UDC 004.056.5:004.738.5

D.V. Melnyk
O.N. Romanyuk

ENSURING PERSONAL DATA SECURITY OF USERS IN CARPOOLING AND RIDE-SHARING SERVICES

Vinnytsia National Technical University

Анотація

У тезах розглядаються ключові загрози безпеці персональних даних у сервісах пошуку попутників та організації спільних подорожей. Проаналізовано основні вразливості таких систем, правові основи захисту даних, а також технічні та організаційні заходи забезпечення конфіденційності. Запропоновано комплексний підхід до проектування безпечних архітектур мобільних та веб-додатків для карпулінгу.

Ключові слова: персональні дані, захист інформації, карпулінг, автентифікація, шифрування, GDPR, кібербезпека, мобільний додаток.

Abstract

The paper addresses key threats to personal data security in carpooling and ride-sharing services. The main vulnerabilities of such systems are analyzed, along with the legal framework for data protection and technical and organizational privacy measures. A comprehensive approach to designing secure architectures for carpooling mobile and web applications is proposed.

Keywords: personal data, information security, carpooling, authentication, encryption, GDPR, cybersecurity, mobile application.

Introduction

The rapid growth of digital platforms for shared mobility and carpooling services has introduced significant challenges related to the protection of users' personal data. Applications such as BlaBlaCar, Uber, and similar services collect extensive sensitive information including real names, phone numbers, geolocation data, payment details, and travel history [1]. As the user base of such services expands, the risk of unauthorized access, data breaches, and misuse of personal information increases proportionally. Ensuring robust data security is therefore not only a technical necessity but also a legal and ethical obligation for service providers.

The urgency of this topic is underscored by the increasing number of high-profile data breaches affecting transportation platforms. In 2022, Uber suffered a major security incident exposing internal systems and user records [2]. Such incidents highlight the need for a systematic approach to data protection from the early stages of software development.

Threat Landscape in Carpooling Applications

Personal data in ride-sharing services is exposed to a broad range of threats. At the network level, insufficiently protected API endpoints may allow attackers to intercept or manipulate data transmissions. Man-in-the-middle (MITM) attacks remain a relevant threat when applications fail to implement proper TLS certificate pinning [3]. At the application level, vulnerabilities such as insecure direct object references (IDOR) and broken access control can expose user profiles, trip history, and contact information to unauthorized parties.

Social engineering poses an additional risk specific to carpooling platforms. Since the core functionality involves connecting strangers, malicious actors may exploit the platform to harvest personal information or conduct targeted phishing attacks. The aggregation of location data over time can reveal sensitive behavioral patterns, including home and work addresses, daily routines, and frequent contacts [4].

Legal Framework and Compliance Requirements

The legal basis for personal data protection in ride-sharing services is primarily defined by the General Data Protection Regulation (GDPR) in the European Union and the Law of Ukraine "On Personal Data Protection" [5]. These regulations impose strict requirements on data minimization, purpose limitation, consent management, and the right to erasure. Service providers are obligated to conduct Data Protection Impact

Assessments (DPIA) for high-risk processing activities, which inherently include real-time location tracking [6].

Non-compliance carries severe financial consequences: under GDPR, fines can reach up to 4% of global annual turnover or €20 million, whichever is greater. Beyond financial risk, data breaches can cause irreparable reputational damage and erode user trust, which is particularly damaging in a market segment where safety perception is paramount.

Technical and Organizational Security Measures

A comprehensive data security strategy for carpooling applications must encompass multiple layers of protection. At the infrastructure level, end-to-end encryption (E2EE) should be applied to all sensitive communications, and data at rest should be encrypted using AES-256 or equivalent standards [3]. Database access should follow the principle of least privilege, and all sensitive fields (e.g., phone numbers, payment data) should be stored in hashed or encrypted form.

Authentication mechanisms play a critical role in securing user accounts. Multi-factor authentication (MFA) significantly reduces the risk of account takeover. OAuth 2.0 with PKCE (Proof Key for Code Exchange) is the recommended authorization framework for mobile applications [7]. Session tokens must be short-lived and securely stored using platform-native secure storage (Keychain on iOS, Keystore on Android).

Geolocation data requires particular attention due to its sensitivity. Applications should implement location data anonymization, storing only aggregated or coarse-grained location information after trip completion. The collection of background location data should require explicit user consent and be disabled by default. Privacy-by-design principles, as advocated in ISO/IEC 27701:2019, should guide all architectural decisions from the earliest development stage [6].

Organizational measures are equally important. Regular security audits, penetration testing, and developer training in secure coding practices (e.g., OWASP Mobile Top 10) help maintain a strong security posture. A documented incident response plan ensures timely notification of affected users and regulatory authorities in the event of a breach [1].

Conclusions

Personal data security in carpooling and ride-sharing services is a multifaceted challenge that demands a holistic approach combining technical controls, legal compliance, and organizational practices. The sensitive nature of the data processed – including real-time geolocation, identity, and payment information – makes these platforms high-priority targets for attackers. Developers must adopt a privacy-by-design methodology, integrating security measures throughout the software development lifecycle rather than treating them as an afterthought. Adherence to GDPR requirements and international security standards provides a solid foundation for building trustworthy and compliant carpooling solutions.

REFERENCES

1. Acquisti A., Brandimarte L., Loewenstein G. Privacy and human behavior in the age of information. Science. 2015. Vol. 347, No. 6221. P. 509–514.
2. Greenberg A. Uber Was Hacked Again, Exposing the Personal Data of 57 Million Riders and Drivers. Wired. 2022. URL: https://www.wired.com/story/uber-hack-2022 (Accessed: May 25, 2026).
3. OWASP Mobile Security Project. OWASP Mobile Top 10. 2024. URL: https://owasp.org/www-project-mobile-top-10 (Accessed: May 25, 2026).
4. Montjoye Y.-A. de, Hidalgo C. A., Verleysen M., Blondel V. D. Unique in the crowd: The privacy bounds of human mobility. Scientific Reports. 2013. Vol. 3. Art. 1376.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union. 2016. L 119. P. 1–88.
6. ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Geneva: ISO, 2019. 73 p.
7. Hardt D. The OAuth 2.0 Authorization Framework. RFC 6749. IETF. 2012. URL: https://datatracker.ietf.org/doc/html/rfc6749 (Accessed: May 25, 2026).

Мельник Дмитро Валерійович – студент групи 1ПІ-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e–mail: dmitromelnik304@gmail.com.

Романюк Олександр Никифорович – доктор технічних наук, професор, професор кафедри програмного забезпечення, завідувач кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e–mail: rom8591@gmail.com.

Melnyk Dmytro V. – student of group 1PI-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dmitromelnik304@gmail.com.

Romanyuk Oleksandr N. – Doctor of Technical Sciences, Professor, Professor of the Software Engineering Department, Head of the Software Engineering Department, Vinnytsia National Technical University, Vinnytsia, e–mail: rom8591@gmail.com.