], [46]
		Data ownership	[29], [47], [48], [10], [11], [49], [50], [51], [52], [53]
Security architecture	Addresses security requirements in vehicular data trading, ensuring data integrity, attack resistance, and secure transactions.	Data integrity	[54], [55], [47], [48], [56], [57], [58], [59], [60], [61]
		Secure trading	[62], [63], [64], [65], [10], [40], [66], [67], [68], [9]
		Attack prevention	[48], [57], [69], [12], [27], [10], [70], [44], [50], [71]
Ethical framework	Establishes ethical guidelines and regulatory compliance for data monetization, focusing on user consent and fair practices.	Consent management	[72], [73], [74], [75], [76], [77], [78], [79], [52], [80]
		Regulatory compliance	[81], [42], [80], [82], [83], [84], [85], [86], [87], [74]
		Fair trading	[64], [88], [20], [89], [4], [90], [91], [92], [93], [94]
Market design	Explores marketplace architectures and business models that balance privacy, security, and monetization.	Architecture	[64], [95], [84], [88], [20], [10], [96], [97], [98], [99]
		Value creation	[20], [88], [84], [95], [64], [42], [100], [18], [101], [102]
		Trading mechanisms	[67], [65], [64], [38], [88], [12], [50], [103], [104], [105]
Implementation	Examines technical implementations with a focus on privacy-preserving and secure architectures.	Blockchain solutions	[106], [107], [5], [55], [41], [108], [109], [110], [111], [112]
		Interoperability	[97], [1], [47], [10], [113], [84], [114], [115], [116], [96]
		Privacy tech	[10], [47], [40], [106], [67], [56], [117], [118], [35], [119]
Vehicle-specific	Addresses unique challenges in vehicular data monetization, including energy trading and history systems.	Data systems	[8], [11], [120], [121], [40], [65], [122], [123], [43], [66]
		Energy trading	[124], [13], [125], [126], [108], [66], [127], [128], [129], [130]
		History systems	[127], [108], [40], [88], [65], [10], [11], [120], [8], [46]

[1] Papers may appear in multiple categories when they address multiple aspects.

to protect user identities while allowing data utilization. For example, blockchain frameworks like those integrated into vehicular systems employ smart contracts to enforce selective disclosure and ensure that only authorized parties access specific datasets. However, these technologies face particular challenges in vehicular contexts, where computational overhead and network synchronization requirements create fundamental tensions with real-time performance demands [12, 120].

Anonymization strategies encounter fundamental challenges when applied to high-dimensional vehicular data streams. Methods such as tokenization and differential privacy are designed to strip datasets of personally identifiable information (PII) [6]. However, re-identification vulnerabilities stem from vehicular data's inherent characteristics: location trajectories, driving patterns, and temporal regularity create unique signatures that persist even after anonymization [127]. These risks highlight the limitations of relying solely on anonymization without incorporating advanced privacy-preserving techniques [7, 47]. Moreover, organizational opacity regarding anonymization implementation compounds this vulnerability, as many platforms provide limited disclosure about their specific procedures, making effectiveness assessment difficult [4, 8]. Privacy-by-design frameworks encounter systematic implementation barriers that highlight tensions between privacy principles and commercial viability [10]. These frameworks advocate for minimizing data collection, employing purpose-specific data usage, and integrating user-centric consent mechanisms [81]. However, user-centric consent mechanisms struggle with the complexity of vehicular data collection scenarios, where continuous, context-dependent data streams make traditional consent models impractical. Additionally, the economic incentives underlying data monetization systems often conflict with data minimization principles [13]. The failure to rigorously enforce these principles has resulted in widespread skepticism among consumers regarding the safety of their data [4].

Interoperability challenges in privacy-preserving mechanisms stem from both technical and regulatory fragmentation [25]. Vehicular data often crosses national borders, where varying regulatory standards can undermine the consistency of privacy protections [64]. Additionally, the absence of standardized data formats and APIs exacerbates the difficulty of implementing cohesive privacy measures. For instance, while GDPR in Europe mandates stringent privacy requirements, equivalent protections are often absent or poorly enforced in other regions, creating disparities in user rights [10]. The transparency deficit in current privacy implementations creates a fundamental accountability gap in vehicular data monetization. Many organizations fail to disclose the specifics of how data is collected, processed, and anonymized [4, 66]. This lack of openness not only undermines consumer trust but also hampers academic and industry efforts to evaluate and improve privacy technologies. Transparency is further limited by the proprietary nature of many data processing algorithms, which are kept from public view under the cover of intellectual property protection [12].

Table 3: Feature analysis of vehicular data monetization works across privacy, security, monetization, evaluation, and transparency perspective

Problem context			Key features																
			Privacy preservation				Security mechanisms				Data monetization				Evaluation			Transparency	
			Data anonymization	Access control	User consent	Data ownership	Encryption	Blockchain integrity	Attack resistance	Secure trading	Market design	Pricing mechanism	Revenue models	Value distribution	Performance	Scalability	Security analysis	User visibility	Market transparency
Work	**Goal**	**Medium**	P1	P2	P3	P4	S1	S2	S3	S4	M1	M2	M3	M4	E1	E2	E3	T1	T2
Koch et al. [25]	Privacy	Blockchain	●	●	●	●	●	●	●	●	●	◐	○	○	●	●	●	●	●
Futoransky et al. [12]	Privacy	Blockchain	●	●	●	◐	●	●	●	●	○	●	○	○	●	●	●	●	●
Klaine et al. [39]	Privacy	Blockchain	●	●	●	●	●	◐	●	◐	○	○	●	○	○	●	●	●	●
Xiong et al. [24]	Privacy	Cloud	●	●	●	●	●	○	●	○	○	○	○	○	●	●	●	●	○
Löbner et al. [32]	Privacy	Edge	●	●	●	◐	●	◐	●	○	○	○	○	○	●	●	●	●	○
Pese et al. [26]	Privacy	Edge	●	●	●	●	●	◐	●	◐	○	○	○	○	●	●	●	●	●
Unterweger et al. [49]	Privacy	EV	●	●	●	●	●	●	◐	○	○	○	○	○	●	○	●	●	●
Song et al. [131]	Privacy	ML	●	●	●	◐	●	●	◐	○	◐	●	○	○	●	●	●	●	○
Gazdag et al. [33]	Privacy	Vehicle	●	●	●	●	●	●	◐	○	○	○	○	○	●	●	●	●	○
Bondia-Barceló et al. [132]	Privacy	Search	●	●	◐	○	●	◐	○	○	○	○	○	○	●	○	●	◐	○
Dai et al. [54]	Security	Blockchain	●	●	●	●	●	●	●	●	●	●	●	◐	●	●	●	●	●
Koutsos et al. [55]	Security	Blockchain	●	●	●	◐	●	●	●	●	○	●	○	○	●	●	●	●	◐
Madine et al. [130]	Security	Blockchain	●	●	●	●	●	●	●	●	●	●	◐	○	●	●	●	●	●
Hong et al. [6]	Security	Blockchain	●	●	●	●	●	●	●	●	●	◐	◐	○	●	●	●	●	◐
Bahrami et al. [48]	Security	Cloud	●	●	●	◐	●	●	●	●	◐	●	○	○	●	●	●	●	○
Li et al. [47]	Security	Edge-Cloud	●	●	◐	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Gupta et al. [29]	Data protection	Blockchain	●	●	●	●	●	●	●	●	●	◐	○	○	●	●	●	●	●
Hei et al. [31]	Data protection	Blockchain	●	●	●	●	●	●	●	●	○	●	○	○	●	●	●	●	●
Badreddine et al. [133]	Data protection	Blockchain	●	●	●	●	●	●	●	◐	●	◐	○	○	●	●	●	●	○
Zhao et al. [129]	Compliance	Data	◐	●	●	◐	●	◐	◐	○	●	●	◐	○	●	◐	○	●	○
Martens et al. [72]	Compliance	Regulatory	●	●	●	●	◐	○	○	○	◐	○	○	○	○	○	○	●	●
Abbas et al. [73]	Compliance	Regulatory	●	●	●	●	●	◐	○	○	◐	◐	○	○	◐	○	○	●	●
Kerber et al. [74]	Compliance	Regulatory	●	●	●	●	◐	○	○	○	◐	○	○	○	○	○	○	●	●
Dogterom et al. [81]	Compliance	Trading	◐	●	●	◐	◐	○	○	○	●	●	◐	○	◐	○	○	●	●
Tang et al. [63]	Data trading	Blockchain	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Li et al. [84]	Data trading	Blockchain	●	●	◐	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Xu et al. [9]	Data trading	Blockchain	●	●	●	●	●	●	●	●	●	●	◐	○	●	●	●	●	●
Yoo et al. [120]	Data trading	Blockchain	●	●	◐	●	●	●	●	●	●	●	◐	◐	●	●	●	●	●
Guan et al. [134]	Data Trading	Blockchain	●	●	◐	●	●	●	●	●	●	●	◐	○	●	●	●	●	●
Chen et al. [62]	Data trading	IoV	○	●	◐	◐	●	◐	●	◐	●	●	●	◐	●	◐	●	◐	●
Javed et al. [7]	Data trading	IoV	●	●	◐	●	●	●	●	●	●	●	●	◐	●	●	●	●	●
Kim et al. [125]	Energy trading	Blockchain	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Aggarwal et al. [126]	Energy trading	Blockchain	●	●	●	◐	●	●	●	●	●	●	●	●	●	●	●	●	●
Lasla et al. [65]	Energy trading	Blockchain	●	◐	●	●	●	●	●	●	●	●	●	◐	●	●	●	●	●
Nguyen et al. [108]	Energy trading	IoV	●	●	●	◐	●	●	●	●	●	●	●	◐	●	●	●	●	●
Hassija et al. [13]	Energy trading	V2G	●	◐	●	●	●	●	●	●	●	●	●	◐	●	●	●	●	●
Xia et al. [124]	Energy trading	V2V	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Wixom et al. [135]	Business	Analysis	◐	○	○	○	○	○	○	○	●	●	●	●	◐	○	○	●	●
Apruzzese et al. [136]	Business	Edge	●	●	●	●	●	◐	●	●	●	●	●	●	●	●	◐	●	●
Sterk et al. [20]	Business	Not specified	○	○	●	○	○	○	○	●	●	●	●	●	●	●	○	●	●
Song et al. [137]	Exchange	Blockchain	●	◐	●	◐	●	●	●	●	●	●	●	◐	●	●	●	●	●
Bauer et al. [88]	Market	Analysis	◐	●	●	◐	◐	○	○	○	●	●	●	●	◐	○	○	●	●
Huang et al. [42]	Market	Analysis	◐	●	●	●	◐	○	○	○	●	●	◐	○	○	○	○	●	●
Xu et al. [64]	Market	Blockchain	◐	●	◐	●	●	●	●	◐	●	●	●	●	●	●	◐	●	●
Pissolatto et al. [95]	Market	Blockchain	●	●	◐	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Samuel et al. [106]	Marketplace architecture	Blockchain	●	●	◐	●	●	●	●	●	●	●	●	◐	●	●	●	●	●
Liu et al. [69]	Marketplace architecture	Blockchain	◐	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Chen et al. [67]	Marketplace architecture	Blockchain	●	●	◐	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Ingrid [113]	Marketplace architecture	Blockchain	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Meneguzzo et al. [107]	Marketplace architecture	Blockchain	●	●	●	◐	●	●	●	●	●	●	◐	◐	●	●	●	●	●
Kilani et al. [138]	Marketplace architecture	Blockchain	●	◐	●	◐	●	●	●	●	●	●	●	◐	●	●	●	●	●
Qabbaah et al. [139]	Marketplace architecture	Data	◐	◐	●	◐	●	◐	◐	●	●	●	●	●	●	◐	○	●	◐
5GMETA [1]	Marketplace architecture	Edge	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Hamed et al. [96]	Marketplace architecture	IoT	◐	●	◐	●	●	◐	●	◐	●	●	◐	○	●	●	◐	●	○
Demchenko et al. [97]	Marketplace architecture	Platform	◐	●	◐	●	●	◐	●	◐	●	●	●	◐	●	●	◐	●	●
Monteiro et al. [140]	Marketplace architecture	Platform	◐	◐	●	◐	◐	◐	◐	●	●	●	●	●	◐	◐	○	●	●

Filled circles ● indicate full support or implementation of a feature, half-filled circles ◐ indicate partial or limited support, empty circles ○ means the feature is not present.

4.1 Privacy-Utility Optimization

Balancing privacy and utility is a critical challenge for vehicular data marketplaces, as stakeholders like automakers, insurers, urban planners, and advertisers each require different levels of data granularity and privacy protection. Several privacy-preserving techniques have distinct limitations: differential privacy protects individuals by adding statistical noise but diminishes data accuracy for applications requiring precise real-time data like navigation or predictive maintenance [84], this trade-off becomes particularly problematic in safety-critical applications where data precision directly impacts operational decisions [20]. Federated learning enables collaborative model training without centralizing raw data but remains vulnerable to adversarial attacks, faces challenges with heterogeneous data distributions common in vehicular contexts, and imposes significant computational overhead in resource-constrained vehicular environments [7, 12]. Similarly, multi-party computation and homomorphic encryption allow secure computations on encrypted data but their substantial complexity and high latency (often seconds or minutes per operation) render them impractical for real-time vehicular applications [8, 141].

The absence of standardized privacy and interoperability protocols further creates friction that reduces marketplace efficiency, with each market participant implementing proprietary solutions that impede seamless data exchange [125]. Recent research suggests that hybrid approaches combining multiple privacy-preserving techniques with context-aware privacy settings may offer more balanced solutions [54], though these approaches require further optimization to address the unique temporal and spatial characteristics of vehicular data [20, 41]. Future research must develop adaptive, context-sensitive privacy mechanisms tailored to the unique requirements of vehicular data ecosystems while accounting for the dynamic nature of both privacy preferences and utility requirements across different use cases.

4.2 Data Governance Framework

Technical data governance in vehicular data ecosystems implements structured control systems through several critical mechanisms. Access control frameworks include role-based approaches [20, 72] that struggle with dynamic stakeholder relationships, more flexible attribute-based systems that better accommodate fluid boundaries but introduce computational complexity [47], and blockchain-enabled solutions [55, 106] that use smart contracts for transparent policy enforcement despite scalability concerns [54, 78]. Data provenance tracking, essential for marketplace trust, employs hash-based integrity verification [54, 55] and distributed ledger systems [5, 106] to document data sources and transformations, though maintaining verifiable records becomes increasingly complex when vehicle sensor data undergoes multiple processing steps (filtering, aggregation, anonymization). These approaches face significant challenges with high-volume vehicular data, leading some implementations to adopt selective provenance tracking that prioritizes critical data streams but requires industry consensus on which data warrants comprehensive documentation.

Interoperability frameworks and metadata management represent crucial yet underdeveloped components of effective governance. The absence of standardized data formats and APIs [64] creates substantial friction in cross-platform exchange, with current vehicular systems operating largely as siloed ecosystems with proprietary data structures despite ongoing standardization efforts by groups like the W3C Automotive Working Group [10, 56, 142]. Semantic interoperability is further complicated by inconsistent interpretations of data across manufacturers, with metrics like "harsh braking" having different threshold definitions [1, 25]. Current metadata tagging systems typically capture only basic attributes such as timestamps and sensor types, lacking comprehensive descriptors for privacy sensitivity and usage restrictions [24, 29], which affects automated governance and compliance verification. Policy expression languages that encode governance rules as machine-readable metadata show promise but lack standardization [8, 25], limiting interoperability between different governance frameworks. Addressing these technical challenges requires a coordinated industry-wide effort to develop common standards as vehicular data volumes continue to grow exponentially [4, 12, 48].

5 Security Strategies for Vehicular Data Integrity and Cyber Threat Mitigation

The security framework for vehicular data monetization forms the foundation of ensuring trust, reliability, and operational integrity in connected ecosystems. As vehicles increasingly become data-generating entities, safeguarding against evolving cyber threats has become an urgent priority. A detailed threat model analysis has been presented in Table 4. This section examines the intertwined pillars of cybersecurity and secure trading frameworks, discussing state-of-the-art approaches, their practical limitations, and the critical gaps that must be addressed to protect vehicular data ecosystems.

5.1 Security and Data Integrity

The challenges of data integrity and security in vehicle data monetization systems stem from fundamental incompatibilities between traditional cybersecurity paradigms and the unique operational demands of connected vehicle environments. Connected vehicles face numerous cybersecurity threats, ranging from data breaches and identity theft to ransomware and DDoS attacks targeting critical vehicular systems [141], while state-of-the-art threat modeling frameworks struggle to account for rapidly evolving attack vectors, such as adversarial manipulations of machine learning-based detection systems [41]. The CIA triad encounters systematic implementation barriers in vehicular contexts, where resource constraints and real-time performance requirements create irreconcilable trade-offs [54]. Traditional cryptographic methods impose computational overhead that exceeds the processing budgets of vehicular hardware while meeting safety-critical latency requirements, and lightweight alternatives raise concerns about their resilience against future quantum computing capabilities [47, 66]. Blockchain technology's immutable transaction records [131] promise enhanced data validation but introduce energy consumption patterns and consensus delays that are systematically incompatible with the immediate response requirements of time-sensitive vehicular applications [20, 107]. These

Table 4: Threat model and impact analysis in vehicular data marketplace

Literature	Data breach	MITM attack	Adversarial ML	DDoS	Ransomware	Re-identification	Insider threat	Quantum threat	Impact on marketplaces	Monetization risks
[10–12, 69]	✓	×	×	×	×	✓	✓	×	Vehicle data leaks compromise sensitive operational patterns and user behaviours, undermining marketplace trust and regulatory compliance	Reduced data sharing willingness leads to decreased marketplace liquidity and revenue streams
[29, 54, 63, 66, 67, 78]	×	✓	✓	×	×	✓	×	×	Manipulated data affects machine learning model accuracy and transaction integrity in automated trading systems	Degraded prediction quality reduces data value and buyer confidence, impacting pricing models
[6, 62]	×	×	×	✓	✓	×	×	×	Service disruptions prevent real-time data exchange between vehicles and infrastructure	Direct revenue loss from service downtime and compensation costs to affected stakeholders
[20, 55, 61, 84]	✓	✓	×	×	×	✓	×	×	Privacy breaches expose vehicle location patterns and user behaviour data	Regulatory fines and reputation damage lead to user withdrawal from data sharing programs
[27, 47, 70, 106]	×	✓	✓	✓	×	×	×	×	Compromised data quality affects real-time decision making in connected vehicle networks	Reduced trust in data authenticity impacts premium pricing and market differentiation
[24, 58]	✓	×	×	×	×	✓	✓	×	Identity exposure risks in vehicle telematics data compromise user privacy	Legal compliance costs increase while data sharing participation decreases
[11, 33, 39, 68]	✓	×	×	×	✓	✓	✓	×	Internal data misuse affects marketplace integrity and stakeholder trust	Increased security costs and reduced marketplace efficiency impact revenue models
[51, 108, 127]	×	✓	×	×	×	×	×	✓	Future quantum computing threats to current cryptographic protections	Investment needed in quantum-resistant security affects operational costs

limitations suggest that vehicular security challenges represent architectural constraints rather than implementation deficiencies, indicating that effective security frameworks must be designed specifically for vehicular operational requirements rather than adapted from traditional computing environments.

5.2 Secure Trading Frameworks

Secure trading frameworks are critical for ensuring trust and operational effectiveness within vehicular data marketplaces. They facilitate smooth data exchanges while protecting against threats such as fraud, unauthorized access, and data manipulation [41]. Trust among diverse stakeholders, including automakers and third-party service providers, is often maintained through reputation-based systems. However, these systems remain susceptible to manipulation, notably through Sybil attacks where malicious actors create multiple false identities to falsely enhance their trustworthiness [63, 121]. Standard encryption protocols such as TLS and DTLS secure communication effectively, but their reliance on centralized certificate authorities creates vulnerabilities like single points of failure [62, 125]. Decentralized alternatives, such as self-sovereign identity systems, address this issue but struggle with interoperability challenges and limited industry acceptance [7, 37]. Furthermore, mechanisms for verifying data integrity—hashing and digital signatures—face challenges due to static key vulnerabilities, computational complexity, high latency, and limited scalability, significantly constraining their effectiveness in real-time, resource-sensitive vehicular contexts [12, 20, 29, 38, 39]. Thus, despite promising advancements, security frameworks in vehicular ecosystems still grapple with significant barriers including centralization risks, interoperability limitations, high computational demands, and latency issues, which collectively restrict broader practical adoption [48].

6 Ethical and Regulatory Landscapes in Vehicular Data Monetization

Ethical and regulatory considerations build trust and legitimacy in vehicular data monetization. They reconcile diverse stakeholder interests while ensuring innovation aligns with both societal values and legal requirements. The following sections examine key ethical and regulatory challenges in this evolving ecosystem.

6.1 Ownership, Consent and Fair Compensation

The fundamental question of data ownership in vehicular ecosystems remains highly contested with significant implications for monetization practices. Automakers frequently assert custodial rights over vehicle-generated data, citing substantial investments in sensory infrastructure and data collection systems [47]. This manufacturer-centric model enables streamlined data commercialization but often marginalizes user interests. Conversely, user-centric models advocate for individual ownership rights, aligning with frameworks like GDPR that recognize personal data as an individual asset subject to user control [39, 47]. This dichotomy creates significant tension in the ecosystem, as neither approach has achieved widespread acceptance or regulatory standardization. Technical solutions attempting to operationalize ownership models through smart contracts and distributed ledger technologies [5, 24, 62] face substantial implementation barriers, including scalability limitations, interoperability challenges, and low user awareness. These persistent gaps highlight the need for balanced governance frameworks that protect individual rights while maintaining sufficient incentives for technological innovation and data utilization.

Informed consent mechanisms, essential for ethical data monetization, remain problematic throughout the industry. Current approaches frequently employ complex, legalistic disclosures that

obscure rather than illuminate data collection, processing, and commercialization practices [20, 29]. Vehicle owners often lack clear understanding of which entities access their data, how it is monetized, and what control options exist. Dynamic consent systems offering granular, context-specific control show promise but face implementation barriers due to integration complexity and substantial development costs, limiting their deployment in production vehicles. Revenue distribution models in current monetization frameworks disproportionately favor industry stakeholders over vehicle owners who generate the valuable data [55]. This imbalance raises significant questions about fairness and creates disincentives for user participation in data sharing. Blockchain-based platforms and tokenization mechanisms offer potential solutions for more equitable value distribution through automated, transparent compensation [39, 56], though these approaches continue to face scalability challenges and lack consensus on fairness metrics for value allocation. The substantial technological literacy required for effective use of data management tools further limits user agency [4], creating practical barriers to the exercise of theoretical data rights. Addressing these interconnected challenges necessitates multidisciplinary solutions combining simplified consent frameworks with equitable monetization models and user education initiatives [84].

6.2 Regulatory Compliance and Data Sovereignty

The regulatory landscape governing vehicular data monetization is characterized by significant fragmentation and jurisdictional complexity. While comprehensive frameworks like GDPR establish data protection principles and user rights [64], their practical application to vehicular contexts remains inconsistent, with technological advancements frequently outpacing regulatory developments. Industry guidelines from standardization bodies [48] attempt to fill these gaps but face enforcement challenges due to their voluntary nature, with many companies implementing guidelines selectively based on commercial priorities [4, 12]. Different regulations across jurisdictions create complex data sovereignty challenges for vehicular data monetization [25, 56]. Vehicle data is typically stored in cloud infrastructures that may operate in different countries than where the vehicles are driven. This separation between data generation and storage locations creates significant compliance problems. For example, data localization laws in some regions require data to be stored locally, which conflicts with global cloud-based storage solutions. Companies must develop hybrid compliance approaches to balance efficient operations with these varied legal requirements [10, 27]. Mechanisms like Standard Contractual Clauses and Binding Corporate Rules help address these cross-jurisdictional data storage issues [66]. However, these legal tools are too complex and expensive for smaller market participants. The limited mutual recognition of data protection standards between countries creates compliance gaps [64, 74]. These regulatory inconsistencies allow questionable data practices to continue where oversight is weaker. The fragmented regulatory landscape encourages many companies to prioritize short-term commercial interests over sustainable data practices [106, 125]. While regulatory bodies have developed accountability frameworks, they see limited voluntary adoption in the automotive sector [25, 143]. Resolving these challenges requires cooperation between regulators, industry leaders, and consumer advocates to develop enforceable international standards that balance accountability requirements with innovation incentives [12, 48].

Figure 2 illustrates an end-to-end architecture for a vehicle data marketplace, depicting the journey from data generation to monetization through four layers. The process begins with Vehicle Data Generation, where connected vehicles (1) utilize their onboard sensors (2) to collect raw data (3), which undergoes initial edge processing for efficiency. This raw telemetry, GPS, and OBD data then flows into the Data Processing and Privacy layer, where incoming processed data (4) undergoes privacy protection measures, resulting in anonymized data (5). The validated data (6) are then managed and prepared for marketplace integration. The architecture leverages Blockchain Infrastructure as its foundational layer, where data assets (7) are transformed into blockchain transactions (8). These transactions are validated through the consensus layer and recorded as blocks (9) in the distributed ledger, ensuring immutability and transparency. The final layer, Marketplace Operations, handles the commercial aspects where listed data (10) is made available through the market interface. This enables trading operations to process orders (11) and facilitate payments (12), completing the monetization cycle. This architecture demonstrates how vehicular data can be securely transformed from raw sensor inputs into valuable marketplace assets while maintaining privacy and ensuring trustworthy transactions through blockchain technology. The systematic flow through these layers ensures data integrity, privacy protection, and efficient market operations, creating a solid foundation for the monetization of vehicular data. However, realizing this architecture depends on a set of enabling technologies that ensure scalability, security, interoperability, and efficiency. The next section explores these technologies, including blockchain, cloud infrastructure, edge and fog computing, advanced communication protocols, and sensor technologies, all of which play a crucial role in the operation of vehicular data marketplaces.

7 Enabling Technologies

The rapid evolution of connected and autonomous vehicles has driven the urgent need for robust technological infrastructure to support data-driven applications and monetization strategies [83, 110]. As vehicular ecosystems become increasingly data-centric, enabling technologies such as blockchain, cloud computing, edge and fog computing, advanced communication protocols, and sensors are revolutionizing how data are processed, secured, and exchanged [60, 61]. These technologies underpin the transformation of vehicular data into a valuable asset, but their integration is riddled with challenges, including interoperability constraints, latency concerns, and security vulnerabilities [103]. This section critically examines the role of these enabling technologies in vehicular data monetization, their state-of-the-art advancements, and the persistent roadblocks that must be addressed to unlock their full potential [58].

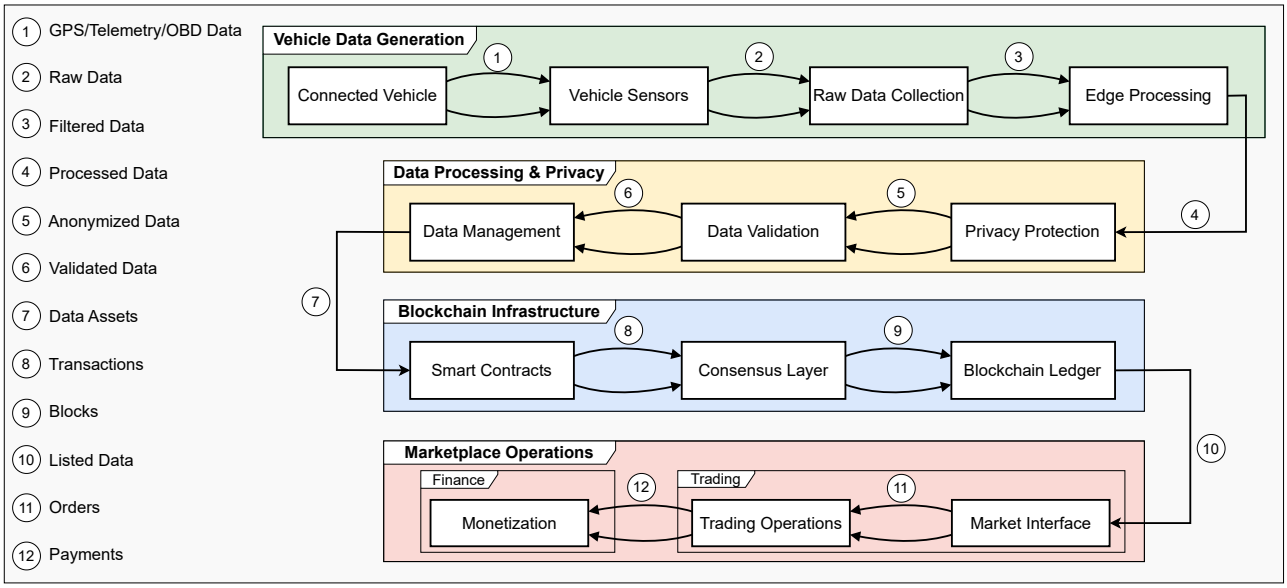

Figure 2: End-to-end architecture for vehicular data marketplaces

7.1 Blockchain

Blockchain has emerged as a foundational technology for vehicular data monetization, offering decentralized solutions that address trust, security, and transparency challenges [41, 63]. By providing an immutable ledger, blockchain facilitates secure data exchanges between stakeholders in vehicular ecosystems [27]. For instance, smart contracts enable automated data transactions while ensuring compliance with predefined terms, reducing reliance on intermediaries [78]. Despite its promise, blockchain faces significant limitations in scalability and energy efficiency [47]. Consensus mechanisms like proof-of-work, while secure, are computationally intensive and ill-suited for high-frequency data exchanges in vehicular networks [84]. Emerging alternatives such as proof-of-stake and proof-of-authority have shown potential to reduce energy consumption, but their adoption is constrained by concerns over centralization and governance [106]. Blockchain applications in vehicular data marketplaces include privacy-preserving trading frameworks and tokenized data economies [55, 57]. However, these solutions often struggle with interoperability, as differing blockchain platforms lack standardized protocols for cross-chain data sharing [68]. Furthermore, the computational overhead associated with blockchain-based solutions limits their applicability in latency sensitive applications, such as real-time navigation and V2V communication [9]. Overcoming these challenges requires innovative approaches, including the development of efficient consensus mechanisms that reduce computational overhead and enhance scalability [47]. Equally important is fostering interoperability through unified standards that allow seamless integration between different blockchain ecosystems and vehicular networks [67].

7.2 Cloud Infrastructure

Cloud infrastructure underpins many of the data storage and processing capabilities required for vehicular data monetization [48, 56]. By providing scalable and cost-effective resources, cloud platforms enable the aggregation and analysis of vast datasets generated by connected vehicles [29]. Applications such as predictive maintenance, dynamic insurance models, and traffic management rely heavily on cloud-based solutions to process real-time data streams [54]. However, the reliance on centralized cloud servers introduces vulnerabilities, including single points of failure and heightened risks of data breaches [27]. Research has explored multi-cloud strategies and hybrid architectures that combine private and public cloud resources to mitigate these risks [63]. These approaches improve system resilience and data redundancy, but they also introduce challenges in managing data governance and ensuring compliance with privacy laws like GDPR and CCPA [74]. Additionally, latency remains a major hurdle, especially for applications that rely on real-time data processing [62]. Future developments must prioritize the integration of edge and fog computing with cloud infrastructure to achieve a balance between scalability and low-latency performance [47].

7.3 Edge and Fog Computing

Edge and fog computing have become critical for decentralizing data processing in vehicular ecosystems [47, 78]. Edge computing processes data locally within vehicles or at nearby nodes, reducing latency and bandwidth requirements [67], which is especially valuable for autonomous driving applications requiring real-time decision-making [29]. Fog computing complements this approach by creating intermediary nodes between edge devices and the cloud, enabling distributed processing across multiple layers [55]. While current implementations include real-time traffic management systems and V2X communication frameworks [57, 63], these technologies face several challenges: localized processing increases hardware tampering risks, poor standardization limits edge-to-cloud interoperability [68], and resource constraints force lightweight

algorithms that may compromise analytical depth [9]. Addressing these issues requires both fortified edge hardware resistant to cyber threats [84] and standardized protocols that ensure smooth data flow across vehicular ecosystems [67].

7.4 Communication Technologies

5G technology has significantly enhanced vehicular communications through features like network slicing and Ultra-Reliable Low-Latency Communication (URLLC) [44]. However, its deployment remains largely urban-centric, leaving rural and remote areas underserved [108]. This disparity has raised concerns over the accessibility and fairness of data monetization models relying on 5G connectivity [57]. Additionally, challenges such as spectrum congestion and high infrastructure costs hinder the widespread rollout of 5G-based vehicular networks [125]. 6G, with its projected advancements in AI-driven networking, sub-millisecond latency, and integrated sensing capabilities, is expected to overcome many of the shortcomings of 5G [110]. Research into THz communications for 6G networks has shown promise in enabling ultra-high-speed data transfers for vehicular applications [9], but practical deployment faces significant barriers, including signal attenuation and the need for new infrastructure [6]. Similarly, VLC technology is being explored as a complementary solution, utilizing light signals for secure, interference-free vehicle communication [84]. While VLC and THz technologies offer high-speed and secure data transmission, their real-world viability remains constrained by line-of-sight dependencies and limited maturity in standardization [67]. Dedicated Short-Range Communication (DSRC) and cellular vehicle-to-everything (C-V2X) technologies remain central to vehicular connectivity [29]. However, DSRC adoption has been slow due to competing standards and regulatory fragmentation [78], while C-V2X adoption is challenged by the need for harmonized frequency allocation across different regions [7]. Hybrid approaches integrating multiple communication technologies, such as a fusion of 5G, VLC, and edge-assisted THz networks, are being investigated to improve network resilience and ensure seamless vehicular connectivity [126]. However, these approaches remain in experimental phases and face challenges related to infrastructure costs, interoperability, and regulatory approval [127].

Despite these advances, vehicular communication technologies continue to grapple with security threats such as eavesdropping, spoofing, and signal jamming [49]. Researchers suggest blockchain-based authentication and quantum encryption techniques to enhance the security of vehicular networks, yet practical implementation remains costly and complex [65]. Furthermore, ensuring interoperability between legacy and next-generation communication protocols is a persistent challenge, requiring industry-wide collaboration to develop standardized frameworks [78]. While the integration of 5G and 6G enabling technologies into vehicular ecosystems holds immense potential, the path to widespread adoption is fraught with technical, economic, and regulatory hurdles [105]. Future research must focus on optimizing these technologies for real-world conditions, enhancing their resilience to ensure equitable and secure vehicular data monetization [74].

7.5 Sensors

Sensors are the primary data generators in connected vehicles, capturing information on vehicle performance, environment, and driver behavior [33]. Advanced sensors such as LiDAR, radar, and high-definition cameras enable applications ranging from autonomous driving to predictive maintenance [34]. These sensors feed vast amounts of data into vehicular ecosystems, forming the foundation for monetization opportunities [77]. The latest advances in sensor technology focus on improving accuracy, range, and integration capabilities [71]. Multi-modal sensor fusion has become a key area of research, enabling more comprehensive and reliable data analysis by combining inputs from multiple sensor types [123]. However, the high cost of advanced sensors remains a barrier to widespread adoption, particularly in low- to mid-range vehicles [60]. Additionally, the massive data volumes generated by sensors strain storage and processing infrastructures, necessitating the adoption of efficient compression and data management techniques [109]. Privacy concerns also arise, particularly with sensors that capture sensitive information, such as in-cabin cameras and biometric sensors [46]. Future research must address these challenges by developing cost-effective sensor solutions, enhancing data compression algorithms, and implementing robust privacy-preserving mechanisms [75].

The effective operation of vehicular data marketplaces relies heavily on these enabling technologies [62]. Individually, each technology contributes uniquely. However, when integrated into a unified system, these technologies frequently encounter significant challenges, particularly related to blockchain scalability, inconsistent data standards, and fragmented cross-border regulatory compliance [67, 69]. Overcoming these barriers requires a collaborative approach between industry, academia, and regulatory institutions to establish comprehensive standards, enhance interoperability, and develop practical and secure technological solutions, and ensure ethical data practices [47, 74]. Such cooperative efforts are essential to fully realize the economic and societal potential of monetising vehicular data.

8 Future Directions

This section outlines key research areas and directions while providing relevant recommendations.

- **Standardizing vehicular data ownership and governance:** To address the existing gaps in vehicular data monetization, future research should focus on developing standardized frameworks for data ownership, security, and fair compensation. Establishing a global consensus on data rights is essential to ensuring that vehicle owners retain greater control over their data while enabling businesses to responsibly extract value. Research should explore decentralized governance models that empower users with direct oversight of data-sharing agreements, potentially through blockchain-based identity and consent management systems.
- **Strengthening security in vehicular data marketplaces:** Vehicular data marketplaces are increasingly vulnerable to security threats such as unauthorized access, data breaches, and data manipulation, particularly given the sensitive nature of the information involved. While blockchain-based architectures offer immutable records and decentralized authentication, challenges

like latency, energy consumption, and scalability in real-time environments remain significant. Emerging solutions, including quantum-resistant cryptography and AI-driven intrusion detection, are essential for countering evolving threats, though they introduce issues such as the need for extensive training data and potential bias. To mitigate these concerns, federated learning models, which facilitate collaborative threat detection without centralized data pooling, and zero-trust architectures employing continuous, multi-factor authentication are being explored to balance robust security with usability in vehicular data transactions.

- **Enhancing privacy in vehicular data marketplaces:** Privacy concerns significantly hinder user participation in vehicular data monetization, as individuals fear losing control over their personal data. While techniques such as differential privacy, homomorphic encryption, and federated learning offer robust protections, they often compromise data utility or face challenges like computational overhead and vulnerability to attacks. Emerging methods such as secure aggregation, adversarially robust models, and synthetic data generation promise to enhance privacy without sacrificing analytical value, yet further research is needed to overcome issues related to network stability, re-identification risks, and legal enforceability. In parallel, regulatory compliance and privacy-by-design frameworks—bolstered by mechanisms like smart contracts—are essential for fostering trust by enabling granular, purpose-specific data sharing.
- **Fair revenue distribution:** The ethical implications of data monetization warrant further exploration, particularly in the areas of transparency, accountability, and value distribution. Research should focus on designing mechanisms for fair revenue sharing that extend beyond traditional corporate-led monetization models. The role of decentralized autonomous organizations (DAOs) in managing data marketplaces could offer a more democratic approach to value distribution, ensuring that data contributors receive equitable returns.
- **Enhancing interoperability across vehicular data ecosystems:** Interoperability remains a critical research challenge, as existing vehicular data ecosystems are highly fragmented. Future work should investigate standardization efforts that facilitate seamless integration between automakers, service providers, and third-party data consumers. Cross-industry collaboration is essential to developing interoperable frameworks that allow data to flow securely and efficiently across different platforms while maintaining compliance with regulatory requirements.
- **Exploring energy data monetization in vehicle-to-grid (V2G) networks:** The monetization of energy data within vehicle-to-grid (V2G) networks is another area that merits deeper investigation. As electric vehicles (EVs) become more prevalent, the ability to trade surplus energy between vehicles and power grids represents a new frontier for data-driven economic models. Research should explore optimal pricing strategies for V2G data transactions, incentive structures for EV owners, and the regulatory implications of decentralized energy markets.

9 Conclusion

This paper has provided a comprehensive exploration of vehicular data monetization, drawing together diverse threads from privacy preservation, cybersecurity, ethical frameworks, and the enabling technologies that underpin these complex ecosystems. The analysis underscores that while advanced cryptographic techniques, privacy-by-design architectures, and decentralized ledger technologies offer promising avenues for protecting user interests, they are consistently challenged by issues of scalability, interoperability, and regulatory fragmentation. The discussion further highlights the critical importance of transparency and accountability in data ownership and access control, illuminating the tensions between the commercial imperatives of automakers and data aggregators and the rights of individual users. Ethical and regulatory considerations have emerged as vital factors in maintaining trust, with informed consent and fair compensation remaining at the forefront of ongoing debates. Simultaneously, the role of emerging technologies—from blockchain and cloud computing to edge and fog processing—has been examined for their capacity to facilitate secure, efficient, and equitable data exchanges, albeit tempered by real-world technical and economic constraints. In synthesizing these findings, the paper not only clarifies current capabilities and limitations but also lays a solid foundation for future research. It calls for a collaborative, interdisciplinary approach to bridge the gap between theory and practice, to standardize protocols across jurisdictions, and to design robust systems that can fully harness the potential of vehicular data while safeguarding privacy and security. This integrated perspective is essential for advancing the field, ensuring that technological innovation aligns with ethical imperatives and regulatory mandates in the pursuit of a truly connected and responsible automotive future.

References

[1] 5GMETA, "5gmeta: Monetizing car data white paper," Sept. 2024.
[2] PTOLEMUS Consulting Group, "The vehicle data market global study," 2020. Accessed: 2025-05-30.
[3] S. Bell, "Global connected vehicle forecast 2024–2035," Apr. 2024. Accessed: 2025-05-30.
[4] Capgemini, "Monetizing vehicle data. how to fulfill the promise," Sept. 2021.
[5] J. Liu, J. Lou, J. Liu, L. Xiong, J. Pei, and J. Sun, "Dealer: an end-to-end model marketplace with differential privacy," *Proceedings of the VLDB Endowment*, vol. 14, p. 957–969, Feb. 2021.
[6] Y. Hong, L. Yang, Z. Xiong, S. S. Kanhere, and H. Jiang, "Ochjrnchain: A blockchain-based security data sharing framework for online car-hailing journey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, p. 5299–5311, June 2024.
[7] M. U. Javed, N. Javaid, M. W. Malik, M. Akbar, O. Samuel, A. S. Yahaya, and J. B. Othman, "Blockchain based secure, efficient and coordinated energy trading and data sharing between electric vehicles," *Cluster Computing*, pp. 1–29, 2022.
[8] A. Engelmann and G. Schwabe, "Certified data chats for future used car markets," *Electronic Markets*, vol. 34, Sept. 2024.
[9] H. Xu, S. Qi, Y. Qi, W. Wei, and N. Xiong, "Secure and lightweight blockchain-based truthful data trading for real-time vehicular crowdsensing," *ACM Transactions on Embedded Computing Systems*, vol. 23, p. 1–31, Jan. 2024.
[10] B.-G. Jeong, T.-Y. Youn, N.-S. Jho, and S. U. Shin, "Blockchain-based data sharing and trading model for the connected car," *Sensors*, vol. 20, p. 3141, June 2020.
[11] C. Chen, C. Wang, T. Qiu, N. Lv, and Q. Pei, "A secure content sharing scheme based on blockchain in vehicular named data networks," *IEEE Transactions on Industrial Informatics*, vol. 16, p. 3278–3289, May 2020.
[12] A. Futoransky, C. Sarraute, A. Waissbein, M. Travizano, and D. Fernandez, "Wibsontree: Efficiently preserving seller's privacy in a decentralized data marketplace," 2020.
[13] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in v2g network," *IEEE Transactions on Vehicular Technology*,

vol. 69, p. 5799–5812, June 2020.
[14] F. Firouzi, B. Farahani, M. Barzegari, and M. Daneshmand, "Ai-driven data monetization: The other face of data in iot-based smart and connected health," *IEEE Internet of Things Journal*, vol. 9, p. 5581–5599, Apr. 2022.
[15] F. Sterk, C. Peukert, F. Hunke, and C. Weinhardt, "Understanding car data monetization: A taxonomy of data-driven business models in the connected car domain," 2022.
[16] Dr. A. Shaji George and A.S. Hovan George, "Data sharing made easy by technology trends: New data sharing and privacy preserving technologies that bring in a new era of data monetization," 2022.
[17] J. Ofulue and M. Benyoucef, "Data monetization: insights from a technology-enabled literature review and research agenda," *Management Review Quarterly*, vol. 74, p. 521–565, Nov. 2022.
[18] V. Kumar, D. Zhu, and S. R. Dadam, "Connected vehicle data – prognostics and monetization opportunity," tech. rep., Oct. 2023.
[19] X. Zhang, W. T. Yue, Y. Yu, and X. Zhang, "How to monetize data: An economic analysis of data monetization strategies under competition," *Decision Support Systems*, vol. 173, p. 114012, Oct. 2023.
[20] F. Sterk, A. Stocker, D. Heinz, and C. Weinhardt, "Unlocking the value from car data: A taxonomy and archetypes of connected car business models," *Electronic Markets*, vol. 34, Feb. 2024.
[21] BMW Group, "BMW CarData - Welcome to BMW CarData," 2025. Accessed: 2025-05-30.
[22] Tesla, Inc., "What is Fleet API?." https://developer.tesla.com/docs/fleet-api/getting-started/what-is-fleet-api, 2025. Accessed: 2025-05-30.
[23] D. Mukherjee, A. Taylor, M. Mikoleizig, R. Kumar, S. Almond, and W. W. Sun, "How volkswagen autoeuropa built a data mesh to accelerate digital transformation using amazon datazone," October 2024. Accessed: 2025-05-30.
[24] J. Xiong, R. Ma, L. Chen, Y. Tian, Q. Li, X. Liu, and Z. Yao, "A personalized privacy protection framework for mobile crowdsensing in iiot," *IEEE Transactions on Industrial Informatics*, vol. 16, p. 4231–4241, June 2020.
[25] K. Koch, S. Krenn, T. Marc, S. More, and S. Ramacher, "Kraken: a privacy-preserving data market for authentic data," in *Proceedings of the 1st International Workshop on Data Economy*, CoNEXT '22, p. 15–20, ACM, Dec. 2022.
[26] M. D. Pesé, J. W. Schauer, M. Mohan, C. Joseph, K. G. Shin, and J. Moore, "Pricar: Privacy framework for vehicular data sharing with third parties," in *2023 IEEE Secure Development Conference (SecDev)*, p. 184–195, IEEE, Oct. 2023.
[27] H. Liu, W. Tai, Y. Wang, and S. Wang, "A blockchain-based spatial data trading framework," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, Aug. 2022.
[28] Y. Liu, Y. Zhang, Y. Yang, and Y. Ma, "Docs: A data ownership confirmation scheme for distributed data trading," *Systems*, vol. 10, p. 226, Nov. 2022.
[29] P. Gupta, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trailchain: Traceability of data ownership across blockchain-enabled multiple marketplaces," *Journal of Network and Computer Applications*, vol. 203, p. 103389, July 2022.
[30] L. Determann, "No one owns data," *Hastings LJ*, vol. 70, p. 1, 2018.
[31] Y. Hei, J. Liu, H. Feng, D. Li, Y. Liu, and Q. Wu, "Making ma-abe fully accountable: A blockchain-based approach for secure digital right management," *Computer Networks*, vol. 191, p. 108029, May 2021.
[32] S. Löbner, F. Tronnier, S. Pape, and K. Rannenberg, "Comparison of de-identification techniques for privacy preserving data analysis in vehicular data sharing," in *Computer Science in Cars Symposium*, CSCS '21, p. 1–11, ACM, Nov. 2021.
[33] A. Gazdag, S. Lestyán, M. Remeli, G. Ács, T. Holczer, and G. Biczók, "Privacy pitfalls of releasing in-vehicle network data," *Vehicular Communications*, vol. 39, p. 100565, Feb. 2023.
[34] S. Prevost and H. Kettani, "On data privacy in modern personal vehicles," in *Proceedings of the 4th International Conference on Big Data and Internet of Things*, BDIoT'19, p. 1–4, ACM, Oct. 2019.
[35] M. Xu, L. A. Dennis, and M. A. Mustafa, "Safeguard privacy for minimal data collection with trustworthy autonomous agents," in *Proceedings of the 23rd International Conference on Autonomous Agents and Multiagent Systems*, AAMAS '24, (Richland, SC), p. 1966–1974, International Foundation for Autonomous Agents and Multiagent Systems, 2024.
[36] E. P. d. Mattos, A. C. Domingues, F. A. Silva, H. S. Ramos, and A. A. Loureiro, "Protect your data and i'll show its utility: A practical view about mix-zones impacts on mobility data for smart city applications," in *Proceedings of the Int'l ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, amp; Ubiquitous Networks*, MSWiM '23, p. 45–52, ACM, Oct. 2023.
[37] M. Travizano, C. Sarraute, G. Ajzenman, and M. Minnoni, "Wibson: A decentralized data marketplace," 2018.
[38] N. Hynes, D. Dao, D. Yan, R. Cheng, and D. Song, "A demonstration of sterling: a privacy-preserving data marketplace," vol. 11, p. 2086–2089, Association for Computing Machinery (ACM), Aug. 2018.
[39] P. V. Klaine, H. Xu, L. Zhang, M. Imran, and Z. Zhu, "A privacy-preserving blockchain platform for a data marketplace," *Distributed Ledger Technologies: Research and Practice*, vol. 2, p. 1–16, Mar. 2023.
[40] Y.-T. Jiang and H.-M. Sun, "A blockchain-based vehicle condition recording system for second-hand vehicle market," *Wireless Communications and Mobile Computing*, vol. 2021, Jan. 2021.
[41] J. Christidis, P. A. Karkazis, P. Papadopoulos, and H. C. N. Leligou, "Decentralized blockchain-based iot data marketplaces," July 2022.
[42] L. Huang, M. Ladikas, G. He, J. Hahn, and J. Schippl, "A multi-sided market of personal data resource allocation: An empirical study of china's car-hailing platform," *Competition and Regulation in Network Industries*, vol. 22, p. 189–211, Sept. 2021.
[43] H. Karim and D. B. Rawat, "Tollsonly please—homomorphic encryption for toll transponder privacy in internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, p. 2627–2636, Feb. 2022.
[44] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, "Sdn-based secure and privacy-preserving scheme for vehicular networks: A 5g perspective," *IEEE Transactions on Vehicular Technology*, vol. 68, p. 8421–8434, Sept. 2019.
[45] I. Sharma and A. Aggarwal, "Digital footprints and the battle for data sovereignty: Digital privacy, security, and ownership," in *Driving Decentralization and Disruption With Digital Technologies*, p. 74–83, IGI Global, Jan. 2024.
[46] P. Bossauer, T. Neifer, G. Stevens, and C. Pakusch, "Trust versus privacy: Using connected car data in peer-to-peer carsharing," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, p. 1–13, ACM, Apr. 2020.
[47] C. Li, Y. Yuan, and F.-Y. Wang, "A novel framework for data trading markets based on blockchain-enabled federated learning," in *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*, p. 3392–3397, IEEE, Oct. 2022.
[48] S. Bahrami and R. Ghasemi, "A new secure and searchable data outsourcing leveraging a bucket-chain index tree," *Journal of Information Security and Applications*, vol. 67, p. 103206, June 2022.
[49] A. Unterweger, F. Knirsch, D. Engel, D. Musikhina, A. Alyousef, and H. de Meer, "An analysis of privacy preservation in electric vehicle charging," Apr. 2022.
[50] A. M. Kharman, C. Jursitzky, Q. Zhou, P. Ferraro, J. Marecek, P. Pinson, and R. Shorten, "An adversarially robust data-market for spatial, crowd-sourced data," *Distributed Ledger Technologies: Research and Practice*, Nov. 2024.
[51] F. A. Al-Zahrani, "Subscription-based data-sharing model using blockchain and data as a service," *IEEE Access*, vol. 8, p. 115966–115981, 2020.
[52] T. Jakobi, F. Alizadeh, M. Marburger, and G. Stevens, "A consumer perspective on privacy risk awareness of connected car data use," in *Mensch und Computer 2021*, MuC '21, p. 294–302, ACM, Sept. 2021.
[53] D. Suo, J. Siegel, and A. Soley, "Driving data dissemination: The "term" governing connected car information," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, p. 20–30, 2021.
[54] W. Dai, C. Dai, K.-K. R. Choo, C. Cui, D. Zou, and H. Jin, "Sdte: A secure blockchain-based data trading ecosystem," *IEEE Transactions on Information Forensics and Security*, vol. 15, p. 725–737, 2020.
[55] V. Koutsos, D. Papadopoulos, D. Chatzopoulos, S. Tarkoma, and P. Hui, "Agora: A privacy-aware data marketplace," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, p. 3728–3740, Nov. 2022.
[56] K. Figueredo, D. Seed, and C. Wang, "A scalable, standards-based approach for iot data sharing and ecosystem monetization," *IEEE Internet of Things Journal*, vol. 9, p. 5645–5652, Apr. 2022.
[57] R. Kakkar, R. Gupta, S. Agrawal, S. Tanwar, and R. Sharma, "Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5g," *Journal of Information Security and Applications*, vol. 67, p. 103179, June 2022.
[58] A. Mohammad, S. Vargas, and P. Čermák, "Using blockchain for data collection in the automotive industry sector: A literature review," *Journal of Cybersecurity and Privacy*, vol. 2, p. 257–275, Apr. 2022.
[59] G. Saldamli, K. Karunakaran, V. K. Vijaykumar, W. Pan, S. Puttarevaiah, and L. Ertaul, "Securing car data and analytics using blockchain," in *2020 Seventh International Conference on Software Defined Systems (SDS)*, p. 153–159, IEEE, Apr. 2020.
[60] A. Javaid, M. Zahid, I. Ali, R. J. U. H. Khan, Z. Noshad, and N. Javaid, "Reputation system for iot data monetization using blockchain," in *Advances on Broad-Band Wireless Computing, Communication and Applications*, p. 173–184, Springer International Publishing, 2020.
[61] Z. Abubaker, A. U. Khan, A. Almogren, S. Abbas, A. Javaid, A. Radwan, and N. Javaid, "Trustful data trading through monetizing iot data using blockchain based review system," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 5, p. e6739, 2022.
[62] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, p. 9110–9121, Sept. 2019.
[63] H. Tang, Y. Qiao, F. Yang, B. Cai, and R. Gao, "dmobas: A data marketplace on blockchain with arbitration using side-contracts mechanism," *Computer Communications*, vol. 193, p. 10–22, Sept. 2022.
[64] C. Xu, K. Zhu, C. Yi, and R. Wang, "Data pricing for blockchain-based car sharing: A stackelberg game approach," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, p. 1–5, IEEE, Dec. 2020.

[65] N. Lasla, M. Al-Ammari, M. Abdallah, and M. Younis, "Blockchain based trading platform for electric vehicle charging in smart cities," *IEEE Open Journal of Intelligent Transportation Systems*, vol. 1, p. 80–92, 2020.

[66] A. Sadiq, M. U. Javed, R. Khalid, A. Almogren, M. Shafiq, and N. Javaid, "Blockchain based data and energy trading in internet of electric vehicles," *IEEE Access*, vol. 9, p. 7000–7020, 2021.

[67] W. Chen, W. Yang, M. Xiao, L. Xue, and S. Wang, "Lbdt: A lightweight blockchain-based data trading scheme in internet of vehicles using proof-of-reputation," *IEEE Transactions on Mobile Computing*, vol. 24, p. 2800–2816, Apr. 2025.

[68] D. Hu, Y. Li, L. Pan, M. Li, and S. Zheng, "A blockchain-based trading system for big data," *Computer Networks*, vol. 191, p. 107994, May 2021.

[69] K. Liu, W. Chen, Z. Zheng, Z. Li, and W. Liang, "A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles," *IEEE Internet of Things Journal*, vol. 6, p. 9098–9111, Oct. 2019.

[70] S. Khezr, A. Yassine, and R. Benlamri, "Towards a secure and dependable iot data monetization using blockchain and fog computing," *Cluster Computing*, vol. 26, p. 1551–1564, Apr. 2023.

[71] S. Sodagari, "Trends for mobile iot crowdsourcing privacy and security in the big data era," *IEEE Transactions on Technology and Society*, vol. 3, p. 199–225, Sept. 2022.

[72] B. Martens and F. Mueller-Langer, "Access to digital car data and competition in aftermarket maintenance services," Mar. 2020.

[73] A. E. Abbas, W. Agahari, M. van de Ven, A. Zuiderwijk, and M. de Reuver, "Business data sharing through data marketplaces: A systematic literature review," Dec. 2021.

[74] W. Kerber and D. Gill, "Access to data in connected cars and the recent reform of the motor vehicle type approval regulation," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 10, p. 244, 2019.

[75] S.-A. Elvy, "The vehicle monitoring and collection technology era," *Iowa L. Rev.*, vol. 110, p. 43, 2024.

[76] J. Clark, "Antitrust and data: What your car knows and who it should tell," *Journal of European Competition Law amp; Practice*, vol. 12, p. 82–91, Feb. 2021.

[77] T. A. Hemphill, P. Longstreet, and S. Banerjee, ""automotive repairs, data accessibility, and privacy and security challenges: A stakeholder analysis and proposed policy solutions"," *Technology in Society*, vol. 71, p. 102090, Nov. 2022.

[78] L. Wu, X. Li, R. Zhao, W. Lu, J. Xu, and F. Xue, "A blockchain-based model with an incentive mechanism for cross-border logistics supervision and data sharing in modular construction," *Journal of Cleaner Production*, vol. 375, p. 133460, Nov. 2022.

[79] W. Koehler, C. Schultz, and C. Rasche, "Data are the fuel for digital entrepreneurship-but what about data privacy?," in *Handbook of Digital Entrepreneurship*, pp. 306–322, Edward Elgar Publishing, Nov. 2022.

[80] W. Kerber, "Data governance in connected cars: The problem of access to in-vehicle data," working paper, University of Marburg - School of Business & Economics, Nov. 2018. Forthcoming in: Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC).

[81] N. Dogterom, D. Ettema, and M. Dijst, "Tradable credits for managing car travel: a review of empirical research and relevant behavioural approaches," *Transport Reviews*, vol. 37, no. 3, pp. 322–343, 2017.

[82] O. Köster, "Legal evaluation of monetizing automotive data," in *Automatisiertes Fahren 2020*, p. 77–89, Springer Fachmedien Wiesbaden, 2021.

[83] D. Wuhrmann and S. Hessel, "Digitalization of the automotive industry: New legal challenges for cyber security and data use," in *Automatisiertes Fahren 2022*, p. 203–213, Springer Fachmedien Wiesbaden, 2024.

[84] J. Li, J. Li, X. Wang, R. Qin, Y. Yuan, and F.-Y. Wang, "Multi-blockchain based data trading markets with novel pricing mechanisms," *IEEE/CAA Journal of Automatica Sinica*, vol. 10, p. 2222–2232, Dec. 2023.

[85] B. Falkhofen, "Car data platforms and the EU acquis for digital services: How the digital transformation of the car interacts with EU data protection, cybersecurity and competition law," *Computer Law Review International*, vol. 19, no. 6, pp. 165–174, 2018.

[86] B. Martens and F. Mueller-Langer, "Access to digital car data and competition in aftersales services," tech. rep., 2018. Available at SSRN 3262807.

[87] M. D. Pesé and K. G. Shin, "Survey of automotive privacy regulations and privacy-related attacks," Apr. 2019.

[88] I. Bauer, L. Zavolokina, and G. Schwabe, "Is there a market for trusted car data?," *Electronic Markets*, vol. 30, no. 2, p. 211–225, 2020.

[89] C. Segerstedt and J. Svedberg, "Understanding the business value of customer data from connected services-an exploratory case study of what business value an emerging automotive oem can create from customer data generated by connected services," 2021.

[90] G. Malgieri and B. Custers, "Pricing privacy – the right to know the value of your personal data," *Computer Law amp; Security Review*, vol. 34, p. 289–303, Apr. 2018.

[91] S. A. Azcoitia, C. Iordanou, and N. Laoutaris, "Measuring the price of data in commercial data marketplaces," in *Proceedings of the 1st International Workshop on Data Economy*, CoNEXT '22, p. 1–7, ACM, Dec. 2022.

[92] P. Hanafizadeh and M. R. Harati Nik, "Configuration of data monetization: A review of literature with thematic analysis," *Global Journal of Flexible Systems Management*, vol. 21, p. 17–34, Dec. 2020.

[93] S. A. Azcoitia and N. Laoutaris, "A survey of data marketplaces and their business models," *ACM SIGMOD Record*, vol. 51, p. 18–29, Nov. 2022.

[94] R. RADEVSKI and D. SANDS, "Exploring data monetization to customers outside the core business," 2021.

[95] E. C. Pissolatto and F. Hessel, "edna: A decentralized marketplace architecture for the automotive sector," in *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*, p. 858–863, IEEE, Nov. 2024.

[96] N. Hamed, A. Gaglione, A. Gluhak, O. Rana, and C. Perera, "Query interface for smart city internet of things data marketplaces: A case study," *ACM Transactions on Internet of Things*, vol. 4, p. 1–39, Aug. 2023.

[97] Y. Demchenko, R. Cushing, W. Los, P. Grosso, C. de Laat, and L. Gommans, "Open data market architecture and functional components," in *2019 International Conference on High Performance Computing amp; Simulation (HPCS)*, p. 1017–1021, IEEE, July 2019.

[98] M. Bark and R. Sheik, "Generation of digital revenue streams in an automobile firm," 2021.

[99] P. Camps-Aragó, S. Delaere, and R. D'Hauwers, "Value networks and monetization strategies for c-its safety use cases," in *Proceedings of the 7th International Conference on Vehicle Technology and Intelligent Transport Systems*, p. 341–349, SCITEPRESS - Science and Technology Publications, 2021.

[100] N. Tsolakis, R. Schumacher, M. Dora, and M. Kumar, "Artificial intelligence and blockchain implementation in supply chains: a pathway to sustainability and data monetisation?," *Annals of Operations Research*, vol. 327, p. 157–210, Aug. 2023.

[101] K. Kirkpatrick, "Monetizing your personal data," *Communications of the ACM*, vol. 65, p. 17–19, Dec. 2021.

[102] J. Baecker, M. Engert, M. Pfaff, and H. Krcmar, "Business strategies for data monetization: Deriving insights from practice," in *WI2020 Zentrale Tracks*, p. 972–987, GITO Verlag, Mar. 2020.

[103] A. Suliman, Z. Husain, M. Abououf, M. Alblooshi, and K. Salah, "Monetization of iot data using smart contracts," *IET Networks*, vol. 8, p. 32–37, Jan. 2019.

[104] W. Xiong and L. Xiong, "Smart contract based data trading mode using blockchain and machine learning," *IEEE Access*, vol. 7, p. 102331–102344, 2019.

[105] O. Briante, C. Campolo, A. Iera, A. Molinaro, S. Y. Paratore, and G. Ruggeri, "Supporting augmented floating car data through smartphone-based crowdsensing," *Vehicular Communications*, vol. 1, p. 181–196, Oct. 2014.

[106] C. N. Samuel, F. Verdier, S. Glock, and P. Guitton-Ouhamou, "A fair crowdsourced automotive data monetization approach using substrate hybrid consensus blockchain," *Future Internet*, vol. 16, p. 156, Apr. 2024.

[107] S. Meneguzzo, A. Favenza, V. Gatteschi, C. Schifanella, *et al.*, "Blockchain for data marketplace: Enhancing security, privacy, and trust," 2021.

[108] L. D. Nguyen, I. Leyva-Mayorga, A. N. Lewis, and P. Popovski, "Modeling and analysis of data trading on blockchain-based market in iot networks," *IEEE Internet of Things Journal*, vol. 8, p. 6487–6497, Apr. 2021.

[109] C. Kaiser, M. Steger, A. Dorri, A. Festl, A. Stocker, M. Fellmann, and S. Kanhere, "Towards a privacy-preserving way of vehicle data sharing – a case for blockchain technology?," in *Advanced Microsystems for Automotive Applications 2018*, p. 111–122, Springer International Publishing, Jan. 2019.

[110] S. Kolasani, "Connected cars and autonomous vehicles: Personalizing owner/customer experiences and innovation using ai, iot, blockchain, and big data," *International Numeric Journal of Machine Learning and Robots*, vol. 8, no. 8, pp. 1–17, 2024.

[111] O. O. Odiete *et al.*, *Using blockchain to support data & service monetization.* PhD thesis, University of Saskatchewan, 2018.

[112] T. Lahtinen, A. Costin, G. Suarez-Tangil, and N. Yousefnezhad, "A review on privacy and monetization aspects within bci and xr-bci ecosystems," in *Business Modeling and Software Design*, p. 166–185, Springer Nature Switzerland, 2024.

[113] I. Bauer-Hänsel, Q. Liu, C. J. Tessone, and G. Schwabe, "Designing a blockchain-based data market and pricing data to optimize data trading and welfare," *International Journal of Electronic Commerce*, vol. 28, p. 3–30, Jan. 2024.

[114] D. A. Kountche, F. Raissi, M. R. Rakotondravelona, E. Bonetto, D. Brevi, A. Martin, O. Otaegui, and G. Velez, "Monetisation of and access to in-vehicle data and resources: the 5gmeta approach," 2022.

[115] C. F. Strnadl, "End-to-end architectures for data monetization in the industrial internet of things (iiot): Concepts and implementations," in *The Monetization of Technical Data*, p. 149–183, Springer Berlin Heidelberg, 2023.

[116] T. Himmelsbach, Y. Mou, S. Decker, and A. Heinzl, "Towards federated machine learning and distributed ledger technology-based data monetization.," in *VLDB Workshops*, 2023.

[117] Q. Han, C. Lucas, E. Aguiar, P. Macedo, and Z. Wu, "Towards privacy-preserving digital marketing: an integrated framework for user modeling using deep learning on a data monetization platform," *Electronic Commerce Research*, vol. 23, p. 1701–1730, June 2023.

[118] R. Garratt and M. J. Lee, "Monetizing privacy," Staff Reports 958, New York, NY, 2021.

[119] B. A. Manko, "Erie insurance: Monitoring technology in the car insurance market and the issue of data privacy," *Journal of Information Technology Teaching Cases*, vol. 13, no. 2, p. 193–198, 2023.

[120] S. G. Yoo and B. Ahn, "A study for efficiency improvement of used car trading based on a public blockchain," *The Journal of Supercomputing*, vol. 77, p. 10621–10635, Mar. 2021.

[121] C. C. Htet and M. Htet, "A secure used car trading system based on blockchain technology," in *Proceedings of the 21st International Conference on Information Integration and Web-based Applications amp; Services*, iiWAS2019, p. 654–658, ACM, Dec. 2019.

[122] F. Sterk, S. Frank, I. Lauster, and C. Weinhardt, "Utilizing fleet data: Towards designing a connected fleet management system for the effective use of multi-brand car data," in *Proceedings of the 56th Hawaii International Conference on System Sciences*, HICSS, pp. 1489–1498, Hawaii International Conference on System Sciences, 2023.

[123] C. Bloom, J. Tan, J. Ramjohn, and L. Bauer, "Self-driving cars and data collection: privacy perceptions of networked autonomous vehicles," in *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, SOUPS '17, (USA), p. 357–375, USENIX Association, 2017.

[124] S. Xia, F. Lin, Z. Chen, C. Tang, Y. Ma, and X. Yu, "A bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, p. 6856–6868, July 2020.

[125] M. Kim, J. Lee, J. Oh, K. Park, Y. Park, and K. Park, "Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers," *Applied Energy*, vol. 322, p. 119445, Sept. 2022.

[126] S. Aggarwal and N. Kumar, "A consortium blockchain-based energy trading for demand response management in vehicle-to-grid," *IEEE Transactions on Vehicular Technology*, vol. 70, p. 9480–9494, Sept. 2021.

[127] M. Baza, A. Sherif, M. M. E. A. Mahmoud, S. Bakiras, W. Alasmary, M. Abdallah, and X. Lin, "Privacy-preserving blockchain-based energy trading schemes for electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, p. 9369–9384, Sept. 2021.

[128] S. Rachamalla and H. Hexmoor, "Improving road safety by blockchain-based monetization of driver behavior.," *International Journal for Computers & Their Applications*, vol. 29, no. 3, 2022.

[129] Y. Zhao, N. Guo, Y. Wu, Y. Tian, and Y. Su, "Leveraging electric power data for enhanced credit assessment and risk control: A framework for data monetization and innovation," in *2024 IEEE 11th International Conference on Cyber Security and Cloud Computing (CSCloud)*, p. 153–158, IEEE, June 2024.

[130] M. Madine, K. Salah, R. Jayaraman, A. Battah, H. Hasan, and I. Yaqoob, "Blockchain and nfts for time-bound access and monetization of private data," *IEEE Access*, vol. 10, p. 94186–94202, 2022.

[131] Q. Song, J. Cao, K. Sun, Q. Li, and K. Xu, "Try before you buy: Privacy-preserving data evaluation on cloud-based machine learning data marketplace," in *Annual Computer Security Applications Conference*, ACSAC '21, p. 260–272, ACM, Dec. 2021.

[132] J. Bondia-Barcelo, J. Castella-Roca, and A. Viejo, "Building privacy-preserving search engine query logs for data monetization," in *2016 Intl IEEE Conferences on Ubiquitous Intelligence amp; Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, p. 390–397, IEEE, July 2016.

[133] W. Badreddine, K. Zhang, and C. Talhi, "Monetization using blockchains for iot data marketplace," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, p. 1–9, IEEE, May 2020.

[134] Z. Guan, X. Shao, and Z. Wan, "Secure fair and efficient data trading without third party using blockchain," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, July 2018.

[135] B. H. Wixom, C. M. Beath, and L. Owens, *2 Data Monetization Capabilities*, pp. 25–45. The MIT Press, Sept. 2023.

[136] M. Apruzzese, N. S. Hadjidimitriou, E. Pautasso, and M. Falbo, "Connecting data providers with data consumers: the 5gmeta data monetisation framework," in *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, p. 1896–1901, IEEE, June 2023.

[137] R. Song, B. Xiao, Y. Song, S. Guo, and Y. Yang, "A survey of blockchain-based schemes for data sharing and exchange," *IEEE Transactions on Big Data*, vol. 9, p. 1477–1495, Dec. 2023.

[138] R. Kilani, A. Zouinkhi, and M. N. Abdelkrim, "Monetization of industrial iot services using blockchain and smart contract," in *2023 IEEE International Workshop on Mechatronic Systems Supervision (IW_MSS), p. 1˜6, $IEEE$, Nov.2023.*

[139] H. Qabbaah, G. Sammour, and K. Vanhoof, "Using k-means clustering and data visualization for monetizing logistics data," in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, p. 1–6, IEEE, Oct. 2019.

[140] D. S. M. P. Monteiro, S. R. L. Meira, and F. S. Ferraz, "Big data monetization: Platforms and business models," in *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, p. 1–4, IEEE, June 2021.

[141] F. Firouzi, B. Farahani, M. Barzegari, and M. Daneshmand, "Ai-driven data monetization: The other face of data in iot-based smart and connected health," *IEEE Internet of Things Journal*, vol. 9, p. 5581–5599, Apr. 2022.

[142] World Wide Web Consortium (W3C), "Automotive working group," 2024. Working Group was closed on 22 February 2024.

[143] Information Commissioner's Office, "Accountability framework," 2023. Accessed on February 24, 2025.