*International Research Journal of Innovations in Engineering and Technology (IRJIET)*

**ISSN (online): 2581-3048**
**Volume 8, Issue 4, pp 236-240, April-2024**
https://doi.org/10.47001/IRJIET/2024.804034

# Safeguarding Passenger Data Privacy in Self-Navigating Vehicles

**[1]Awadh Sao, [2]Ashish Deharkar, [3]Pushpa Tandekar**

[1]Student, Department of CSE, Shri Sai College of Engineering and Technology, Chandrapur, Maharashtra, India
[2,3]Assistant Professor, Department of CSE, Shri Sai College of Engineering and Technology, Chandrapur, Maharashtra, India

***Abstract* - As the automotive industry undergoes a transformative shift towards autonomous vehicles (AVs), the integration of advanced self-driving technologies presents new opportunities and challenges. [1] AVs, defined as systems capable of dynamic driving tasks with limited human intervention, are poised to revolutionize transportation. With governments, private firms, and research centers investing heavily in AV development, the realization of fully autonomous vehicles in everyday life appears imminent. The advent of self-driving cars brings forth novel prospects for passenger-centric services, including sophisticated information systems facilitating Passenger-AV interaction. [2] This interaction empowers passengers to supervise vehicle behavior, control destinations, and engage in high-level dialogue with AVs. However, as AV information systems collect and process sensitive passenger data, ensuring data privacy and security becomes paramount. To instill trust in self-driving technology and safeguard passenger privacy, stringent privacy and security measures must be implemented. Adhering to legislative mandates and organizational responsibilities is crucial to mitigate risks associated with data misuse and system compromise. [4, 5] Moreover, as AVs transition from Human-Computer Interaction (HCI) to Human-Robot Interaction (HRI), it is imperative to reassess information systems security risk management (ISSRM) procedures in the context of Passenger-AV interaction. This research focuses on investigating the applicability of ISSRM methods in HCI to ensure data privacy and security in Human-AV interaction scenarios, particularly Passenger-AV interaction. By scrutinizing the processing of sensitive personal data within AV information systems, the study aims to address emerging privacy and security challenges. [6] Emphasizing the legal imperative for information security and data privacy, this endeavor seeks to establish robust frameworks for protecting passenger data in the era of autonomous vehicles.**

***Keywords:*** Risk Management, Data Protection, GDPR Compliance, Ride Fulfillment, Autonomous Vehicle, Threat Identification, Tool-supported Analysis.

## I. INTRODUCTION

As autonomous driving technology advances, concerns about information security and data protection in autonomous vehicles (AVs) have emerged. Security researchers have demonstrated vulnerabilities in AV systems through proof-of-concept attacks, highlighting the need for robust security measures. These attacks, which enable remote manipulation of AVs' infotainment systems and driving functions, underscore the inadequacy of current security protocols.

The repercussions of security breaches in AVs are significant, including vehicle damage, financial losses, and unauthorized disclosure of personal data. To address these risks, a systematic approach to data protection is essential. Segmenting AV functionality into distinct use cases and conducting individualized risk analyses can help identify vulnerabilities and threats. [7] This is particularly crucial for Passenger-AV interaction scenarios, where data sharing with external service providers and intelligent transportation system components occurs.

Despite the critical need for enhanced data protection measures, no standardized approach currently exists. This research aims to fill this gap by proposing a comprehensive framework for personal data protection in Passenger-AV interaction scenarios. [3] Drawing upon principles of privacy management and information security risk management, this framework seeks to establish guidelines for ensuring the confidentiality, integrity, and availability of passenger data within AVs. Through a thorough examination of legislative requirements and a threat-driven approach to security risk management, this investigation aims to lay the groundwork for effective data protection strategies in the realm of autonomous driving technology.

### 1.1 Research Questions

Protecting the information exchanged in Passenger-Autonomous Vehicle interaction is paramount, particularly safeguarding passenger's personal data. The privacy of this data is mandated by human rights, necessitating adherence to stringent rules on data processing. To address this, we

 

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 4, pp 236-240, April-2024

https://doi.org/10.47001/IRJIET/2024.804034

delineate two distinct approaches: information security and general privacy management.

**1. Information Security Risks Management (RQ1):** We propose an approach for identifying and mitigating information security risks. This involves identifying the assets at risk, assessing potential threats, and implementing countermeasures to mitigate risks effectively.

**2. Privacy Management (RQ2):** Building upon the framework established in RQ1, we outline strategies for lawfully collecting and processing passenger data. This includes leveraging compliance checks and data disclosure analysis to prevent data breaches. Additionally, we propose the adoption of privacy-enhancing technologies to enhance personal data protection.

Through this research, we aim to establish a systematic approach for ensuring personal data protection in the Passenger-AV interaction business process. By addressing both information security and privacy management concerns, we lay the groundwork for a secure and privacy-preserving interaction environment.

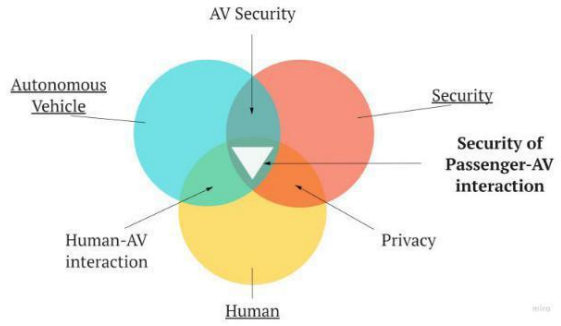


**Figure 1: Context of Passenger-AV interaction security**

### 1.2 Contribution

This work enhances understanding of autonomous vehicle systems management through the following outcomes:

**1. Threat Model for AV Systems:** We introduce a threat model facilitating a threat-driven approach, serving as a foundational tool for managing information security risks in Passenger-AV interaction. [9] Demonstrating its value, the model is utilized as a baseline for risk assessment and requirement elicitation, benefiting information security specialists and process owners in AV system development organizations.

**2. Tool-supported Privacy Analysis:** We demonstrate the efficacy of tool-supported privacy analysis in AV system management processes. Data protection officers can leverage these insights to understand the benefits of employing specialized tools for privacy analysis within their organizations.

**3. Security Measures for Data Protection:** We propose a set of security measures tailored for data protection in Passenger-AV interaction scenarios. AV system developers can utilize these security control mechanisms to meet security requirements during system design and development phases effectively.

## II. METHODOLOGY

SRQ1.1: Identifying Protected Assets: This inquiry aims to delineate the assets within the Passenger-AV interaction, essential for understanding the security criteria imperative for their safeguarding.

SRQ1.2: Unveiling Security Threats: Following the asset identification in SRQ1.1, this question delves into vulnerabilities and corresponding security threats. By pinpointing potential risks, we lay the groundwork for effective risk management.

SRQ1.3: Defining Security Requirements: Addressing security concerns identified in SRQ1.2, this query focuses on eliciting specific security requirements to mitigate risks within the Passenger-AV interaction.

The research methodology, depicted in Figure below, encompasses two concurrent processes: theoretical artifact development based on literature review and case analysis demonstrating practical application. This dual approach allows for comprehensive exploration of the under-researched realm of Passenger-AV interaction, providing valuable insights for theory and practice alike.

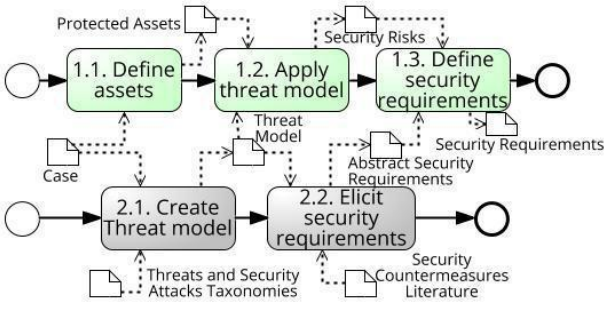


**Figure 2: Security risk management: research method**

The methodology for developing a threat model to assess security risks and requirements is outlined. Initially, Bolt's information system architecture is identified to encompass security threats, along with recognizing critical business assets for protection. [8] Subsequently, four leading threat taxonomies and libraries - STRIDE, CAPEC, ATT&CK, and OWASP Top Ten - are chosen to inform the creation of the

 

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 4, pp 236-240, April-2024

https://doi.org/10.47001/IRJIET/2024.804034

threat model. [10] Risks associated with the identified assets within the case's context are then identified, and potential mitigation measures are articulated as security requirements. Furthermore, preliminary validation results are presented, highlighting the need for further validation of the requirements elicitation approach. The subsequent chapter delves into the management of personal data within Bolt systems participating in the Ride Fulfillment process. Whereas this chapter addresses managing uncertainties impacting overall organizational security, the upcoming chapter focuses on the management of personal data collected by the organization.

**Table 1: Security countermeasures for IR5 mitigation**

| Security Requirement | Security Control Components |
|---|---|
| Ensure unauthorized connections are identified to the local area network by the In-Vehicle Controller | Implement an authenticated application layer proxy to monitor network traffic to and from the Internet. |
| Ensure confidentiality of transmitted information via Transmission Channel by the In-Vehicle Controller | Employ cryptographic mechanisms such as SSL/TLS protocol and IPSec protocol suite, along with Advanced Encryption Standard (AES) for encrypting wireless data in transit. |
| Control physical access to transmission channel within organizational facilities by the service provider owning the vehicles | Implement wiretapping sensors, maintain locked wiring closets, and protect cabling with conduit or cable trays. |
| Authenticate mobile devices before establishing connection by the In-Vehicle Controller | Employ bidirectional cryptographically based authentication. |
| Follow wireless capabilities policies by the Service Provider System | Utilize wireless networking capabilities solely for essential functions. |

## III. THREAT MODEL

To construct a comprehensive threat model, we thoroughly analyze the scenario outlined. Our approach involves several key steps. Initially, we employ the STRIDE methodology to brainstorm potential attack vectors, focusing on understanding the intricacies of the AV system architecture and the Ride Fulfillment process. Following this, we delve into the OWASP Top Ten list to identify vulnerabilities within the web application component of the AV system. Subsequently, we explore concrete attack scenarios using both the CAPEC and ATT&CK taxonomies, meticulously selecting attacks based on factors such as the requisite skills and targeted vulnerabilities. [4] This iterative process allows us to form a robust threats model tailored specifically to the nuances of Passenger-AV interaction, addressing potential risks across various components of the system.

The resulting threat model, comprising 17 distinct threats, is systematically categorized into six groups derived from the STRIDE approach. [5] Each threat is thoroughly analyzed and referenced for further examination. A detailed breakdown of the identified threats, including their targeted vulnerabilities, potential impact, and attack methods, is provided for comprehensive understanding and analysis.

These threats encompass a wide range of potential risks, including identity spoofing, data tampering, manipulation of API parameters, repudiation attacks, information disclosure, denial of service, and elevation of privileges. By addressing these threats, we aim to safeguard the authentication, integrity, confidentiality, and availability of data within the Passenger-AV interaction, ensuring the overall security and reliability of the system.

## IV. ANSWER TO RESEARCH QUESTIONS

The research investigates strategies for safeguarding information exchanged in Passenger-AV interaction, approaching the main research goal from two distinct angles.

RQ1: Addressing information security risks in Passenger-AV interaction involves applying security risk management. Through this process, assets susceptible to threats are identified, including both business and system components.

Notably, 22 security risks are delineated, primarily targeting assets containing passenger location and ride details. Proposed security requirements aim to mitigate these risks, serving as foundational measures to bolster information security in the Bolt AV system and potentially in similar ride-hailing systems.

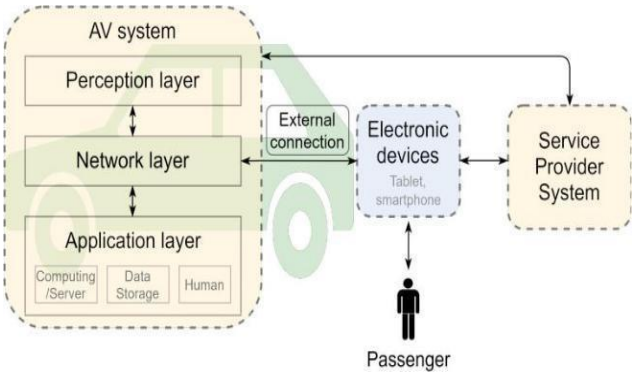


**Figure 3: The autonomous vehicle system model**

RQ2: Ensuring passenger personal data privacy necessitates compliance with local data protection legislation, such as the GDPR in EU countries where Bolt operates. [2] Business processes must align with GDPR requirements, with tools like the DPO tool aiding in identifying non-compliance issues. Privacy by design principles and privacy-enhancing technologies (PETs) are essential, with PET selection facilitated by tool-supported disclosure analysis. Proposed process designs ensure GDPR compliance and pinpoint potential data leakages, emphasizing the importance of employing PETs and specialized business process analysis tools in the Passenger-AV interaction.

 

ISSN (online): 2581-3048
Volume 8, Issue 4, pp 236-240, April-2024
https://doi.org/10.47001/IRJIET/2024.804034

## V. RESULTS AND FUTURE WORK

To address the primary goal of the case analysis, we conducted a literature review to identify methodologies for information risk analysis in Passenger-AV interaction. We identified a gap in methods for ensuring personal data protection in autonomous vehicles, highlighting two distinct approaches: privacy protection and information security, with the latter being a prerequisite for the former. Applying a threat-driven approach, we elicited security requirements for Passenger-AV interaction, leveraging a created threat model. It's noteworthy that the threat model encompasses threats relevant to ride-hailing service contexts, where external providers deliver infotainment systems. For broader application, attention to system architecture is crucial as threats may manifest differently based on technology stacks. Moreover, compliance with local legislation and adoption of privacy-enhancing technologies are vital considerations. [7] Employing security and privacy by design approaches is imperative, especially given legislative requirements like GDPR. Additionally, case studies are valuable for gaining insights into current theories and motivating further research in information security management. While this research focuses on Passenger-AV interaction at the application layer, similar research across all AV processes is essential for comprehensive data protection in autonomous vehicles.

## VI. CONCLUSION

The present research stems from research conducted within the autonomous driving lab, aiming to discern strategies for safeguarding information exchanged in Passenger-Autonomous Vehicle interactions. Our focus lies in ensuring data protection through two distinct lenses - information privacy and security risk management. Employing a threat-driven approach, we delve into security risk management to elicit requisite security measures. Consequently, a set of security requirements is identified, along with recommendations for validation and prioritization before integration into systems. Given the involvement of personal passenger data in the Ride Fulfilment process, we explore specific measures for preserving personal data privacy. Furthermore, we undertake a tool-supported analysis of personal data management within business processes, culminating in proposed designs for leveraging privacy-enhancing technologies in the investigated scenario.

## REFERENCES

[1] OneTrustDataGuidance, "Comparing privacy laws: GDPR/CCPA." https://www.dataguidance.com/sites/default/files/ccpa_v_gdpr_latest_edition.pdf, December 2019.

[2] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." http://data.europa.eu/eli/reg/2016/679/2016-05-04, 2016.

[3] "Driverless public bus route now open in Tallinn." https://e-estonia.com/driverless-public-bus-tallinn/.

[4] F. Jahan, W. Sun, Q. Niyaz, and M. Alam, "Security modeling of autonomous systems: A survey," ACM Comput. Surv., vol. 52, Sept. 2019.

[5] European Union Agency for Cybersecurity, "ENISA good practices for security of Smart Cars." https://www.enisa.europa.eu/publications/smart-cars, November 2019.

[6] "Personal Data Protection Act 2012 (No. 26 of 2012)." https://sso.agc.gov.sg/Act/

[7] European Union Agency for Cybersecurity, "ENISA: Guidelines for SMEs on the security of personal data processing." https://op.europa.eu/s/ou6H, January 2017. Last accessed 4-Dec-2020.

[8] The MITRE Corporation, "Common Weakness Enumeration (CWE)."https://cwe.mitre.org/.

[9] P. Pullonen, J. Tom, R. Matulevicius, and A. Toots, "Privacy-enhanced BPMN: enabling data privacy analysis in business processes models," Software and Systems Modeling, vol. 18, pp. 3235–3264, Dec 2019.

[10] "ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements." https://www.iso.org/standard/54534.html.

[11] Lowlesh Yadav and Asha Ambhaikar, "IOHT based Tele-Healthcare Support System for Feasibility and perfor-mance analysis," Journal of Electrical Systems, vol. 20, no. 3s, pp. 844–850, Apr. 2024, doi: 10.52783/jes.1382.

[12] L. Yadav and A. Ambhaikar, "Feasibility and Deployment Challenges of Data Analysis in Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489389.

[13] L. Yadav and A. Ambhaikar, "Approach Towards Development of Portable Multi-Model Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489468.

[14] Lowlesh Yadav and Asha Ambhaikar, Exploring Portable Multi-Modal Telehealth Solutions: A

 

ISSN (online): 2581-3048
Volume 8, Issue 4, pp 236-240, April-2024
https://doi.org/10.47001/IRJIET/2024.804034

Development Approach. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 10, pp. 873–879, Mar. 2024.11(10), 873–879, DOI: 10.13140/RG.2.2.15400.99846.

[15] Lowlesh Yadav, Predictive Acknowledgement using TRE System to reduce cost and Bandwidth, March 2019. International Journal of Research in Electronics and Computer Engineering (IJRECE), VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).

## AUTHORS BIOGRAPHY

**Awadh Sao** is a final year student at SSCET, Bhadrawati. He specializes in Computer Science and Engineering and leading research on passenger data privacy in self-navigating vehicles, Awadh Sao has advanced understanding in this critical area. Integrating previous work with original methodologies, they've developed a robust model ensuring passenger privacy, enhancing safety in self-navigating vehicles.

**Prof. Ashish Deharkar** is an Assistant Professor of CSE at SSCET, Bhadrawati. Having completed his M. Tech in Computer Science and Engineering from Gondwana University in 2022, Prof. Ashish Deharkar brings a wealth of expertise to the team. His contributions to this research have been instrumental, enriching. The study with his unique perspective and experience.

**Prof. Pushpa Tandekar** is an Assistant Professor of CSE at SSCET, Bhadrawati, specializing in Computer Science and Engineering. Having completed their M. Tech from RGPV, Bhopal in 2014, they bring valuable expertise to the team. Their contributions to this research have been significant, providing valuable insights and expertise. Prof. Pushpa Tandekar adds depth to the study with their innovative approach and dedication.

**Citation of this Article:**

Awadh Sao, Ashish Deharkar, Pushpa Tandekar, "Safeguarding Passenger Data Privacy in Self-Navigating Vehicles", Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 4, pp 236-240, April 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.804034

*******

 