RADemics

IoT Powered Autonomous Vehicles and Connected Mobility Solutions for Sustainable and Smart Urban Transportation

Arun B Mathews, A.Prabhaharan, T.Kamalkumar
MTHSS P Venmony, RVS College Of Arts And Science,
T.J.S. Engineering College

IoT Powered Autonomous Vehicles and Connected Mobility Solutions for Sustainable and Smart Urban Transportation

[1]Arun B Mathews, HSST Sel Grade, Computer Science, MTHSS P Venmony. marthomat@gmail.com

[2]A. Prabhaharan M.Sc., M.Phil., (Ph. D)., Assistant Professor, Computer Science, RVS College Of Arts And Science, Sulur – 641402.Coimbatore (DT). prabhavsr@gmail.com

[3]T. Kamalkumar, Assistant Professor, EEE, T.J.S. Engineering College, TJS Nagar, Peruvoyal Near Kavaraipettai Gummidipoondi Taluk, Tiruvallur District 601206. prabhavsr@gmail.com

Abstract

The integration of Internet of Things (IoT) technologies within autonomous vehicles (AVs) is revolutionizing modern transportation by enabling intelligent, connected, and self-operating mobility systems. However, this digital interconnectivity significantly expands the attack surface, exposing vehicular networks to sophisticated cybersecurity threats that could compromise safety, data privacy, and operational integrity. This chapter presents a comprehensive examination of cybersecurity architectures tailored for IoT-enabled autonomous vehicles, with a focus on identifying prevalent attack vectors, including denial-of-service (DoS/DDoS), spoofing, and data injection threats. The discourse extends to secure microcontroller and SoC designs, cryptographic protocols, authentication mechanisms, and privacy-preserving techniques such as homomorphic encryption and secure multiparty computation. Additionally, the chapter explores the role of intrusion detection and prevention systems (IDPS) and collaborative threat intelligence frameworks in fortifying AV ecosystems. Emerging challenges in secure key management, system scalability, and real-time performance are critically analyzed. The chapter concludes with strategic future directions and architectural recommendations to foster resilient, privacy-aware, and sustainable AV cybersecurity infrastructures. This work contributes to advancing secure intelligent mobility within the broader paradigm of smart urban transportation.

Keywords: Autonomous Vehicles, IoT Security, Cybersecurity Architectures, Privacy Preservation, Intrusion Detection Systems, Connected Mobility.

Introduction

The emergence of autonomous vehicles (AVs) integrated with Internet of Things (IoT) technologies marks a transformative shift in the transportation domain, enabling real-time communication, predictive decision-making, and intelligent mobility [1]. The fusion of sensors, actuators, control systems, and cloud-based services has facilitated unprecedented levels of automation and interconnectivity [2]. These advancements are at the core of smart urban transportation systems, offering solutions for congestion, emissions reduction, and improved road

safety [3]. while the integration of IoT technologies facilitates enhanced functionality, it concurrently introduces complex cybersecurity challenges [4]. The dynamic nature of AV environments—where vehicles continuously interact with infrastructure, pedestrians, other vehicles, and cloud platforms—presents an ever-evolving threat landscape. This scenario necessitates the development of robust and adaptive cybersecurity architectures capable of addressing both conventional and emerging threats in real time. The need for intelligent protection mechanisms is magnified by the potential consequences of cyberattacks, which may compromise not only data integrity and vehicle control systems but also endanger public safety [5].

Autonomous vehicle ecosystems rely on various communication protocols, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Cloud (V2C) communications, collectively referred to as V2X [6]. These networks exchange high-frequency data that must remain untampered and confidential to ensure reliable operation [7]. The distributed and decentralized nature of IoT components embedded within AVs makes them susceptible to a wide spectrum of cyberattacks such as eavesdropping, data manipulation, spoofing, and denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks [8]. Such incidents could lead to catastrophic failures in real-world traffic scenarios, such as causing abrupt braking, misrouting, or collision events [9]. The increasing complexity of onboard systems, including sensors, artificial intelligence algorithms, and embedded microcontrollers, increases the difficulty of implementing uniform security standards across diverse platforms. Consequently, designing scalable, resilient, and interoperable cybersecurity frameworks becomes an essential aspect of AV development and deployment within smart city infrastructures [10].

The cybersecurity risks in AVs are further exacerbated by their reliance on external computing resources and third-party service providers [11]. The adoption of edge and cloud computing in vehicular systems improves computational efficiency but simultaneously creates vulnerabilities through open APIs, unsecured data links, and potential misconfigurations [12]. Adversaries may exploit these interfaces to launch targeted attacks that compromise data confidentiality or inject malicious code into control systems [13]. As AVs become increasingly software-defined, continuous updates and over-the-air (OTA) programming expose vehicles to new threat vectors that require secure update protocols and real-time anomaly detection [14]. These evolving attack surfaces underscore the urgency of implementing multilayered security models that span hardware, firmware, communication protocols, and application layers. A comprehensive understanding of these challenges forms the foundation for proposing integrated defense strategies that address security, privacy, and trust simultaneously [15].