HILL PUBLISHING

Engineering Advances, 2025, 5(4), 160-165
https://www.hillpublisher.com/journals/ea/
ISSN Online: 2768-7961

Exploration of the Application of the LINDDUN Model in Privacy Protection for Electric Vehicle Users

Mingjie Chen

Software and Societal Systems Department, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA.

How to cite this paper: Mingjie Chen. (2025) Exploration of the Application of the LINDDUN Model in Privacy Protection for Electric Vehicle Users. *Engineering Advances*, 5(4), 160-165.
DOI: 10.26855/ea.2025.10.006

Received: August 28, 2025
Accepted: September 25, 2025
Published: October 23, 2025

***Corresponding author:** Mingjie Chen, Software and Societal Systems Department, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA.

Abstract

Electric vehicles generate a vast amount of sensitive data involving travel, identity, and location during operation, which makes the risk of privacy leakage increasingly prominent. This paper introduces the LINDDUN model to analyze threats from three dimensions: data collection and transmission, identity and location privacy, and third-party service interfaces, thereby revealing key risk points. On this basis, it proposes application strategies such as optimization of technical systems and enhancement of protective capacity, establishment of compliance governance and institutional frameworks, user empowerment, cultivation of privacy awareness, and promotion of industry collaboration and standardization. The findings indicate that the LINDDUN model provides a systematic methodology for privacy protection in the electric vehicle sector, offering valuable reference for policymaking and industry regulation improvement.

Keywords

Electric Vehicles; Privacy Protection; LINDDUN Model; User Data

With the widespread adoption of electric vehicles, the volume of data related to personal travel, identity, and user behavior generated during operation has increased rapidly, posing unprecedented challenges to user privacy. Privacy breaches may not only harm individual rights but also weaken social trust and compromise public safety. Effective privacy protection is therefore vital to safeguarding user rights, enhancing regulatory standards across the industry, and promoting the sustainable development of intelligent transportation. Meanwhile, a systematic analysis of privacy risks helps clarify potential threat sources and protection priorities, providing scientific support for policymaking, technical optimization, and management practices. Such efforts can ultimately promote a balanced approach to data utilization and user privacy protection.

1. LINDDUN Model and Privacy Characteristics of Electric Vehicle Users

As an essential component of modern transportation, electric vehicles generate and rely on a wide range of data types, including vehicle status, travel trajectories, user identity, and information from in-car entertainment and communication systems. The collection and use of such data are highly real-time and continuous, creating a complex threat environment for user privacy. Data flows among onboard systems, cloud platforms, and third-party services improve service efficiency but simultaneously increase the potential for leakage. The characteristics of user privacy are multidimensional and dynamic, encompassing not only directly identifiable personal information but also indirectly inferred privacy content derived from behavior patterns and location trajectories.

The LINDDUN model provides a structured framework for privacy threat analysis, capable of identifying and evaluating risks from multiple perspectives. Its threat categories include linkability, identifiability, non-repudiation, data disclosure, unauthorized access, and misuse, which collectively offer a systematic methodology for analyzing the privacy characteristics of electric vehicle data ecosystems. In practice, the LINDDUN model facilitates a comprehensive understanding of the complexity of user privacy, highlights the information most vulnerable to threats, and offers theoretical support for the design of protective measures, thereby striking a balance between data utilization and privacy assurance.

2. Privacy Threats to Electric Vehicle Users Based on the LINDDUN Model

2.1 Privacy Risks in Data Collection and Transmission

During operation, electric vehicles continuously collect multidimensional data such as speed, location, status, and user behavior, which are then transmitted via onboard terminals to cloud platforms and service systems. The frequent data flows within these processes heighten the possibility of unauthorized access or interception, exposing travel trajectories (see Fig. 1), vehicle conditions, and personal behavior to potential leakage. When protection measures in data transmission and storage are inadequate, the risks are especially severe, particularly in public networks or open-interface environments where sensitive information is prone to third-party misuse. Such vulnerabilities not only endanger user privacy but also undermine system security over the long term. Without effective technical and managerial safeguards, these risks may escalate into irreparable security hazards.

Figure 1. Travel Trajectories of Electric Vehicle Users.

2.2 Risks of Identity and Location Privacy Leakage

User identity and location data are frequently recorded and analyzed over long-term vehicle use. Through data aggregation and behavioral pattern mining, user identities may be recognized or correlated. Continuous trajectory tracking enables external parties to infer personal travel habits, frequented locations, and life patterns, creating significant risks of identity and location disclosure. Such risks extend beyond individual privacy concerns, potentially leading to broader security issues such as behavioral prediction, location tracking, and targeted harassment by malicious actors. Once these data are cross-referenced with other sources, the consequences of disclosure may be magnified, exposing users to increasingly complex threat environments.

2.3 Privacy Threats from Third-Party Services and Platform Interfaces

The electric vehicle ecosystem involves numerous third-party services and platform interfaces. During data invocation, processing, and storage, issues such as abuse of permissions, weak governance, or security loopholes may expose user information to additional risks. Although openness and multi-party collaboration enhance functionality and convenience, they simultaneously heighten the likelihood of data leakage and misuse. The interplay of multiple actors and processes produces privacy threats that are increasingly complex and layered, demanding stronger protective measures [1]. Without unified supervision and coordination, these risks may become unmanageable. Particularly in cross-platform collaborations, a single vulnerability can trigger chain reactions, resulting in large-scale privacy breaches.

3. Application Strategies for Protecting Electric Vehicle User Privacy

3.1 Strengthening Technical Systems and Protective Capacity

During the operation of electric vehicles, a continuous stream of multi-source data related to identity, travel, and user behavior is generated. If this information flow lacks effective safeguards, it can easily become a breakthrough point for privacy risks. Building a comprehensive technical framework requires multi-level, end-to-end security protection. End-to-end encryption can prevent data from being intercepted during transmission, while anonymization and de-identification technologies can, to some extent, reduce the likelihood of reverse identification. At the same time, dynamic access control and multi-factor authentication ensure that the use of sensitive information remains strictly confined. Technical protection is not merely a static barrier but should also feature real-time monitoring and rapid response capabilities, allowing privacy threats to be detected and addressed as early as possible [2]. With the advancement of intelligent technologies, proactive defense and adaptive learning mechanisms are increasingly being incorporated into privacy protection systems. By continuously optimizing algorithmic models and security protocols, these systems are able to maintain flexibility and foresight when facing emerging and unknown threats [3].

Some electric vehicle companies have begun exploring technical defense mechanisms. For example, distributed encryption schemes have been deployed in interactions between onboard terminals and cloud platforms, ensuring that breaching a single node does not compromise the entire system. Certain back-end systems automatically detect abnormal login behavior, such as one account logging in from multiple regions within a short timeframe, triggering temporary freezes and manual verification. Additionally, privacy modules embedded in smart charging stations locally encrypt user identity data before matching with cloud platforms using anonymized identifiers. These practices enhance technical defenses and provide industry-level examples worth referencing.

Table 1. LINDDUN Threat Modeling

Element	L (Linkability)	I (Identifiability)	N (Non-repudiation)	D (Detectability)	D (Disclosure)	U (Unawareness)	N (Non-compliance)
Entity: User	X	X				X	
Data Store: Encrypted Storage				X	X		
Data Flow: User ↔ Vehicle Terminal	X		X				
Data Flow: Terminal ↔ Cloud		X			X		
Process: Cloud Authentication Module	X	X		X			
Process: Local Charging Module				X			X

The LINDDUN threat modeling in Table 1 highlights core vulnerabilities in technical protection—especially linkability, identifiability, and unawareness. The analysis shows that even strong encryption cannot fully eliminate traceability or data disclosure when terminal－cloud isolation is weak. Discussions around these issues are valuable for security designers. When Privacy-Enhancing Technologies (PETs), such as homomorphic encryption or differential privacy, are applied, mitigation improves notably. Yet, certain on-board anonymization areas remain underdeveloped, so progress depends on advances in state-of-the-art PETs. In practice, companies may replace theoretical controls with practical APIs or governance tools for better operational adaptability.

3.2 Compliance Governance and Institutional Frameworks

Privacy protection, as a long-term and systematic task, cannot be fully addressed by technology alone. Compliance governance, through the integration of laws, industry standards, and corporate policies, provides a sustainable guarantee for safeguarding user privacy. A comprehensive governance framework should encompass legitimacy reviews prior to data collection, minimization principles during data use, security measures throughout data storage, and compliance control in the process of data sharing. Clear responsibilities and institutional constraints can effectively prevent excessive collection and misuse of data. At the same time, compliance governance needs to be supplemented by supervisory mechanisms and accountability channels, ensuring that violations are corrected and sanctioned in a timely manner so that the system truly fulfills both its regulatory and incentive functions [4]. Moreover, regular evaluations of implementation are essential to ensure that governance does not become a formality but instead dynamically adapts to emerging technologies and evolving business practices.

Now, some enterprises have introduced internal compliance review processes. Before new functions are launched, data protection teams assess the scope of involved data to verify compliance with legality, necessity, and appropriateness principles. For third-party collaborations, agreements clearly define partners' responsibilities for data storage and use, while also mandating periodic compliance audits. Some companies have even established dedicated privacy governance committees to coordinate across departments and evaluate risks, ensuring that R&D, operations, and marketing follow unified standards in handling user data. Such initiatives signify a transition from reactive compliance to proactive governance.

Table 2. The LINDDUN analysis

Component	L	I	N	D	D	U	N
Entity: Compliance Officer	X	X			X		
Data Store: Compliance Audit Database	X	X	X	X			
Data Flow: Department ↔ Compliance Review Committee		X	X	X		X	
Process: Legitimacy Assessment	X	X		X	X		
Process: Third-party Contract Evaluation		X		X		X	
Process: Periodic Review and Feedback	X		X		X		X

The LINDDUN analysis in Table 2 reveals that compliance governance addresses multiple privacy threats, especially identifiability, detectability, and non-compliance. These findings show that institutional mechanisms—like legitimacy assessments and contract reviews—can reduce governance-related privacy risks. Discussions on these points guide compliance teams in replacing technical fixes with policy measures. Though PETs such as provenance tracking can enhance audits, their maturity still lags behind regulation. Thus, many enterprises rely on standardized reviews and manual documentation until regulatory technologies become more practical and automated.

3.3 User Empowerment and Privacy Awareness Cultivation

Users' roles in privacy protection are not merely passive recipients but should be regarded as active participants in data management. In theory, granting users the rights to be informed, to choose, and to delete can provide them with greater autonomy in the collection and use of personal data [5]. Well-designed privacy control tools should embody usability and transparency in both interface and functionality, allowing users to determine the extent of data disclosure without imposing excessive operational burdens. At the same time, cultivating privacy awareness is an indispensable part of the process. Continuous publicity and educational activities can help users recognize the potential risks of data misuse, thereby fostering proactive protective habits in daily use and gradually nurturing long-term attention to privacy management[6].With the overall advancement of digitalization, the supervisory and feedback roles that users play in privacy protection will become increasingly significant, not only driving enterprises to improve their mechanisms but also promoting the formation of a healthier governance environment across the industry.

Also, some carmakers have introduced measures to empower users. In-car systems and mobile applications allow users to opt in or out of location-sharing services or disable background uploads of driving habit data. Data access logs display recent instances of information use, enabling users to monitor and revoke permissions when necessary. If users lose trust in certain functions, authorization can be instantly disabled, halting related data collection. At the point of vehicle delivery, companies provide privacy education through videos and manuals, explaining risks and protection methods. These measures enhance user control and strengthen trust in the ecosystem.

Table 3. LINDDUN Threat Modeling Table (3)

Element	L	I	N	D	D	U	N
Entity: User						X	
Data Store: Cloud Log System		X		X			
Data Flow: User ↔ Settings Interface						X	
Data Flow: Interface ↔ Control Module				X			X
Process: Access Control Module	X	X			X		
Process: Log Audit System				X			X

Table 3's LINDDUN assessment shows that user empowerment mainly mitigates unawareness and disclosure threats. Discussion of these factors supports better usability and transparency in privacy tools. PETs like consent dashboards, minimization APIs, and preference automation help users maintain control. However, many user-side technologies remain fragmented or hard to use, so simplified interfaces and behavioral nudges serve as interim solutions. The goal is to develop adaptive, intuitive systems that empower users effectively and bridge the gap between awareness and real control.

3.4 Industry Collaboration and Standardization Promotion

The protection of privacy in the electric vehicle industry not only involves automakers, but also component suppliers, platform service providers, and relevant regulatory bodies. Without unified industry standards and collaborative mechanisms, security disparities among different entities can become new sources of privacy risks. The significance of industry collaboration lies in the joint development and enforcement of standards, thereby forming a collective force that spans enterprises and sectors [7]. Standardized regulations help reduce vulnerabilities caused by inconsistent interfaces and disjointed processes, while also enabling coordinated responses among different parties when risks arise. As the ecosystems of connected vehicles and smart mobility expand, the establishment of unified industry norms has become indispensable. At the same time, industry collaboration can improve resource utilization efficiency, lower compliance and protection costs for individual companies, and, in the long run, foster a trust-based security system that covers the entire industrial chain, laying a more solid foundation for the future of intelligent transportation [8].

Certain regional alliances have taken the lead in promoting standardization. For example, member enterprises have jointly formulated secure protocols for vehicle data interfaces and subjected participating companies to unified security testing, ensuring that cross-platform data flows do not generate extra risks. In addition, regional platforms have established joint emergency response mechanisms, enabling members to share defensive experiences and patch solutions rapidly during security incidents. These practices demonstrate that industry collaboration enhances collective protective capacity while subtly fostering user trust in the ecosystem.

Table 4. LINDDUN Threat Modeling Table (4)

Element	L	I	N	D	D	U	N
Entity: Enterprise A	X						
Data Store: Alliance Shared Database		X			X		
Data Flow: Enterprise A ↔ Platform			X				X
Data Flow: Platform ↔ Enterprise B	X						
Data Flow: Platform ↔ Regulator		X		X			
Process: Alliance Coordination							X

The LINDDUN results in Table 4 indicate that collaboration risks stem from linkability and unawareness across shared databases and interfaces. Open discussion of these issues helps identify where joint governance and common protocols are crucial. PETs such as federated learning, secure computation, and blockchain audits can mitigate risks, though many are still evolving. In the interim, alliances can implement partial controls through standardized APIs and transparency agreements. As cooperation matures, these practices will evolve into proactive, trust-based privacy management frameworks across the industry.

4. Conclusion

Privacy protection for electric vehicle users is vital to maintaining security and trust. Looking ahead, as technologies of intelligence and connectivity continue to evolve, data volumes and interaction complexities will further intensify, leading to increasingly diverse and dynamic privacy risks. This calls for ongoing improvements in technical defenses, governance systems, and user awareness to achieve multi-dimensional coordination among technology, institutions, and users. The industry should focus on emerging data types and application scenarios, advance standardization, and explore cross-platform data governance methods to ensure the long-term security and sustainable use of personal information within the electric vehicle ecosystem.

References

[1] Sion L, Landuyt VD, Wuyts K, et al. Robust and reusable LINDDUN privacy threat knowledge. Comput Secur. 2025;154:104419.

[2] Pöhls CH, Kügler F, Geloczi E, et al. Segmentation and Filtering Are Still the Gold Standard for Privacy in IoT—An In-Depth STRIDE and LINDDUN Analysis of Smart Homes. Future Internet. 2025;17(2):77.

[3] Farias DALCJ, Carniel A, Bezerra MDJ, et al. Approach based on STPA extended with STRIDE and LINDDUN, and blockchain to develop a mission-critical e-voting system. J Inf Secur Appl. 2024;81:103715.

[4] Li Z, Bian Z, Chen Z, et al. Synthesis of electric vehicle charging data: A real-world data-driven approach. Commun Transp Res. 2024;4:100128.

[5] Mookherji S, Odelu V, Prasath R. Secure ultra fast authentication protocol for electric vehicle charging. Comput Electr Eng. 2024;119(P A):109512.

[6] Sahu LB, Chandrakar P. Enhanced Privacy Preservation and Data Storage in Blockchain-Based Electric Vehicle Network. Procedia Comput Sci. 2024;235:2144-53.

[7] Ali AW, Fanti PM, Roccotelli M, et al. A Review of Digital Twin Technology for Electric and Autonomous Vehicles. Appl Sci. 2023;13(10).

[8] Andreas U, Fabian K, Dominik E, et al. An analysis of privacy preservation in electric vehicle charging. Energy Inform. 2022;5(1).