City Research Online

City St George's, University of London

Citation: Bilal, A., Sharif, K., Li, F., Bukhari, S., Zhu, L., Xu, C. & Biswas, S. (2026). Impact of Intelligent Technologies on IoV Security: Integrating Edge Computing and AI. ACM Computing Surveys, 58(15), pp. 1-35. doi: 10.1145/3816144

This is the published version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/38053/

Link to published version: https://doi.org/10.1145/3816144

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

Impact of Intelligent Technologies on IoV Security: Integrating Edge Computing and AI

AWAIS BILAL, School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China
KASHIF SHARIF*, School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China
FAN LI, School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China
SADAF BUKHARI, School of Computer Science and Technology, Beijing Institute of Management, Beijing, China
LIEHUANG ZHU, School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, China
CHANG XU, School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, China
SUJIT BISWAS, Department of Computer Science, City St. George's, University of London, London, United Kingdom of Great Britain and Northern Ireland

The rapid development and integration of intelligent technologies in the Internet of Vehicles (IoV) have revolutionized transportation systems by enhancing connectivity, automation, and safety. However, the complexity and connectivity of IoV networks also introduce security challenges, including data privacy concerns, cyber threats, and system vulnerabilities. This paper surveys the role of Edge Computing (EC), Machine Learning (ML), and Deep Learning (DL) in strengthening IoV security frameworks. It examines the synergy between these technologies, highlighting their individual capabilities and their collective impact on enhancing threat detection, response times, and adaptive security. Through real world case studies and practical deployments, we demonstrate how EC, ML, and DL are currently improving security and operational efficiency in IoV systems. The paper also identifies key research gaps and future directions for further advancements in IoV security, including the need for scalable, privacy preserving solutions and robust defense mechanisms against emerging cyber threats. By integrating EC, ML, and DL, this work lays the groundwork for developing adaptive, efficient, and resilient IoV security infrastructures capable of addressing evolving challenges in the transportation ecosystem.

CCS Concepts: • **Security and privacy → Network security**; • **Networks** → *Network security*; • **Computing methodologies** → *Machine learning approaches.*

*Corresponsing Author.
This work was supported by Beijing Natural Science Foundation (IS23056).

Authors' Contact Information: Awais Bilal, School of Computer Science and Technology, Beijing Institute of Technology, Beijing, Beijing, China; e-mail: awaisbilal@bit.edu.cn; Kashif Sharif, School of Computer Science and Technology, Beijing Institute of Technology, Beijing, Beijing, China; e-mail: kashif.sharif@ieee.org; Fan Li, School of Computer Science and Technology, Beijing Institute of Technology, Beijing, Beijing, China; e-mail: fli@bit.edu.cn; Sadaf Bukhari, School of Computer Science and Technology, Beijing Institute of Management, Beijing, Beijing, China; e-mail: sadaf@bit.edu.cn; Liehuang Zhu, School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, Beijing, China; e-mail: liehuangz@bit.edu.cn; Chang Xu, School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, Beijing, China; e-mail: xchang@bit.edu.cn; Sujit Biswas, Department of Computer Science, City St. George's, University of London, London, England, United Kingdom of Great Britain and Northern Ireland; e-mail: sujit.biswas@city.ac.uk.

This work is licensed under a Creative Commons Attribution 4.0 International License.
© 2026 Copyright held by the owner/author(s).
ACM 1557-7341/2026/7-ART
https://doi.org/10.1145/3816144

Just Accepted

Additional Key Words and Phrases: Internet of Vehicles (IoV), IoV Security, EC, ML, Predictive Analytics, Intelligent Transportation Systems

1 Introduction

The Internet of Vehicles (IoV) integrates vehicles, roadside units, and cloud platforms into a unified, cyber physical transportation network, enabling real time data exchange for traffic management, V2I communication, and automated driving services [171]. However, pervasive connectivity also broadens the attack surface: compromised sensors, spoofed messages, or hijacked control channels can breach privacy, disrupt services, and endanger lives [112].

Conventional security solutions, firewalls, signature based Intrusion Detections Systems (IDS), and centralised analysis, struggle with IoV's stringent latency requirements (sub-10 ms), high mobility, and device heterogeneity. Edge Computing (EC) mitigates these constraints by processing data locally, cutting round trip delays and reducing backbone exposure [64]. Machine Learning (ML) adapts to evolving attack patterns via predictive classifiers and clustering [28, 121], while Deep Learning (DL) uncovers subtle, high dimensional anomalies that shallow models miss [31, 45].

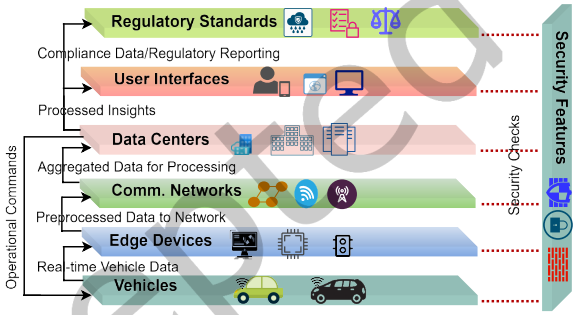

Fig. 1. Data flow and interactions within the IoV framework: Integrating components with security measures.

Each technology alone reveals gaps: EC lacks deep analytics, ML falters on zero day exploits, and DL can overwhelm resource limited nodes. Their *synergistic integration*, e.g., edge hosted ML filters that pre-screen data for downstream DL inference, plus federated updates that protect raw data, promises a real time, scalable, and privacy preserving IoV security fabric [189].

The Figure 1, offers a comprehensive view of the dynamic interactions and data flow among all technologies within the IoV framework. This figure illustrates the essential roles of various IoV components, showing how data traverses the system from vehicles to edge devices and then to central data hubs, finally reaching end user interfaces, all underpinned by robust security protocols and standards. The synergy between these technologies is vital for strengthening IoV security.

Scope of this Survey: This survey examines the latest advancements in EC, ML, and DL with a specific focus on their role in IoV security, covering research published between 2019 and 2026. Foundational works are referenced where necessary to provide historical context and highlight the evolution of artificial intelligence driven cybersecurity in IoV. This study not only analyzes the theoretical and practical integration of edge intelligence and AI-based security mechanisms but also presents real world applications through case studies, illustrating how these technologies enhance threat detection, intrusion prevention, and data privacy in IoV. Furthermore, this survey examines emerging technological trends that are expected to reshape IoV security frameworks, including quantum computing, AI-driven autonomous security models, and next generation networks. By identifying current challenges and future directions, this work provides a structured foundation for researchers and practitioners seeking to advance scalable, adaptive, and privacy preserving security solutions for IoV ecosystems.

Key Research Questions: This survey explores the integration of EC, ML, and DL in securing IoV systems by addressing the following research questions:

(1) What are the distinct vulnerabilities and threat vectors present within different IoV architectures and connectivity models?

Just Accepted

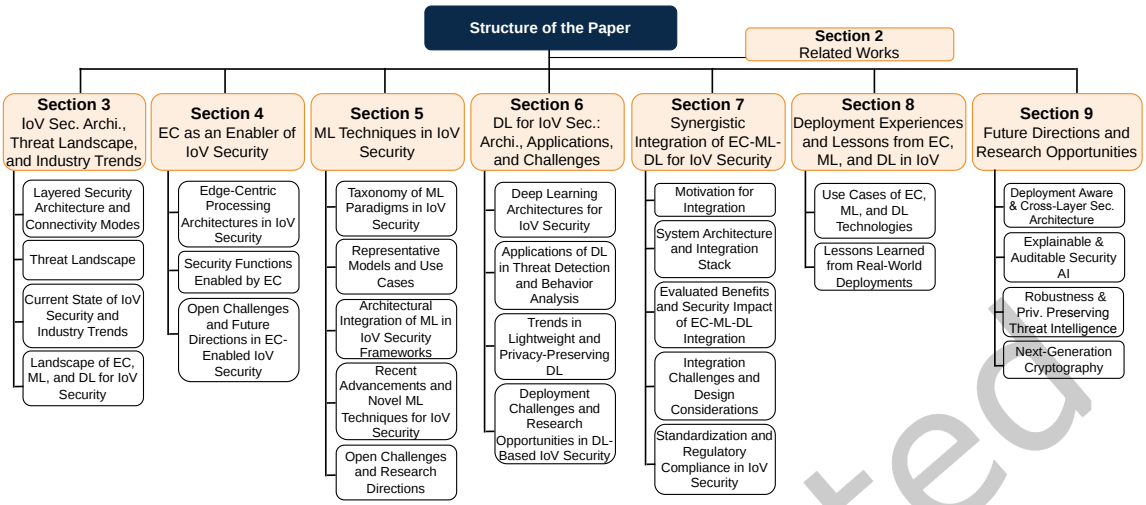

Fig. 2. Overview of the paper structure.

Just Accepted

(2) How does the incorporation of EC influence latency reduction, scalability, and real time security enforcement in IoV networks?
(3) In what ways do ML and DL techniques advance the detection, classification, and mitigation of security threats compared to traditional approaches?
(4) How do ML and DL models enhance pattern recognition and anomaly detection capabilities within complex, high dimensional IoV data streams?
(5) What synergistic benefits emerge from integrating EC with ML and DL technologies in designing adaptive and resilient IoV security frameworks?
(6) How does the adoption of emerging technologies affect regulatory compliance and the evolution of industry standards within the IoV security domain?
(7) What operational and technological challenges persist in deploying integrated IoV security frameworks, particularly concerning interoperability, system maintenance, and scalability?
(8) What future directions and emerging research areas are poised to drive advancements in AI-driven IoV security frameworks?

Structure of the Paper: This survey explores the integration of advanced technologies in IoV security. Figure 2, outlines the organization. Section 2, *Related Works*, reviews prior surveys and positions this study's contributions. Section 3, *IoV Security Architecture, Threat Landscape, and Industry Trends*, discusses layered models, threat evolution, and industry responses. Section 4, *Role of EC in IoV Security*, highlights EC's role in real time defense. Sections 5 and 6, *ML* and *DL Techniques*, examine AI approaches for adaptive threat mitigation. Section 7, *Synergistic Effects of Combining Technologies*, assesses integrated EC-ML-DL frameworks. Section 8, *Case Studies*, presents real world deployments, and Section 9, *Future Directions and Research Opportunities*, identifies open challenges. Section 10 concludes with a synthesis of insights.

Table 1. Comparison of existing surveys on IoV security and research gaps analyzed in this work.

Ref (Year)	EC	ML	DL	Focus	Gaps	Improvements in This Work
[157]⊕ (2019)	✗	✓	✗	ML in 5G/6G IoV	Missing DL + EC	Unified ML + DL + EC
[125]∗ (2020)	✗	✓	✗	Resilience in IoV	Privacy; EC	Privacy-preserving ML + EC
[173]∗ (2020)	✓	✗	✓	EC for DL	Real-time detection; resource mgmt	EC-enhanced ML/DL security
[48]‡ (2020)	✓	✗	✗	EC real-time processing	DL security	EC + DL + ML integration
[132]∗ (2020)	✗	✓	✗	Adversarial defense	EC for adversarial ML	ML + DL + EC defense
[156]∗ (2021)	✗	✓	✗	ML threat mitigation	EC integration	Edge-augmented ML mitigation
[34]‡ (2021)	✗	✗	✓	DL analytics	Security analytics	DL + real-time detection
[114]∗ (2021)	✓	✓	✗	Edge ML processing	Security at edge	Scalable edge ML detection
[49]∗ (2022)	✓	✓	✓	Resource allocation	Security measures	Secure resource allocation
[175]† (2023)	✓	✗	✗	Blockchain integrity	ML/DL detection	ML/DL + Blockchain security
[100]† (2023)	✓	✗	✓	Privacy-preserving IoV	Scalability	Scalable privacy-preserving framework
[22]∗ (2023)	✓	✓	✓	5G-V2X misbehavior	Real-time; scalability	Real-time EC integration
[7]∗ (2024)	✗	✗	✓	DL for IDS	Scalability; edge processing	Scalable edge-driven IDS
This Work (2026)	✓	✓	✓	Integrated IoV security	–	Unified, real-time ML/DL/EC focus

ML: Machine Learning; DL: Deep Learning; EC: Edge Computing. ✓= Present, ✗= Not Present.
⊕: Security-Focused; ∗: Survey/Review; ‡: Applied Research; †: Framework/Model.

Just Accepted

2 Related Works

2.1 Comparison of Existing Works

Existing surveys and comparative studies on IoV security has explored ML, DL, and EC, but most studies treat these technologies in isolation, lacking a unified or integrated approach. Table 1 classifies the surveyed literature into four categories: security focused studies, survey/review papers, applied research, and framework/model proposals. This categorization helps distinguish between foundational surveys, practical implementations, and theoretical models, highlighting existing gaps in cross technology integration. Several works have investigated ML and DL based security mechanisms, primarily focusing on threat detection and anomaly classification [7, 132, 156]. However, these studies often overlook scalability issues and fail to address how EC can enhance real time processing in resource-constrained vehicular environments. Conversely, research focused on EC highlights its benefits for IoV security, including latency reduction and computational offloading [48, 173]. Yet, these approaches generally lack integration with ML/DL models needed for adaptive and intelligent security systems. Privacy preserving techniques such as FL and blockchain have also been examined in recent literature [100, 175]. These works emphasize data integrity and privacy but do not fully address computational efficiency or the challenges of scaling such methods in large vehicular networks.

This survey advances the existing body of work by offering an integrated analysis of EC, ML, and DL technologies in the context of threat detection, scalability, and privacy preserving mechanisms. It further investigates emerging challenges in 5G/6G network environments, AI-driven adaptive security, and quantum-resistant cryptographic approaches, delivering a comprehensive and forward-looking perspective on IoV security frameworks. Some of the crucial *research gaps* in comparative studies are:

- *Fragmented integration.* EC, ML, and DL are often evaluated in isolation; cross layer frameworks that coordinate them remain scarce [64].
- *Privacy vs. performance.* Certificateless crypto, FL, and blockchain each tackle privacy, but their joint use with edge intelligence is poorly understood [175, 182].
- *Real time scalability.* Offloading lowers latency [185] yet little work couples it with adaptive ML/DL for large scale, dynamic fleets.
- *Next-gen threats.* 5G/6G slicing attacks, adversarial ML, and post quantum cryptography are recognized individually [157] but not analysed within an integrated IoV security stack.

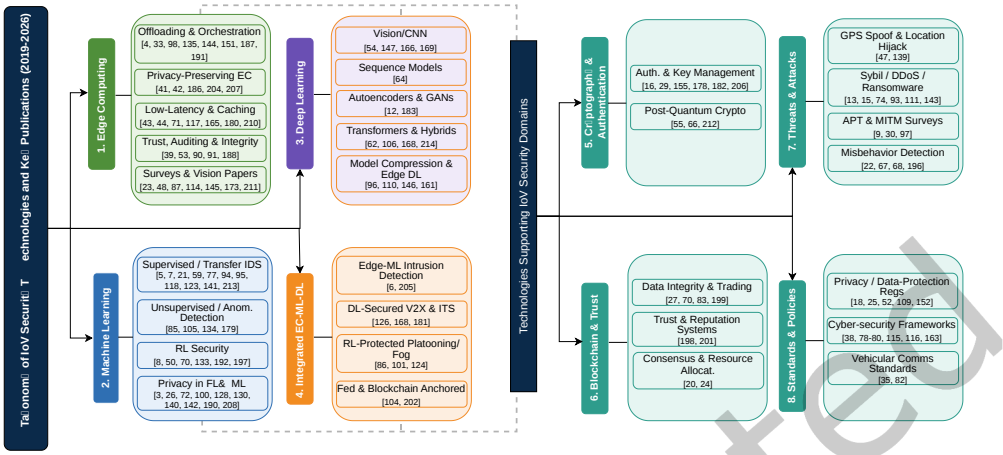

Fig. 3. Taxonomy of IoV security technologies and key publications (2019–2026).

2.2 Our Contributions

To address the fragmentation and rapid evolution of IoV security research, this survey makes five key contributions:

(1) *Comprehensive Taxonomy.* We synthesize over 200 works published between 2019 and 2026 into a unified taxonomy in Figure 3, categorizing EC, ML, DL, and fully integrated EC–ML–DL solutions according to their primary security functions and deployment models.
(2) *In-Depth Technology Analysis.* For each pillar (EC, ML, DL) we critically examine fundamental methods (e.g., offloading strategies, supervised vs. unsupervised learning, CNN/RNN architectures), quantify their performance trade-offs in latency, accuracy, energy, and privacy, and compare edge native optimizations such as pruning, quantization, and federated updates.
(3) *Real World Case Studies & Lessons.* We curate a diverse set of large scale deployments, from keyless vehicle authentication and collision avoidance to city scale traffic monitoring, and distill actionable lessons on data governance, scalability, interoperability, continuous adaptation, and user privacy.
(4) *Challenges & Mitigation Strategies.* Drawing on the literature and our case study insights, we map out critical obstacles, resource constraints, network reliability, regulatory compliance, and propose concrete mitigation tactics, including neuromorphic/event driven inference, blockchain anchored model provenance, and hybrid cryptographic schemes.
(5) *Future Research Roadmap.* We chart a forward looking agenda covering post quantum and homomorphic encryption, explainable and adversarially robust AI, cross layer adaptive security architectures, and 6G enabled V2X trust frameworks, each linked to open questions that will guide the next wave of IoV security innovation.

2.3 Literature Review Process

Figure 4 depicts our six stage review process. We queried IEEE Xplore, ACM DL, SpringerLink, and ScienceDirect with terms such as “IoV security”, “edge computing”, “machine/deep learning in IoV”, and “FL”; filters retained peer reviewed work from 2019-2026, plus seminal older papers. Full text screening assessed methodological rigour and real world relevance. Selected studies were coded into themes: EC frameworks, ML based defences,

Just Accepted

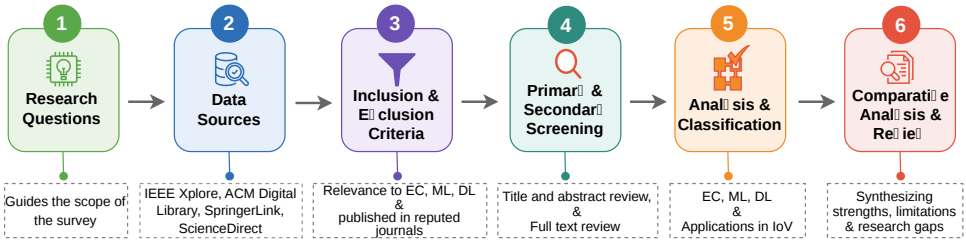

Fig. 4. Search methodology for IoV security survey: Systematic data collection, screening, & analysis.

DL anomaly detection, and privacy preserving techniques (FL, blockchain). The process supports a transparent, reproducible evidence base for the survey's findings.

3 IoV Security Architecture, Threat Landscape, and Industry Trends

3.1 Layered Security Architecture and Connectivity Modes

The security architecture of the IoV is typically conceptualized as a three-layered model, as illustrated in Figure 5. This layered view facilitates the decomposition of security responsibilities across vehicular, edge, and cloud infrastructures. At the *vehicle network layer*, on-board units (OBUs) are responsible for authenticating V2V communications using short lived public key infrastructure (PKI) credentials. These units also perform frame validation to filter malformed or malicious packets at the point of origin. The *local communication layer*, which operates through RSUs, is tasked with aggregating traffic, applying intrusion detection mechanisms, and enforcing rate limiting to counter volumetric DoS attacks. The uppermost *cloud analytics layer* integrates telemetry from distributed vehicular sources with external threat intelligence feeds. This layer increasingly leverages DL classifiers and FL frameworks to support privacy-preserving threat detection and adaptive response.

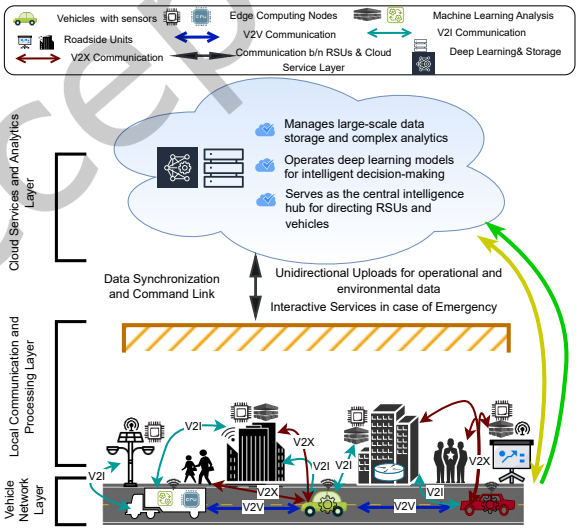

Fig. 5. Hierarchical architecture of IoV.

3.2 Threat Landscape

Understanding the threat landscape is essential for identifying the limitations of conventional security models and motivating the adoption of emerging solutions. Figure 6 illustrates common attack vectors across the IoV stack, while Figure 7 shows that recent incidents most frequently target telematics units (43%), infotainment systems (15%), and public APIs (13%). Table 2 complements these figures by showing that IoV threats differ not only in attack method, but also in operational impact, ranging from privacy leakage and service disruption to direct safety-critical control compromise. Attacks can be broadly categorized as follows:

Network centric attacks, such as Sybil and DoS, are commonly mitigated using distributed trust models and entropy based filtering [93, 143, 198]. *Identity based threats*, including GPS spoofing and certificate forgery, are

Just Accepted

Table 2. Summary of IoV threats, manifestations, and defense implications.

Refs	Threat	Typical manifestation	Defense implication
[93, 111]	Sybil	Fake identities; false events	Requires identity consistency checks & cross-node validation
[93, 143, 181]	DoS/DDoS	Flooding; botnet surges	Requires low-latency availability protection and rate control
[16, 37]	MitM	Data injection; tampering	Requires integrity validation and session protection
[29, 47, 139]	Spoofing	GPS/device impersonation	Requires sensor/context cross-validation
[40, 150]	Identity theft	Credential theft; takeover	Requires credential protection and rapid revocation
[60, 178, 186]	Session hijack	Session reuse; route change	Requires re-authentication and session continuity checks
[29]	API vuln.	API exploitation	Requires backend monitoring and application-layer hardening
[17, 73]	Eavesdropping	Sniffing; traffic analysis	Requires encryption and metadata exposure control
[94]	Timing	Cryptographic timing leakage	Requires implementation-level hardening
[29, 85, 155]	Replay	Frame replay; packet delay	Requires freshness and timing validation
[3, 65, 193]	False data	Traffic/status falsification	Requires plausibility and cross-source consistency checks
[84, 86, 181]	Platoon attacks	Tampering; jamming	Requires coordinated low-latency response
[95, 203]	CAN bus hack	Rogue control commands	Requires onboard millisecond-scale detection
[15, 74]	Ransomware	System lock	Requires resilience and recovery planning

addressed through Long Short-Term Memory (LSTM) based sensor fusion techniques [47, 178]. *Data integrity breaches* are countered by timestamp verification and encrypted cooperative perception [85, 150]. *Physical and software exploits*, such as CAN bus injection and unsecured APIs, require hardened gateways and encrypted internal communication [29, 84, 203].

Implications: The threat landscape highlights the multidimensional nature of IoV security risks, which span from physical-layer intrusions to protocol level and application layer exploits. These observations underscore the limitations of traditional perimeter based defenses in coping with dynamic, large scale, and latency sensitive vehicular environments. The complexity and distribution of these threats necessitate layered mitigation strategies that combine local anomaly detection, secure communication protocols, and resilient network architectures. Accordingly, understanding the characteristics of these attack vectors is essential for assessing the effectiveness of existing security architectures and identifying areas that demand more adaptive and context aware solutions.

3.3 Current State of IoV Security and Industry Trends

Conventional IoV security relies on encryption, transport layer security, multi-factor authentication, and rule based IDS to provide baseline protection [11, 19, 29, 136, 149]. These mechanisms remain useful against known

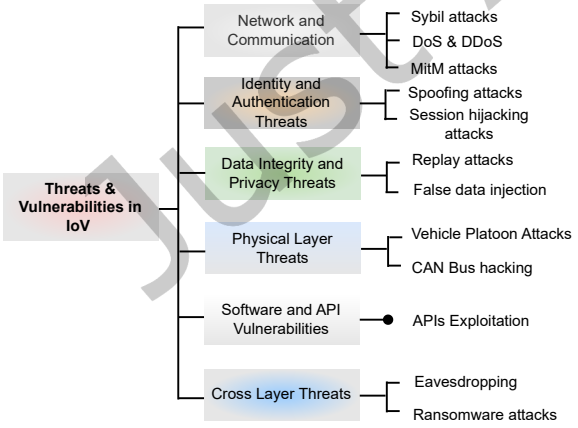

Fig. 6. Security threats in the IoV ecosystem.

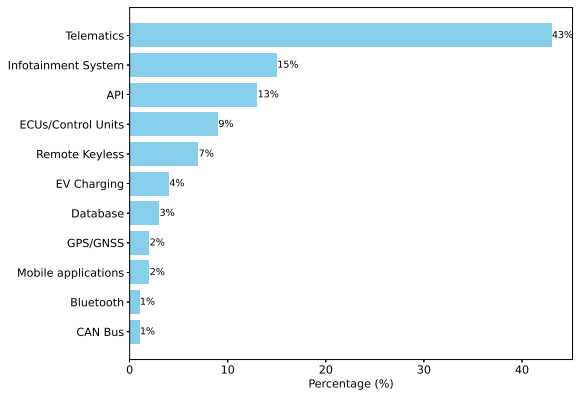

Fig. 7. Distribution of different attack vectors in connected vehicles (2023) [158].

Just Accepted

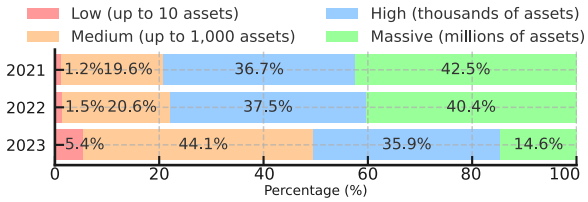

Fig. 8. Impact of security incidents (year-wise % of severity of incidents) in the IoV ecosystem.

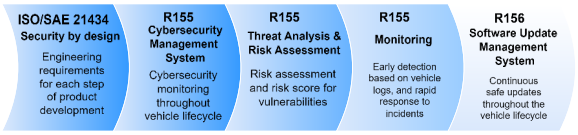

Fig. 9. Cybersecurity standards and practices in IoV.

threats, but they are increasingly limited in large and mobile IoV environments: deep packet inspection adds latency [46], signature based IDS misses novel attacks [123], and centralized telemetry collection scales poorly under dynamic vehicular traffic [117].

3.3.1 Modern countermeasures. Recent work therefore shifts toward AI driven and data centric defense. ML based IDS improves adaptability to evolving threats [16], while DL models such as CNNs and RNNs have reported detection accuracies above 99% in selected settings [126]. Edge accelerators enable sub-10 ms inference for near real time response [75], and FL reduces raw data transfer while preserving privacy [113]. Blockchain based integrity mechanisms [83, 201], lightweight cryptography, and quantum resistant primitives [66] further strengthen trust and resilience. Table 3 summarizes this transition toward distributed analytics, adaptive models, and decentralized enforcement, while also showing remaining challenges in edge scalability, jurisdiction specific compliance, and auditability [30].

3.3.2 Industry pulse. Market trends reinforce the urgency of connected vehicle security. The global connected car market is projected to grow from $80.0B in 2023 to $92.6B in 2024, driven by 5G infrastructure and AI integration [158]. At the same time, attacks are increasing: Figure 8 shows a 380% rise in API-related breaches since 2021 [14, 164]. Reported cases include remote control exploits affecting more than 25 automotive OEMs and a $2.25M Bitcoin extortion incident targeting NIO [69, 122].

3.3.3 Standardization and regulation. Standards and regulations are evolving in response to these risks. ISO/SAE 21434 and UNECE WP.29 emphasize cybersecurity by design, secure software updates, and incident response readiness, as summarized in Figure 9 [38, 80, 163]. The NIST Cybersecurity Framework further promotes continuous monitoring, OTA patching, and automated compliance verification [116]. Overall, IoV security is moving from static, infrastructure centric protection toward AI-augmented, edge-assisted, and standards-aligned defense. The following sections examine how EC, ML, and DL support this transition.

Just Accepted

Table 3. Comparison of traditional and current IoV security solutions.

Aspect	Traditional	Current	Advances & Limitations
Regulatory	Region-specific **[18]**	GDPR, NIST **[152]**	Better global alignment; cross-border compliance challenges
Energy	High consumption **[58]**	AI/EC-optimized **[146]**	Improved power management; DL remains energy-intensive
Data processing	Centralized, high latency **[46]**	Edge-powered, low latency **[145]**	Real-time responses; potential edge bottlenecks
Threat detection	Signature-based **[123]**	ML/DL-driven **[126]**	Proactive analytics; high compute and false positives
Security protocols	Static rules **[9]**	Adaptive models **[202]**	Responsive to new threats; complexity and compliance risks
Interoperability	Device-specific **[117]**	Standardized protocols **[44]**	Broad compatibility; legacy integration issues
Scalability	Poor at scale **[180]**	Modular AI/EC **[128]**	Handles large data; demands robust infrastructure
System updates	Manual, infrequent **[27]**	Automated, real-time **[20]**	Continuous adaptation; update rollout risks

3.4 Landscape of EC, ML, and DL for IoV Security

The scale and heterogeneity of IoV systems have pushed security architectures toward EC, ML, and DL as operational components rather than isolated research tools. Together, they support low latency detection, adaptive response, and privacy aware processing across vehicle, edge, and cloud layers.

3.4.1 Edge Computing Developments. MEC servers at RSUs increasingly host containerized security services such as certificate validation, local filtering, and misbehavior logging [64]. Context aware offloading uses vehicle speed, channel quality, or workload state to decide whether raw data, features, or inference outputs should be transmitted [185]. Certificateless cryptography reduces handshake latency [182], while fog based clustering improves fault tolerance through service replication across RSUs [124]. Remaining challenges include cross-infrastructure trust coordination and protection of edge hardware against side-channel attacks.

3.4.2 ML Approaches. Supervised models such as Random Forest and SVM remain common in IDS and report strong results on datasets such as CIC-IDS-2018 and VeReMi [132, 156]. Unsupervised methods are useful for zero-day discovery but often produce high false positives in dense traffic [22]. FL supports distributed training with reduced raw data exposure [48], and graph based methods improve context aware threat scoring from vehicle interactions [196]. Key limitations remain data imbalance, limited onboard compute, and adversarial vulnerability.

3.4.3 DL Architectures. DL supports RF fingerprinting, LiDAR analysis, CAN bus anomaly detection, and other high dimensional IoV security tasks [7, 31]. Lightweight autoencoders and variational models have been studied for real time anomaly detection on constrained hardware [45]. Layer splitting can move early processing to vehicles and later inference to edge servers, reducing onboard load while preserving low-latency response [191]. Persistent gaps include concept drift, adversarial robustness, and stable deployment under resource limits.

3.4.4 Integration Patterns. Three integration patterns are common: edge-hosted inference at RSUs for low-latency DL based threat detection [64]; hierarchical learning that combines RSU-level filtering with cloud-level model aggregation [100]; and collaborative analytics where blockchain records model hashes and verdicts for auditability [175]. However, these components are still often deployed separately. A unified architecture that jointly optimizes model placement, privacy, auditability, and detection accuracy remains an open requirement.

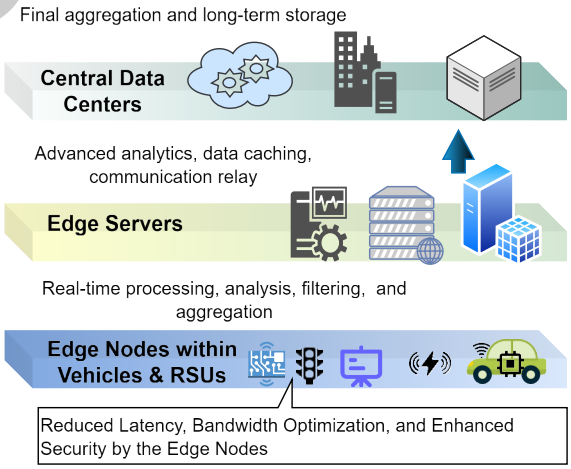

Fig. 10. Generalized EC architecture for IoV.

4 EC as an Enabler of IoV Security

The previous section outlined the architectural structure of IoV systems and highlighted the security threats that arise from centralized processing. In response to these limitations, EC has emerged as a foundational enabler of scalable, low latency, and privacy preserving security frameworks. By relocating computation closer to vehicles, via OBUs and RSUs, EC reduces decision latency, limits attack surfaces, and supports localized analytics. This section surveys the role of

Just Accepted

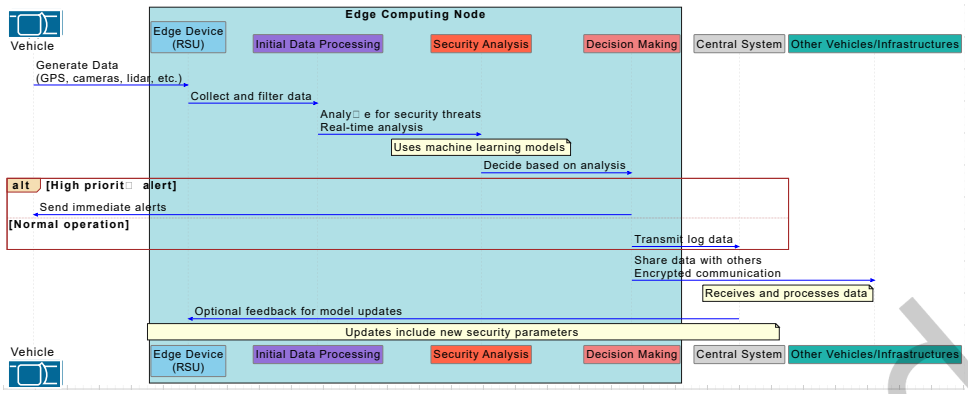

Fig. 11. EC in IoV security: Data flow & real time processing between vehicles, edge nodes, & central server.

Just Accepted

EC in IoV security, focusing on processing architectures, supported security functions, and outstanding research challenges.

4.1 Edge-Centric Processing Architectures in IoV Security

EC introduces a distributed processing paradigm within the IoV security architecture, enabling low latency threat detection, localized decision making, and reduced reliance on centralized cloud infrastructures. Figure 10 illustrates a commonly adopted three tier architecture, comprising vehicle level micro edge nodes, RSUs, and cloud based services. This hierarchy reflects increasing processing capacity and decreasing responsiveness from edge to core. At the lowest tier, OBUs process high frequency sensor data streams such as CAN bus messages, LiDAR point clouds, and GPS telemetry. Lightweight models, typically 1D CNNs or statistical filters, are employed to discard malformed packets or detect basic anomalies in real time [71, 107]. These micro edge functions reduce the computational burden on RSUs while enabling initial threat filtering at the data source. The intermediate tier consists of RSUs equipped with MEC servers that support more computationally intensive tasks. Models such as GRU-based autoencoders or CNN-LSTM hybrids are deployed to identify stealthier threats, including distributed DDoS bursts, spoofed beacons, or protocol misuse [98, 144]. RSUs may also perform data aggregation, rate limiting, and policy enforcement based on local context. At the top tier, cloud services handle global threat correlation, policy dissemination, and model refinement. Rather than transmitting raw sensor data, edge nodes forward meta-features or encrypted gradient updates, preserving privacy and reducing bandwidth consumption [41, 42, 188]. FL paradigms are commonly used to support collaborative model improvement across distributed sites without centralized data collection [195].

Figure 11 illustrates the secure data flow in an EC-enabled IoV architecture. Vehicles generate sensor data that is transmitted to nearby RSUs for real-time analysis and initial threat detection. High-priority alerts trigger immediate broadcasts to surrounding vehicles to support cooperative awareness [176]. In cases of uncertainty, RSUs forward encrypted feature summaries to the central system for further evaluation. Model updates and refined security parameters are periodically sent back to edge nodes, enabling adaptive local detection. This tiered architecture balances responsiveness, scalability, and security while enabling fine-grained policy enforcement and coordinated defense.

4.2 Security Functions Enabled by EC

EC has been widely adopted in recent IoV security frameworks due to its ability to support localized decision making, reduce data exposure, and improve system responsiveness. This subsection surveys how existing research leverages EC to enable core security functions, grouped by capability domain.

4.2.1 Reduced Exposure and Attack Surface. Several studies emphasize EC's role in minimizing the system's exposure to external threats. Zhao et al. demonstrate that executing threat detection tasks at RSUs reduces the number of packets transmitted over public networks, thereby limiting opportunities for interception and MitM attacks [209]. Quarantining compromised nodes at the edge, before their behavior influences global analytics, has also been proposed as a containment strategy.

4.2.2 Data Protection and Confidentiality. The work by Zhang et al. introduces LVPDA, a lightweight protocol tailored for resource constrained OBUs, enabling secure communication without significant memory overhead [204]. In a similar direction, Fan et al. propose DR-BFT, a blockchain-based framework that enables tamper evident logging with minimal RSU storage requirements [53]. Table 4 summarizes several design approaches that preserve privacy at the edge. Techniques such as attribute based encryption and homomorphic aggregation are employed to ensure that only processed insights, not raw data, are shared with cloud infrastructure.

4.2.3 Low Latency Threat Detection. Researchers have explored deploying layered detection models to balance speed and accuracy. Cui et al. evaluate shallow models for anomaly detection at micro edge devices, enabling sub-millisecond inference for coarse threats [39]. In contrast, deeper models such as CNN-LSTM hybrids deployed at RSUs are used to detect stealthy or high-dimensional attacks. Table 5 outlines use cases where these models are particularly effective in time-critical scenarios. Work by Li et al. further integrates authentication mechanisms using aggregate signatures and decentralized token checks directly at the edge [91].

4.2.4 Operational Efficiency and Proactive Response. Edge enabled architectures also support broader system level goals. Hou et al. and Abouaomar et al. show that local inference reduces communication overhead and radio congestion in dense vehicular environments [4, 71]. Work by Cui et al. and Zhu et al. demonstrates that predictive models deployed at RSUs can preemptively detect intrusion and unsafe driving conditions, enabling real time actuation in V2X applications [41, 213]. Overall, the literature confirms that EC strengthens both the defensive and operational dimensions of IoV security. By pushing intelligence closer to data sources, EC enables scalable and context aware mechanisms that align with the timing, privacy, and resource constraints of connected vehicle ecosystems.

4.3 Open Challenges and Future Directions in EC-Enabled IoV Security

EC has enabled advancements in IoV security, several technical and architectural challenges remain unresolved. This subsection surveys key limitations identified in the literature and highlights promising directions for future research, with emphasis on deployment scalability, trust management, and convergence with emerging technologies.

4.3.1 Resource Allocation and Model Placement. Efficient distribution of computation between vehicle, RSU, and cloud tiers remains a core challenge. Hou et al. and Zhao et al. discuss the difficulty of supporting GPU-class

Table 4. Key advantages of EC in IoV.

Refs	Advantage	Description	Use Case
[135, 209]	Bandwidth opt.	Reduces upstream data; eases network congestion	Smart-city traffic mgmt
[41, 43]	Enhanced privacy	Local data processing; lowers breach risk	AV location sharing
[4, 71]	Latency cut	Edge-side analytics; faster response	Real-time obstacle avoidance

Just Accepted

Table 5. Key security features enabled by EC in IoV and real-world applications.

Ref	Latency↓	FW-Upd	Encrypt	Detect	Auth	Access	Integrity	Anomaly
[146]	✓	×	×	×	×	×	×	×
[206]	×	✓	×	×	×	×	×	×
[145]	×	×	✓	×	×	×	×	×
[126]	×	×	×	✓	×	×	×	×
[44]	×	×	×	×	✓	×	×	×
[128]	×	×	×	×	×	✓	×	×
[27]	×	×	×	×	×	×	✓	×
[23]	×	×	×	×	×	×	×	✓

Table 6. Future EC technologies for IoV security: technology use (✓/ ×) and their impact.

Refs	AI	QC	BC	AR/VR	5G/6G	Pred Ana.	Auto	Impact
[211]	✓	×	×	×	×	×	×	Threat Detection
[55]	×	✓	×	×	×	×	×	Data Protection
[87, 199, 200]	×	×	✓	×	×	×	×	Integrity
[131]	×	×	×	✓	×	×	×	Situational Awareness
[103, 127]	×	×	×	×	✓	×	×	Low Latency
[168] (Pred. Anal.)	×	×	×	×	×	✓	×	Proactive Defence
[168] (Auto Edge Mgmt)	×	×	×	×	×	×	✓	Continuous Integrity

inference at scale across RSUs [71, 207]. Existing work explores dynamic offloading strategies that consider local queue length, wireless channel state, and model complexity, but real-time guarantees and generalizability across scenarios remain open problems [53, 64].

4.3.2 Trust Management and Security Foundations. Establishing trust at the edge involves trade-offs between performance and cryptographic rigor [170, 187]. Xu et al. and Wang et al. emphasize the need for tamper proof hardware, secure boot processes, and continuous attestation to prevent side channel attacks on exposed edge nodes [64]. Grover et al. highlight the complexity of key revocation in local escrow schemes [55]. Fernandez et al. propose integrating post quantum cryptography to future-proof V2X communication.

4.3.3 Scalability and Heterogeneity. EC deployments face management overhead due to heterogeneous hardware, varied software stacks, and patching complexity [64]. Studies have proposed containerized, OTA update mechanisms to streamline DevSecOps for distributed edge environments, yet coordinating updates across thousands of mobile and static edge nodes introduces reliability and consistency concerns.

4.3.4 Privacy Preserving Learning and Concept Drift. Adaptive security frameworks based on FL must account for rapidly changing traffic conditions and adversarial patterns [48]. Deng et al. propose scheduling update intervals to manage radio contention in vehicular platoons [188]. Xu et al. examine trust-aware aggregation in the presence of compromised edge nodes. However, maintaining model accuracy under concept drift without compromising privacy remains an active area of research.

4.3.5 Integration with Emerging Technologies. Recent studies envision the convergence of EC with complementary technologies [211]. Zhou et al. investigate continual learning for predictive, rather than reactive, threat detection [87]. Lightweight blockchains for telemetry integrity, quantum resistant cryptographic schemes, and deterministic networking over 5G/6G links are increasingly proposed as architectural extensions [55, 103]. Edge-rendered augmented reality (AR) dashboards have also been explored for real-time threat visualization [131].

Table 6 summarizes these future facing developments. Integrating such technologies into a unified, resource aware edge intelligence stack that complies with both safety and regulatory requirements presents a key direction for the next generation of IoV systems.

Just Accepted

5 ML Techniques in IoV Security

ML is reshaping threat detection and mitigation in IoV systems. This section examines how ML enhances detection, integrates with IoV security frameworks, and compares with traditional approaches, highlighting key strategies, challenges, and future directions.

5.1 Taxonomy of ML Paradigms in IoV Security

ML underpins adaptive, data-driven IoV security, overcoming the limits of static rule-based defenses. This subsection classifies key paradigms, supervised, unsupervised, and reinforcement learning (RL), and examines their security roles. Figure 12 highlights the shift toward predictive analytics, while Table 7 summarizes their representative use cases.

5.1.1 Supervised Learning. Supervised learning remains the most widely adopted paradigm in IoV security research. Classifiers such as Random Forests, SVMs, and Gradient Boosting Machines can detect replayed beacons, forged packets, and malware with over 95% accuracy on public datasets [213]. Gao et al. and Li et al. further show that these models outperform traditional intrusion-detection baselines in latency and precision [59, 91]. However, their practical strength is greatest for well-characterized attacks, since they depend on labeled data and often require retraining to remain effective under evolving threats such as novel DoS variants and distribution shift.

5.1.2 Unsupervised Learning. Unsupervised methods are increasingly used to detect previously unseen or zero-day threats. Clustering algorithms such as k-Means and Self-Organizing Maps (SOM), together with dimensionality-reduction techniques such as Principal Component Analysis (PCA), have been applied to identify anomalous behavior in unlabeled vehicular traffic [179]. These approaches are attractive in open V2V environments where labels are unavailable, but this flexibility comes with weaker decision boundaries and higher false-positive rates. In practice, their operational value often depends on human review or hybrid pipelines that can filter noisy alerts before enforcement.

5.1.3 Reinforcement Learning. RL offers a dynamic alternative to static policy enforcement by allowing agents to adapt defense strategies from real-time feedback. RL-based tuning of firewall rules and quality-of-service settings has been explored in vehicular edge environments [90, 197]. Although RL can react quickly to probing attacks and stealthy behavior, its deployment remains challenging because reward design, training stability, and continuous policy adaptation can impose substantial overhead on resource-constrained RSUs. As a result, RL is promising for adaptive control, but typically less straightforward to operationalize than lightweight supervised or hybrid defenses.

5.1.4 Hybrid and Layered Approaches. Recent platforms combine multiple ML paradigms to build layered security defenses. Supervised classifiers are used for well-characterized threats, unsupervised detectors monitor for emerging anomalies, and RL agents adapt firewall or routing policies in real time. This multi-paradigm design is attractive because it better matches IoV deployment realities. Importantly, no single learning paradigm simultaneously offers stable accuracy, novelty awareness, and low operational cost. Hybrid systems therefore provide a more practical balance among detection quality, adaptability, and computational efficiency across heterogeneous IoV conditions [59, 179, 197, 213].

Table 7. ML paradigms for IoV security.

Paradigm	Strengths	Limitations	Typical IoV Use
Supervised	✓High accuracy on known patterns	× Needs labeled data; weak on zero-day	Malware / IDS (known attacks)
Unsupervised	✓Detects unknowns; unlabeled data	× Many false positives; needs validation	V2X anomaly spotting
Reinforcement	✓Adapts to dynamics; policy learning	× Compute heavy; reward tuning	Adaptive IDS; policy optimisation

Just Accepted

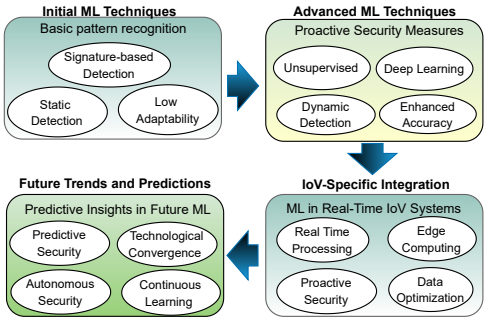

Fig. 12. Evolution of ML in cybersecurity.

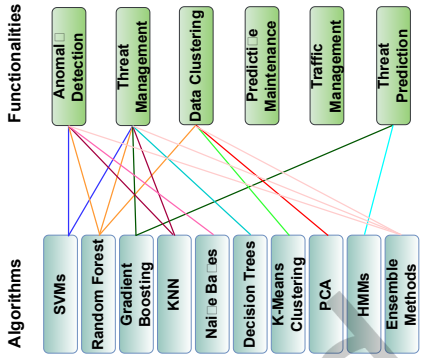

Fig. 13. Relationship between ML algorithms & their functionalities within IoV context.

5.2 Representative Models and Use Cases

This subsection examines representative ML models for IoV security across intrusion detection, anomaly detection, behavior prediction, and flow classification, emphasizing generalization, interpretability, overhead, and robustness. Figure 13 maps these models to security functions, while Table 8 summarizes reported benchmark performance.

5.2.1 Classification and Filtering. Supervised classifiers such as SVMs, Random Forests, and Gradient Boosting Machines remain dominant because they perform well on labeled benchmarks and are easier to validate than adaptive or unsupervised methods. They achieve over 95% accuracy in detecting malware injections and replay attacks in V2X communications [59, 213]. However, benchmark accuracy often reflects controlled distributions rather than open IoV conditions. SVMs handle high-dimensional features but are sensitive to tuning and scalability limits. Ensembles improve robustness under class imbalance, yet increase inference cost and reduce interpretability. Lightweight classifiers such as *k*-Nearest Neighbors (k-NN), Naïve Bayes, and Decision Trees remain useful for real-time OBU filtering, mainly for bounded and well-characterized attacks.

5.2.2 Anomaly and Outlier Detection. Unsupervised models complement supervised classifiers by targeting zero-day threats and protocol deviations. k-Means and PCA identify deviations in vehicular telemetry, while Hidden Markov Models (HMMs) capture temporal anomalies in CAN messages and beacon sequences [179]. Their main advantage is reduced dependence on labeled attack data, which is valuable in open V2V settings. However, anomaly is not equivalent to maliciousness. These models therefore face weak decision boundaries, threshold sensitivity, and higher false-alarm rates, making them more suitable as early-warning components than standalone enforcement mechanisms.

5.2.3 Intrusion Detection Enhancements. Recent IDS studies improve performance through ensemble tuning, hybrid pipelines, and transfer learning. Intrusion-detection accuracies above 98% have been reported after Bayesian optimization and semi-supervised reinforcement learning [50, 126]. Precision gains also come from multi-stage classifiers, reputation scoring, and feature selection [77, 134], showing that improvements increasingly depend on pipeline design rather than a single classifier. However, higher accuracy may add training cost, latency, and integration complexity. Transfer learning helps reduce labeled-data scarcity by fine-tuning pre-trained models on related vehicular datasets [67], but its benefit can degrade under cross-domain mismatch.

5.2.4 Behavior Modeling and Prediction. Predictive modeling increasingly uses sequence-aware models such as RNNs and LSTM networks for sensor and trajectory time series [13, 168]. These models capture temporal

Just Accepted

Table 8. ML-based studies and their roles in intrusion or misbehavior detection.

Refs	ML Technique(s)	Focus	Role
[94]	Transfer learning	IoV intrusion detection	Cross-domain adaptation
[126]	DL + SHAP (Shaply Explainable)	Transportation IDS	Detection + interpretability
[77]	Optimized multi-stage ML	Network intrusion detection	Model/feature optimization
[134]	Adaptive ML classifiers	VANET malicious node detection	Real-time node screening
[67]	SVM + reputation model, Feed Forward NN	Vehicular misbehavior detection	Joint trust-aware detection
[141]	Classical ML classifiers	IoV misbehavior detection	Data-centric misbehavior screening
[1]	Ensembles, Comparative ML evaluation	Anomaly-based IoT IDS	Model benchmarking
[50]	Semi-supervised deep RL	Abnormal traffic detection	Adaptive detection with limited labels

Entries summarize the primary role of each study. Datasets, baselines, and evaluation metrics differ across papers.

dependencies but require larger datasets, more computation, and careful tuning. Graph-based models can represent dynamic vehicular relationships and cooperative threats, but their deployment remains limited by modeling complexity, resource demand, and lower maturity than lightweight classifiers. Behavior modeling is therefore most useful when temporal or relational context is central to the threat, not for routine low-cost filtering.

Table 8 summarizes representative ML-based studies by technique, security focus, and reported role in intrusion or misbehavior detection.

5.3 Architectural Integration of ML in IoV Security Frameworks

Effective deployment of ML in IoV security depends on coordinated placement across OBUs, RSUs, edge gateways, and cloud infrastructure. Figure 14 illustrates the multi-tier pattern commonly adopted in recent studies. At the embedded layer, lightweight classifiers on OBUs and RSUs support real-time anomaly detection from control messages and sensor data. Ullah et al. show that such models can detect anomalies in CAN bus signals within milliseconds, enabling fail-safe triggers close to the point of data generation [162].

At the network tier, edge nodes aggregate traffic across vehicles and expose flow-level correlations that are not visible to individual nodes. Aslam et al. show that clustering and supervised classification at this tier can identify coordinated scans and distributed attacks more effectively than isolated in-vehicle detectors [13]. At the operations tier, ML-enhanced SOC platforms integrate ensemble classifiers, reputation-based scoring, and incident response workflows to coordinate alerts and mitigation across the broader IoV environment [92, 126]. At the backend, cloud services provide wider threat visibility and retrain detection models on broader datasets. As shown by Alsharif et al. and Javaid et al., cloud-trained models can be compressed and pushed to the edge for deployment on resource-constrained OBUs [10, 81], while FL further reduces raw-data exposure by supporting local training with global aggregation.

This layered design balances fast local response with broader analytical depth. Embedded and edge models are better suited to low-latency detection, whereas cloud-tier intrusion analysis support wider visibility, retraining, and cross-domain adaptation. Its main challenge is not whether ML can operate at each tier, but how to distribute detection, retraining, and policy coordination without exceeding latency, bandwidth, and privacy constraints.

5.4 Recent Advancements and Novel ML Techniques for IoV Security

Recent IoV security research focuses adaptability, privacy, and robustness through *federated learning*, *adversarial training*, *graph-based models*, *self-supervised learning*, and early work on *quantum-assisted inference*. Yamany et al. and Cao et al. use *federated learning* to train models across OBUs and RSUs without centralizing raw vehicular data [26, 190]. FL reduces privacy and bandwidth costs, but its decentralization also increases exposure to poisoning, non-IID data drift, and unreliable edge participation. Thus, its practical value depends on robust aggregation, client validation, and trust management. *Adversarial training*, including GAN-augmented IDS

Just Accepted

Table 9. DL architectures in IoV: Advantages, Limitations, and Use Cases.

Architecture	Advantage	Limitation	Use Case
CNN	High image accuracy	High compute/memory	Traffic monitoring, obstacle detection
RNN	Temporal modeling	Vanishing gradients	Trajectory forecasting, flow analysis
AE	Anomaly detection	Noise sensitivity	IDS anomaly spotting
GAN	Data augmentation	Training instability	Synthetic attack data generation

pipelines, improves resistance to evasion and poisoning attacks [23, 197]. However, these gains come with higher training complexity and weaker deployment maturity than lightweight IDS models.

Context-aware methods offer another direction. *Graph neural networks* model V2V relations and collaborative threat patterns [62, 106], while *sequence-aware models* such as RNNs and LSTMs capture temporal dependencies in vehicular telemetry [168]. These models provide richer behavioral context than static classifiers, but require greater computation, data quality, and tuning. *Self-supervised learning* is comparatively more deployable because it exploits unlabeled vehicular data through pretext tasks [62], making it useful where labeled attacks are sparse or delayed.

Quantum-assisted learning remains largely exploratory. Huang et al. note its potential for cryptographic analysis and anomaly inference, but practical IoV deployment is still speculative [72]. Overall, these advances show a shift from static detection toward proactive, privacy-aware, and context-sensitive defense. Their deployment readiness is uneven: FL and SSL are the most actionable, graph-based and adversarial methods are promising but heavier, and quantum-assisted learning remains a longer-term research direction.

5.5 Open Challenges and Research Directions

Despite progress in ML-driven IoV security, practical deployment remains limited by *data availability*, *model adaptivity*, *system scalability*, and the feasibility of *collaborative, self-evolving defenses*.

Prior work highlights *data availability and quality*: privacy constraints, inconsistent formats, and annotation cost restrict large-scale IoV datasets [92, 142]. LiDAR, CAN, and GPS data require specialized preprocessing and are difficult to harmonize across platforms, so scarcity is both a volume and comparability problem. Synthetic-data generation and simulation-based augmentation can improve rare-event coverage, but only when synthetic conditions reflect deployment realities. *Model drift and adaptivity* are equally difficult because IoV environments are non-stationary. Static ML models degrade as attacker behavior, network conditions, and traffic patterns evolve. Incremental learning and online RL offer adaptive alternatives, but remain constrained by edge-device compute, memory, and validation limits [142, 197].

From a systems perspective, *scalability and deployment complexity* remain major rollout bottlenecks. Grover et al. and Zhao et al. note that orchestrating pruned models, over-the-air updates, and cross-node consistency is difficult under mobility and bandwidth constraints [64, 207]. Finally, *collaborative and self-evolving security* is attractive but not yet routine. FL, adversarial training, and self-supervised pipelines offer distributed intelligence, but require stronger evidence under adversarial conditions, real-time response limits, and privacy-audit requirements before they can be treated as deployment-ready [23, 26, 62, 190]. Progress therefore depends not only on better models, but also on realistic evaluation, update governance, and evidence that adaptive defenses remain dependable at fleet scale.

6 Deep Learning for IoV Security: Architectures, Applications, and Challenges

DL pushes IoV security beyond feature engineered ML by extracting multi scale patterns from images, signals, and traffic flows in real time. Its layered representations unlock fine grained object detection for automated driving, sequence modelling for behaviour prediction, and unsupervised anomaly discovery in high velocity data streams.

Just Accepted

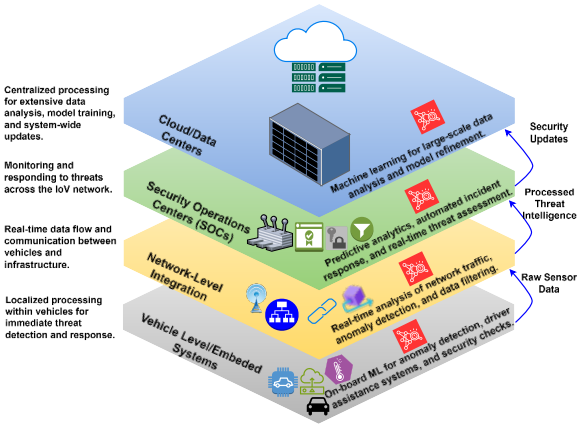

Fig. 14. High-level architecture of ML integration within IoV security frameworks.

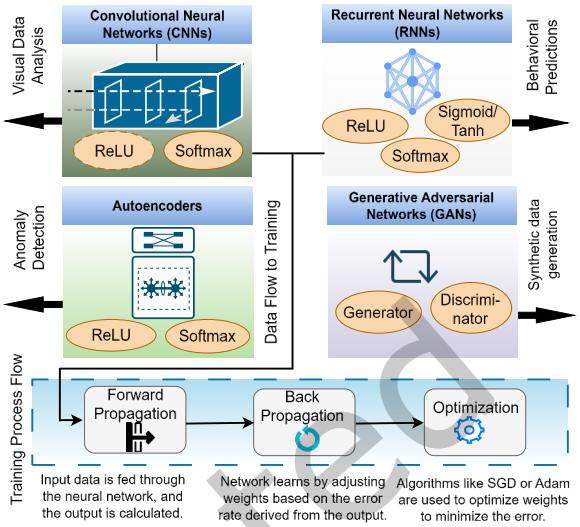

Fig. 15. Core deep-learning architectures for IoV security: key roles and applications.

6.1 Deep Learning Architectures for IoV Security

DL architectures support IoV security by learning from high-dimensional inputs such as images, time series, RF signals, and sensor telemetry. Table 9 summarizes key DL models and their vehicular security applications.

Convolutional neural networks are widely used for spatial data, including visual frames, RF signals, and radar inputs. Nie et al. and Luo et al. show their utility in intrusion detection, spoofing classification, and license plate recognition [105, 118]. Their main advantage is efficient local feature extraction, but practical deployment usually favors compact variants because deeper CNNs often require offloading to cloud or GPU-enabled RSUs. *Recurrent neural networks* and *LSTMs* model temporal patterns in CAN bus traffic and V2X communications. Grover et al. show that gated architectures preserve long-term dependencies for behavior-based threat detection [64]. However, their sequential computation and state maintenance can limit edge efficiency under strict latency constraints. *Autoencoders (AEs)* support unsupervised detection by flagging high reconstruction loss. Ashraf et al. apply AEs to malformed and malicious vehicular traffic [12]. In practice, their usefulness also depends on stable reconstruction thresholds under changing traffic conditions.

Transformer-based models and hybrid CNN-Transformer designs capture local and global patterns in traffic logs. Zhu et al. propose FC-Trans for rare-event detection using attention-based modeling [214]. These architectures are attractive for multimodal fusion and long-range dependency handling, but they remain operationally heavier and less mature for routine OBU-class deployment than lightweight CNN or recurrent models. *Generative adversarial networks* simulate adversarial behavior and enrich rare-attack training data. Xu et al. show that GAN-based trace generation improves generalization [183]. This makes GANs valuable for augmentation, but less straightforward to operationalize than discriminative DL pipelines.

Figure 15 illustrates a typical DL training pipeline, including forward and backward propagation, loss optimization via SGD or Adam, and regularization using dropout, batch normalization, and L_2 norms [88]. Overall, these architectures improve detection capability, but their practical value differs markedly across deployment tiers: compact CNNs, recurrent models, and selective autoencoder pipelines are currently more edge-feasible, whereas transformers and GAN-based systems offer richer modeling at higher runtime and maintenance cost.

Just Accepted

Table 10. IoV security protocols: evolution from traditional to adapted use and core impact.

Refs	Protocol	Traditional Use → IoV Adaptation	Impact
[29]	Digital Cert.	CA-issued web auth → Veh-infra identity vetting	Prevents spoofing; boosts trust
[206]	Asym. Encryption	Email security → Secure V2V handshakes	Strong auth; ↑ compute cost
[136]	TLS	Web channel protection → V2V/V2I data integrity	Stops eavesdropping; ensures confidentiality
[19]	Symm. Encryption	Pre-shared key streams → Real-time vehicle data encryption	Fast encrypt; key distrib. challenge
[6]	Firewall & IDS	Network filtering → DPI-aware IoV traffic inspection	Blocks advanced threats; needs tuning
[83]	Blockchain	Financial ledger → Tamper-proof IoV logs & updates	Immutable records; trust enhancement
[66]	Quantum Crypto	Future-proof comms → Quantum-safe key distribution	Unbreakable encryption; emerging tech

6.2 Applications of DL in Threat Detection and Behavior Analysis

DL models support IoV security across intrusion detection, anomaly analysis, and behavior modeling. This subsection surveys key application domains where DL enhances threat response, pattern recognition, and situational awareness. Table 9 summarizes representative model types, but their practical value differs substantially with respect to latency tolerance, data dependence, and deployment cost.

6.2.1 Intrusion and Threat Detection. DL models detect intrusions, spoofing, malware propagation, and unauthorized access in IoV environments. CNNs process image and radar inputs for monitoring and license plate verification [118], with lightweight variants improving edge feasibility [105]. RNNs and LSTMs analyze telemetry and communication sequences to identify temporal anomalies [64], while autoencoders detect deviations in network traffic indicative of DDoS or malware activity [12]. GANs generate synthetic attack traces to improve robustness against rare threats [183]. In practice, however, these gains are not stable, compact CNN and recurrent models are more readily deployable, whereas GAN-augmented pipelines improve robustness at the cost of greater training complexity and lower operational maturity.

6.2.2 Scalability and Real Time Performance. IoV systems generate high-velocity multimodal data from sensors and communication interfaces. CNN parallelism supports scalable processing across streams [133], while transfer learning reduces training data requirements for domain-specific tasks [120]. These approaches improve scalability, but real-time feasibility still depends on compression, hardware support, and stability across heterogeneous vehicle fleets rather than on model accuracy alone.

6.2.3 Behavioral Modeling and Predictive Analytics. DL models enable predictive security by modeling driving behavior, traffic flow, and communication patterns. Time-series models identify abnormal behavior or communication outliers linked to compromised systems [119, 174]. DL is also integrated into automated response systems such as REACT [68]. These capabilities improve responsiveness, but their reliability depends on whether prediction quality remains stable under drift, sparse labels, and changing traffic contexts.

6.2.4 Reducing False Positives and Alert Fatigue. False positives remain a key limitation in large-scale IoV deployments. DL models, including autoencoders and GAN-based filters, refine anomaly scores and reduce redundant alerts [12]. Although such refinements can improve signal-to-noise ratio for SOCs, the benefit often depends on threshold selection and may not transfer cleanly across datasets or deployment domains.

6.2.5 Hardware Acceleration for Edge DL. Edge deployments use GPUs and NPUs to support real-time inference. Wang et al. report improved latency and energy efficiency using neural accelerators [172]. These advances make edge DL more practical, but they also increase dependence on specialized hardware and do not remove the broader maintenance costs of updating, validating, and coordinating DL models across fleets.

These applications show that DL is most compelling where richer context or multimodal inputs materially improve detection, but its deployment value still depends on whether those gains justify higher model complexity, hardware dependence, and maintenance overhead.

Just Accepted

6.3 Trends in Lightweight and Privacy-Preserving DL

As IoV systems scale, DL research targets edge efficiency and privacy-preserving deployment. This subsection distinguishes deployment-ready directions from techniques that remain promising but operationally heavier.

6.3.1 Model Compression and Edge Optimization. Recent work reduces DL model size and computation through pruning, quantization, and knowledge distillation to meet OBU and RSU latency and energy limits [130, 161]. Bhatia et al. deploy CNNs on constrained devices using depthwise separable convolutions and activation sparsity [21], while Luo et al. show millisecond-level anomaly detection through spectral residual filtering [105]. These methods are among the most deployment-ready DL trends in IoV, although compression is valuable only when it yields measurable runtime and memory gains on target hardware.

6.3.2 Federated and Collaborative Learning. FL reduces privacy risk and transmission overhead by distributing training across RSUs and vehicles. FED-IoV and VAN-FED-IDS enable gradient aggregation without raw data sharing [97, 104]. FL is attractive for privacy-sensitive and cross-domain IoV settings, but its value depends on robust aggregation, synchronization stability, and poisoning resistance under non-IID edge data. Table 10 summarizes their protocol-level contributions.

6.3.3 Online and Continual Learning. Online and continual learning address concept drift by updating DL models as IoV traffic and threat patterns change. Lim et al. explore edge-based incremental updates that reduce delay between data collection and response [97]. Such adaptivity is important for long-lived deployments, but it requires version control, automated validation, and rollback mechanisms to prevent unstable models from propagating across fleets.

6.3.4 Security Protocol Innovations. DL-based security also depends on supporting protocols. Blockchain-anchored logs provide auditable model-output trails [212], while quantum-resistant cryptography and secure firmware delivery aim to connect detection, response, and recovery [19, 136, 206]. These advances improve trust and auditability, but they are less deployment-ready than compression and edge optimization because verification cost, interoperability, and lifecycle management remain major barriers.

Overall, the most practical directions reduce edge cost and preserve privacy without excessive coordination overhead, whereas protocol-heavy designs remain important but comparatively less mature for large-scale IoV deployment.

6.4 Deployment Challenges and Research Opportunities in DL-Based IoV Security

Integrating DL into IoV security requires balancing architectural, computational, and regulatory constraints under real-time conditions. This subsection highlights the main deployment bottlenecks that limit DL effectiveness in IoV, rather than assuming performance gains translate directly into deployable solutions. Table 11 summarizes key limitations and mitigation strategies.

Table 11. Challenges, Impacts, and Solutions for IoV security systems using DL.

Refs	Challenge	Solution	Notes
[172]	↑ Latency	HW/software pipeline optim.	Safety-critical; infra compatibility
[32, 96]	↑ Compute	Model pruning & quantization	Trade-off: accuracy vs. size
[161]	Edge device constraints	Edge-optimized AI accelerators	Requires edge-specific hardware
[130]	↑ Energy use	Low-power model design	Battery-sensitive; lightweight arch.
[104]	↑ Data needs	FL	Privacy-preserving; comms overhead
[104]	Scalability issues	FL	Sync protocols for consistency
[208]	Privacy & bias	Differential privacy & encryption	Compliance critical; bias mitigation
[140]	Continuous updates	Modular update frameworks	Downtime minimization; robust testing
[97]	Model drift	Online monitoring & retraining	Automated anomaly detection

Just Accepted

A primary constraint is *computational efficiency*. DL models such as CNNs and RNNs often exceed OBU processing and power budgets, limiting their use in latency-critical settings. Chen et al. and Prakash et al. show that uncompressed models degrade responsiveness, with delays beyond 100 ms undermining real-time decisions [32, 130, 172]. Optimization techniques, including quantization, pruning, and distillation [96, 161], as well as lightweight architectures such as depthwise convolutions and spectral residual filters [105], improve feasibility. However, their value depends on whether these reductions translate into stable latency gains on target hardware rather than only smaller model size. Offloading inference to RSUs can reduce local load and enable faster responses [64, 119], but its effectiveness depends on communication stability, scheduling overhead, and cross-tier coordination, making it context-dependent rather than a universal solution.

Data privacy and adaptability remain tightly coupled challenges. DL requires diverse training data, yet regulatory and proprietary constraints limit centralization [208]. FL frameworks such as FED-IoV and VAN-FED-IDS address this by aggregating encrypted updates [97, 104], supporting decentralized learning. However, decentralization expands the attack surface. In IoV environments, non-IID data, intermittent connectivity, and participant churn make malicious updates difficult to distinguish from benign drift. Compromised participants may bias gradients or suppress anomalies without exposing raw data. As a result, FL reduces privacy risk while increasing model-integrity risk, requiring robust aggregation, trust-aware weighting, node attestation, update-level anomaly screening, and auditable training logs.

Scalability across heterogeneous devices introduces further constraints. IoV deployments involve mobility, intermittent connectivity, and diverse hardware capabilities. Hardware accelerators (e.g., NPUs, GPUs, ASICs) can restore real-time inference on constrained platforms [21, 172], but system performance depends equally on model placement, scheduling, and communication co-design [151]. Scalability therefore depends not only on adding compute, but on maintaining stable performance across heterogeneous hardware, connectivity, and workloads.

DL-based IoV systems must also support *trustworthy operation*. Techniques such as blockchain-based audit trails, adversarial training, and continuous FL improve traceability and resilience [212]. However, these mechanisms differ in deployment readiness, with lightweight optimization and controlled adaptation being more practical, while fully autonomous, self-defending DL pipelines lack validation under realistic latency, drift, and verification constraints. Reliable over-the-air updates, tamper-evident validation, and continuous resilience testing remain necessary for production systems. Overall, the key challenge is not whether DL improves IoV security, but whether its gains remain reliable under simultaneous constraints on latency, scalability, energy, privacy, and governance.

7 Synergistic Integration of EC, ML, and DL for IoV Security

7.1 Motivation for Integration

While individual technologies, EC, ML, and DL, have advanced IoV security, each presents distinct limitations when deployed in isolation. EC enables low-latency inference by relocating computation to OBUs and RSUs, yet its limited compute power restricts analytic depth [71, 184]. ML models improve detection accuracy, particularly for known threats, but struggle with zero-day attacks and adversarial inputs [59, 213]. DL excels at capturing high-dimensional patterns and temporal anomalies using architectures like LSTM autoencoders and GANs [12, 118], yet these gains are bounded by energy and hardware constraints in vehicular settings.

A combined architecture aligns these technologies to offset their individual constraints. EC provides low-latency local processing for V2X safety operations, ML supports adaptive filtering and policy adjustment at the edge, and DL enables deeper threat understanding through advanced sequence modeling and representation learning. As illustrated in Figure 16, this integration forms a closed cloud–edge security loop where edge nodes perform local inference, filtering, and response, while summarized observations and model updates are propagated to

Just Accepted

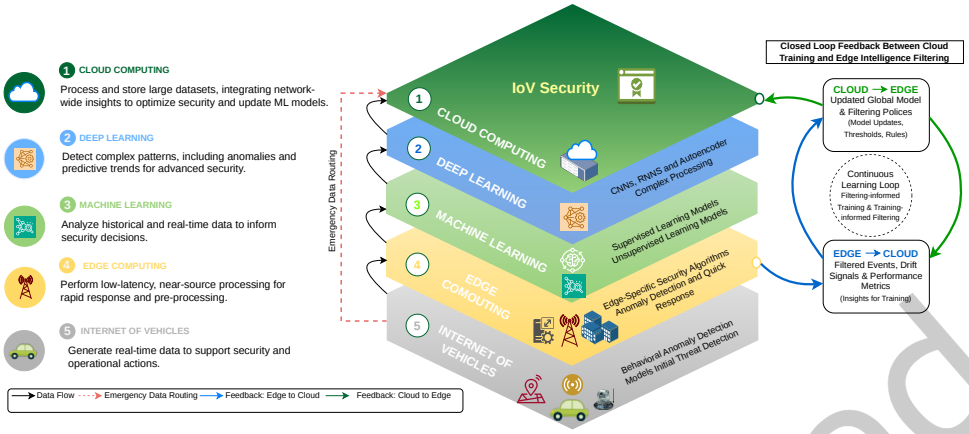

Fig. 16. Integrated cloud-edge feedback loop for adaptive IoV security.

higher layers for aggregation, retraining, and policy refinement. The updated models and control logic are then redistributed to edge nodes for subsequent deployment and mitigation. This tiered workflow localizes immediate response while preserving global learning and coordinated adaptation across the IoV system. The following subsections examine this integration model, its benefits, and its operational challenges.

7.2 System Architecture and Integration Stack

Figure 16 illustrates a four-tier IoV security architecture that integrates EC, ML, and DL into a unified, adaptive defense framework. Each tier contributes complementary strengths, supporting a scalable pipeline from real-time filtering to global orchestration.

At the *edge tier*, OBUs and RSUs execute lightweight anomaly detection, using threshold-based filters and statistical checks to isolate malformed packets or abnormal signal patterns within sub-100 ms latency windows [41]. These initial responses are enhanced at the ML tier, where supervised, unsupervised, and reinforcement models refine alerts and adapt policies in response to traffic dynamics, achieving over 90% precision on known threats [59, 197]. The *DL tier* processes high-dimensional inputs, such as sensor streams and log sequences, using CNNs, RNNs, and autoencoders to detect stealthy or high-complexity threats. GANs are also employed to augment training with synthetic attack traces [12, 118]. Finally, the orchestration tier synchronizes updates across nodes, manages FL cycles, and implements predictive countermeasures based on inferred threat trajectories [174].

This layered architecture enables distributed IoV systems to maintain low latency, high accuracy, and robust coordination. The tiered design ensures modularity and resilience, allowing each computational layer to contribute efficiently to proactive and scalable security enforcement.

7.3 Evaluated Benefits and Security Impact of EC-ML-DL Integration

The combined use of EC, ML, and DL enables IoV security systems to achieve substantial improvements in detection accuracy, responsiveness, bandwidth efficiency, and system scalability. By distributing inference across OBUs, RSUs, and cloud layers, integrated frameworks achieve end to end visibility and adaptivity. Empirical evaluations report that EC-based local filtering reduces sensor stream latency to under 120 ms [166, 184], while ML classifiers detect flow anomalies with 95–99% precision [59, 213]. DL layers such as CNNs and autoencoders further enhance detection of zero-day attacks, achieving over 99% accuracy on benchmark datasets with diverse threat models [168, 189]. Beyond accuracy, integration leads to tangible performance gains. Round-trip latency is

JIST Accepted

Table 12. Key metrics Before vs. After EC+ML/DL integration in IoV.

Refs	Metric	Pre (Cloud Only)	Post (Edge + ML/DL)
[166]	Response time (ms)	$>$ 500 ms	$\approx$ 115 ms
[166]	Power/Tx Cost	High, continuous TX	$\downarrow$ 60$\times$ (local processing)
[2]	Accuracy (%)	$\approx$ 95.2%	$\approx$ 99.2%
[160]	Scalability	Poor, centralized	High, distributed
[110]	Adaptability	Manual tuning	Automatic reconfig.
[148]	Integration complexity	Low; simple setup	High; secure sync

Table 13. Key barriers in IoV integration and concise solutions.

Refs	Barrier	Solutions & Notes
[33, 64, 138, 195]	Interoperability	Define unified protocols; test across platforms; ensure backward compatibility
[102, 128, 137, 146]	Maintenance & Updates	Automate health checks and patching; schedule regular software/hardware audits
[108, 109, 152]	Regulatory	Align with GDPR, CCPA, NIS, NIST; embed compliance checks in workflows
[44, 57, 61, 70]	Industry Standards	Standardize data formats & security specs; adopt ISO/SAE 21434; liaise with regulatory bodies

reduced from over 500 ms to approximately 115 ms by localizing inference at the edge [21, 71], and power-efficient implementations, such as model pruning and quantization, achieve up to 60$\times$ energy savings, preserving EV battery range [165], as detailed in Table 12. Scalability benefits emerge from FL and distributed model updates, which eliminate centralized bottlenecks while complying with data privacy mandates [31, 194]. Additionally, blockchain-anchored logs enforce tamper resistance and prepare the system for post-quantum cryptographic resilience [24, 212].

Proactive defense is another key advantage. DL-based time series models forecast intrusion surges and trigger preemptive mitigation, such as access throttling or node isolation, reducing response delays and improving fleet-wide resilience [126]. Orchestrated playbooks automate these actions, minimizing mean time to respond and increasing overall security readiness [51]. Collectively, these outcomes demonstrate that EC-ML-DL integration is not merely additive but synergistic, achieving sub-second reaction times, privacy preservation, and high detection accuracy that standalone techniques cannot deliver in isolation.

7.4 Integration Challenges and Design Considerations

While the integration of EC, ML, and DL enhances IoV security, it also introduces complex operational and architectural challenges. These challenges span system interoperability, lifecycle maintenance, and regulatory compliance, all of which must be addressed to ensure secure, scalable, and standards-aligned deployments. Table 13 summarizes key barriers and mitigation strategies reported in recent literature.

7.4.1 System Interoperability. Integrated IoV systems often suffer from mismatches in data granularity and representation. Edge-layer devices emit low-dimensional metrics, while DL models require structured, high-dimensional tensors. Without standardized transformation pipelines, these format mismatches can lead to false positives or dropped alerts [64, 138]. Furthermore, legacy communication protocols such as CAN and DSRC complicate AI-driven integration, particularly when aligning inputs across heterogeneous modules [33]. To bridge this gap, recent studies propose adaptive feature conversion pipelines and standard-compliant APIs for secure model interfacing.

7.4.2 Model Maintenance and Lifecycle Management. Security models must continuously adapt to shifting traffic patterns and evolving attack vectors. However, maintaining model relevance across distributed nodes introduces risks related to update validation, backward compatibility, and runtime integrity. Liu et al. [102] and Resende et al. [137] emphasize that poorly synchronized updates or aging hardware can degrade detection accuracy or interrupt safety-critical functions. Emerging DevSecOps pipelines push signed updates over-the-air, while local

Just Accepted

Table 14. Mapping of ML/DL mechanisms to traceability-related compliance functions in IoV.

Mechanism	Primary compliance support
Federated learning	Data minimization; local training; reduced raw-data transfer
Tamper-evident logging / blockchain anchoring	Audit trail; provenance; post-incident verification
Explainable AI	Decision interpretability; accountability; output traceability
Model versioning and signed updates	Model-state reconstruction; deployment traceability
Encrypted inference / secure aggregation	Reduced data exposure during training and inference

health monitors detect degraded or misaligned nodes [56, 146]. FL complements these approaches by enabling local retraining, reducing the reliance on centralized data transfer [128].

7.4.3 Regulatory Compliance and Data Governance. Integrated AI-driven security must operate within the constraints of global data protection regulations such as GDPR, CCPA, and UNECE WP.29 [25, 52, 108, 109, 152]. These mandates require traceability, auditability, and minimal exposure of personal data, particularly for edge-to-cloud data pipelines. Solutions such as differential privacy, encrypted model sharing, and federated inference workflows have been proposed to satisfy legal constraints without undermining analytical accuracy [195]. Aligning these strategies with evolving regulatory frameworks remains an ongoing research and engineering challenge.

Together, these design considerations underscore the need for co-optimized software-hardware stacks, lifecycle-aware update systems, and privacy-centric architectures that can operate reliably under real-world IoV constraints.

7.5 Standardization and Regulatory Compliance in IoV Security

Integrating edge computing, machine learning, and deep learning into IoV security requires alignment with both technical standards and regulatory mandates. Without this alignment, deployments risk interoperability failures, fragmented governance, weak auditability, and non-compliance with cybersecurity and privacy obligations. This subsection summarizes the standards and compliance mechanisms most relevant to integrated IoV security.

7.5.1 Interoperability and Framework Alignment. IoV ecosystems combine heterogeneous OBUs, RSUs, VANETs, and AI-driven security functions that operate across different communication, control, and security protocols. Standards such as ISO/SAE 21434 provide lifecycle-oriented cybersecurity guidance for consistency across devices, interfaces, and vendors [35, 61]. Protocol-level standards such as IEEE 802.11p further support secure, low-latency V2V/V2I communication, which is needed for coordinated edge inference, distributed sensing, and AI-assisted control loops [82].

7.5.2 Privacy, Traceability, and Legal Compliance. IoV platforms must also comply with data protection and cybersecurity regulations such as the GDPR, CCPA, and UNECE WP.29, which require lawful data handling, security by design, traceability, and accountability [52, 108, 109, 152]. In this context, ML and DL techniques should not be treated as generic compliance enablers because each mechanism supports a different regulatory function. FL supports data minimization by keeping raw vehicular data local to OBUs, RSUs, or fleet domains, reducing cross-domain exposure of personally identifiable information. Blockchain-anchored or tamper-evident logs support auditability by preserving verifiable records of model updates, security events, and operational decisions across the edge-to-cloud pipeline. Explainable AI contributes to decision-level traceability by helping operators inspect which signals or features influenced an IDS or anomaly-detection outcome, supporting post-incident review and accountability. However, XAI alone does not establish compliance. Auditable IoV AI requires interpretability to be combined with secure logging, model versioning, signed update provenance, and human oversight so that investigators can reconstruct how a decision was generated and deployed. Table 14 summarizes this mapping.

Just Accepted

Table 15. Edge-computing case studies in IoV security: Entities, tech, and core impacts.

Ref	Entity	Tech	Impact & Applications
[129]	Porsche	FogHorn EC	Multi-factor auth; traffic optimization; predictive maintenance; V2H infotainment
[167]	Volvo	EC-driven collision avoidance	Real-time safety decisions; "Safe Space" accident prevention
[89]	Barcelona (Smart City)	IoT+EC	Congestion reduction; adaptive traffic lights
[36]	Shanghai (Smart City)	Intersection EC	Smooth traffic flow; real-time signal control

Table 16. DL application domains in IoV security.

Ref	Domain	Implementation	Benefit
[64, 118, 126]	Network Security	CNN/LSTM monitoring	Ensures comms integrity
[153, 177]	Autonomous Vehicles	Sensor-data DL models	Reduces accidents and breaches
[63]	Traffic Mgmt	Flow-analysis networks	Minimizes disruptions
[54, 147, 169]	Surveillance	Video-analytics CNNs	Improves incident response

Table 17. ML case studies in IoV security: approach, outcome, and lesson.

Ref	Approach	Outcome	Lesson
[192]	Continuous learning framework	Real-time mitigation of simulated attacks	Ongoing model adaptation is critical
[5]	Sensor-data predictive modeling	Enhanced safety; reduced downtime	ML adds operational efficiency beyond security
[154]	Real-time traffic-pattern analysis	Optimized flow; lower delays	ML supports broader IoV ecosystem management
[99]	Automated detection and isolation	Contained threat spread swiftly	Automation dramatically improves response time

7.5.3 Security and Real-Time Processing Standards. Cybersecurity risk management frameworks such as ISO 27001 and NIST SP 800-53 define baseline practices for confidentiality, integrity, and availability in AI-assisted systems [79, 115]. In IoV, these controls must coexist with low-latency processing and safety-sensitive decision paths. Emerging standards such as IEEE P2418.5 and ISO/TC 307 further support blockchain-based trust management and tamper-evident logging, enabling decentralized accountability in edge-assisted vehicular environments [76, 78].

7.5.4 Toward AI-Specific IoV Standards. As AI becomes integral to vehicular security, future standards must address explainability, adversarial robustness, model-update governance, and trust in autonomous decision pipelines. The literature therefore points toward domain-specific compliance frameworks that connect AI lifecycle governance with real-time vehicular constraints rather than treating them as separate concerns [44, 108]. Table 12 and Table 13 further illustrate the trade-offs among performance, privacy, and standard conformance in current IoV deployments.

8 Deployment Experiences and Lessons from EC, ML, and DL in IoV

8.1 Use Cases of EC, ML, and DL Technologies

EC, ML, and DL are now used in practical IoV deployments rather than only as conceptual security tools. Table 15 and Table 16 summarize representative automotive and smart-city implementations.

In *vehicle-centric deployments*, Porsche and FogHorn use EC modules for offline multimodal biometric authentication, secure keyless entry, and predictive diagnostics without continuous cloud dependence [129]. Volvo's Safe Space system applies onboard EC to fuse LiDAR, radar, and camera data for automated braking within 50 ms [167]. Autonomous fleets have also trialed CNN-LSTM models for obstacle detection and spoofed-signal mitigation, with Waymo reporting safety improvements [153, 177]. ML-based intrusion detection and predictive maintenance are similarly moving toward deployment: Yang et al. [192] and Adi et al. [5] show adaptive retraining for zero-day threats and fault prediction. Related examples include traffic-flow optimization [154] and automated vehicle isolation after intrusion detection [99]. Table 17 summarizes these ML case studies and their main operational lessons.

Just Accepted

Table 18. Research areas in AI-powered IoV security: core challenges and key questions.

Area	Core Challenges	Key Research Question
Deployment-aware and cross-layer security architectures	Compute efficiency; split inference; orchestration stability; heterogeneous hardware; validation under mobility and loss	Can one cross-layer policy sustain high accuracy, sub-100 ms response, and practical energy efficiency across OBUs and RSUs?
Explainable and auditable security AI	Runtime explainability; regulator-meaningful auditing; provenance tracking; rollback and governance	How can IoV IDSs provide auditable, regulator-meaningful explanations without exposing proprietary models or violating edge latency limits?
Robust and privacy-preserving collaborative threat intelligence	Adversarial robustness; poisoning resistance; privacy leakage; cross-domain trust; timely fleet-scale sharing	How can collaborative threat intelligence remain timely, auditable, poisoning-resilient, and privacy-preserving at fleet scale?
Next-generation cryptography	Post-quantum transition; handshake latency; verification cost; secure inference overhead; interoperability with legacy V2X	Can hybrid post-quantum authentication and secure inference fit vehicular latency budgets without overwhelming constrained OBUs?

Urban and infrastructure-focused deployments show a similar pattern. Barcelona, Singapore, and Wuxi use intersection-level EC nodes with lightweight ML for adaptive signal control, congestion reduction, and autonomous coordination [36, 89, 210]. Vienna and Rome apply DL-driven surveillance for suspicious activity and road-anomaly detection [63], while CNN/LSTM-based IDS platforms monitor CAN traffic and V2X logs for anomalous behavior [64, 118]. Integrated EC-ML-DL deployments combine these benefits: EC with lightweight ML has supported in-vehicle intrusion response and reduced cyberattack success in fleet trials [205], while EC-enhanced RNNs and RL models have secured V2X channels at intersections with reported sub-100 ms response and improved threat isolation [101, 168].

Together, these cases show that intelligent IoV security is most mature where local inference, adaptive learning, and cloud-edge coordination are matched to concrete vehicular or infrastructure constraints.

8.2 Lessons Learned from Real-World Deployments

Real-world deployments highlight three recurring requirements for EC-, ML-, and DL-enabled IoV security: low-latency local response, continuous adaptation, and deployable governance.

First, edge processing is essential for real-time protection. Across vehicle and infrastructure scenarios, sub-100 ms response is mainly achieved through local ML filtering and DL inference, which reduce cloud dependence, bandwidth use, and exposure of sensitive data [64, 167, 168].

Second, protection must adapt after deployment. Retraining pipelines, automated updates, and FL frameworks help address changing traffic patterns and adversarial behavior [61, 192]. However, adaptation must be hardware-aware: OBU-class platforms require structured pruning, low-bit quantization, compact models, or split inference, whereas RSUs can support heavier models and mixed-precision execution under less restrictive power and memory limits [146].

Third, scale introduces interoperability and governance constraints. Heterogeneous ECUs, RSUs, and cloud services require standardized data formats, communication protocols, and secure APIs for coordinated defense [8, 205]. Privacy-preserving analytics and end-to-end encryption remain necessary for regulatory compliance and user trust [159]. Thus, practical IoV security depends not only on detection accuracy, but also on modularity, explainability, hardware fit, and regulatory alignment.

9 Future Directions and Research Opportunities

AI-enabled IoV systems expand defensive capability while extending the attack surface and tightening deployment constraints. The key research challenge is no longer whether AI improves IoV security, but which combinations of intrusion detection, privacy protection, and trust mechanisms can operate under strict latency, resource, and governance limits. Table 18 summarizes the main open challenges, including trade-offs among accuracy, latency, poisoning resilience, explainability, and deployment feasibility.

Just Accepted

9.1 Deployment-Aware and Cross-Layer Security Architectures

Edge NPUs can deliver several TOPS under tight power budgets, yet full-precision DL models still exceed the compute, memory, and thermal limits of many OBUs in dense traffic. Compression is therefore a deployment requirement, not merely an optimization. Structured pruning, low-bit quantization, compact backbones, and knowledge distillation are the most practical options for OBU-class hardware because they reduce latency and memory overhead while remaining compatible with embedded runtimes. RSUs can support larger models, mixed-precision execution, or split inference, but their gains remain bounded by bandwidth variability and synchronization cost.

Future IoV security architectures must coordinate sensing, inference, retraining, and trust enforcement across vehicles, RSUs, edge servers, and cloud backends rather than optimize each layer separately. Near-term progress is more likely to come from deployment-aware compression, split inference, event-triggered execution, and simplified orchestration policies than from increasingly large end-to-end models. Fully adaptive partitioning across vehicles, RSUs, and cloud tiers, combined with dynamic resource balancing and end-to-end cryptographic coordination, remains promising but harder to validate under mobility, packet loss, heterogeneous hardware, and certification constraints.

Open question. Can one cross-layer deployment policy jointly sustain high detection accuracy, sub-100 ms response, and practical energy efficiency across heterogeneous OBU and RSU hardware without sacrificing coordination reliability?

9.2 Explainable & Auditable Security AI

Opaque IDS decisions are difficult to justify in safety-critical environments, especially when false positives can block legitimate vehicular functions. Regulatory pressure is therefore shifting evaluation from detection accuracy alone toward auditable decision pipelines that support incident review, accountability, and model governance.

Future work should prioritize lightweight explanations, model provenance, and rollback mechanisms that operate within edge latency budgets. Counterfactual analysis and blockchain-anchored provenance are useful for forensic reconstruction, but only if they remain interpretable, low-overhead, and compatible with proprietary deployment constraints. XAI is therefore most credible when paired with logging, version control, and human-review workflows rather than treated as a standalone compliance solution.

Open question. How can XAI-enabled IoV IDSs provide auditable and regulator-meaningful explanations without exposing proprietary models or violating edge latency limits?

9.3 Robust and Privacy-Preserving Collaborative Threat Intelligence

Adversarial patch attacks, CAN-bus poisoning, and membership inference show that IoV security models can fail through manipulated confidence, corrupted training signals, and privacy leakage, not only through lower accuracy. In collaborative settings, mobility, non-IID data, intermittent participation, and cross-domain trust make it harder to separate benign drift from malicious behavior. Centralized SOC pipelines also struggle with fleet-scale telemetry, while fragmented OEM and operator platforms limit cross-domain threat visibility.

Near-term defenses should therefore emphasize lightweight adversarial training, robust federated aggregation, privacy-preserving updates, hierarchical federated IDSs, and standardized threat-sharing formats that reduce raw-data exposure while improving situational awareness. More ambitious mechanisms, including blockchain-based incentives and fully automated smart-contract remediation, remain useful but operationally heavier, especially where latency, policy disputes, and chain growth must be tightly controlled. The main challenge is not sharing more intelligence, but sharing it with enough trust, timeliness, and governance to remain useful under attack.

Open question. How can cross-domain threat intelligence remain timely, auditable, poisoning-resilient, and privacy-preserving at fleet scale without introducing excessive coordination or latency overhead?

Just Accepted

9.4 Next-Generation Cryptography

Conventional public-key schemes can satisfy current latency requirements, but they do not provide long-term post-quantum assurance. IoV systems therefore need cryptographic agility without handshake, storage, or verification costs that exceed vehicular edge budgets.

Lattice-based signatures and hybrid post-quantum schemes are becoming more relevant as recent implementations, including verification on Cortex-A55-class processors, move closer to deployment feasibility. Efficient homomorphic inference and hybrid credential designs are also promising for privacy-preserving intrusion detection, but near future adoption will likely remain limited to selected functions unless verification cost, key size, and interoperability improve.

Open question. Can hybrid post-quantum authentication and secure inference be deployed within vehicular latency budgets without overwhelming constrained OBUs and legacy V2X stacks?

Meeting these challenges will depend less on isolated algorithmic gains than on credible deployment trade-offs across latency, privacy, robustness, auditability, and cryptographic longevity.

10 Conclusion

In this survey, we have examined how EC, ML, and DL technologies, individually and in concert, can address the unique security challenges of the IoV. EC brings critical low latency, localized processing that shrinks the attack surface and enables real time anomaly filtering. ML contributes adaptive, data driven detection of both known and novel threats, while DL unlocks high-dimensional pattern recognition for subtle or zero-day attack signatures. Our comparative analysis demonstrated that no single technology suffices: only a layered EC-ML-DL stack can deliver sub-10 ms response, > 99% detection accuracy, and scalable, privacy preserving operation. Real world case studies from automotive OEMs and smart cities confirm the feasibility and benefits of these integrations, keyless edge authentication at Porsche, millisecond scale collision avoidance at Volvo, adaptive traffic control in Barcelona, and fleet wide intrusion shields in autonomous vehicles. Lessons learned underscore the importance of robust data governance, interoperable protocols, and continuous model adaptation to keep pace with evolving threats. Additionally, IoV security must overcome resource constraints, ensure explainability, and achieve resilience against adversarial and quantum era attacks. Promising research avenues include federated and event driven edge learning, post quantum cryptography tailored to V2X, and blockchain anchored audit trails for model integrity. By charting these directions, we aim to provide researchers and practitioners with a roadmap for building the next generation of secure, efficient, and intelligent IoV systems, capable of safeguarding connected transportation ecosystems.

Just Accepted

References

[1] Ghada Abdelmoumin et al. 2022. On the Performance of Machine Learning Models for Anomaly-Based Intelligent Intrusion Detection Systems for the Internet of Things. *IEEE Internet of Things Journal* 9, 6 (March 2022), 4280–4290.

[2] Abebe Abeshu et al. 2018. Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing. *IEEE Communications Magazine* 56, 2 (Feb. 2018), 169–175.

[3] Mariam M. N. Aboelwafa et al. 2020. A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. *IEEE Internet of Things Journal* 7, 9 (Sept. 2020), 8462–8471.

[4] Amine Abouaomar et al. 2021. Resource Provisioning in Edge Computing for Latency-Sensitive Applications. *IEEE Internet of Things Journal* 8, 14 (July 2021), 11088–11099.

[5] Erwin Adi et al. 2020. Machine learning and data analytics for the IoT. *Neural Computing and Applications* 32, 20 (May 2020), 16205–16233.

[6] Tejasvi Alladi et al. 2021. Artificial Intelligence (AI)-Empowered Intrusion Detection Architecture for the Internet of Vehicles. *IEEE Wireless Communications* 28, 3 (June 2021), 144–149.

[7] Mohammed Almehdhar et al. 2024. Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems for Intelligent Vehicle Networks. *IEEE Open Journal of Vehicular Technology* 5 (2024), 869–906.

[8] Ricardo S. Alonso et al. 2020. Deep Reinforcement Learning for the Management of Software-Defined Networks and Network Function Virtualization in an Edge-IoT Architecture. *Sustainability* 12, 14 (July 2020), 5706.
[9] Adel Alshamrani et al. 2019. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys & Tutorials* 21, 2 (2019), 1851–1877.
[10] Maram Alsharif et al. 2021. Study of Machine Learning for Cloud Assisted IoT Security as a Service. *Sensors* 21, 4 (Feb. 2021), 1034.
[11] Muhammad Naveed Aman et al. 2021. A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles. *IEEE Internet of Things Journal* 8, 2 (Jan. 2021), 1123–1139.
[12] Javed Ashraf et al. 2021. Novel Deep Learning-Enabled LSTM Autoencoder Architecture for Discovering Anomalous Events From Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems* 22, 7 (July 2021), 4507–4518.
[13] Muhammad Aslam et al. 2022. Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT. *Sensors* 22, 7 (March 2022), 2697.
[14] Upstream Auto. 2023. 2023 Automotive Cybersecurity Report. https://upstream.auto/reports/2023report/ Accessed: 2024-07.
[15] Amin Azmoodeh et al. 2017. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *Journal of Ambient Intelligence and Humanized Computing* 9, 4 (Aug. 2017), 1141–1152.
[16] Palak Bagga et al. 2021. On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System. *IEEE Transactions on Vehicular Technology* 70, 2 (Feb. 2021), 1736–1751.
[17] Chandra Bajracharya et al. 2022. Performance Evaluation for Secure Communications in Mobile Internet of Vehicles With Joint Reactive Jamming and Eavesdropping Attacks. *IEEE Transactions on Intelligent Transportation Systems* 23, 11 (Nov. 2022), 22563–22570.
[18] Masoud Barati et al. 2020. GDPR Compliance Verification in Internet of Things. *IEEE Access* 8 (2020), 119697–119709.
[19] Deebak B.D. et al. 2020. A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. *Ad Hoc Networks* 97 (Feb. 2020), 102022.
[20] Showkat Ahmad Bhat et al. 2020. Edge Computing and Its Convergence With Blockchain in 5G and Beyond: Security, Challenges, and Opportunities. *IEEE Access* 8 (2020), 205340–205373.
[21] Surbhi Bhatia et al. 2022. Improved Multimedia Object Processing for the Internet of Vehicles. *Sensors* 22, 11 (May 2022), 4133.
[22] Abdelwahab Boualouache et al. 2023. A Survey on Machine Learning-Based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks. *IEEE Communications Surveys & Tutorials* 25, 2 (2023), 1128–1172.
[23] Amira Bourechak et al. 2023. At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives. *Sensors* 23, 3 (Feb. 2023), 1639.
[24] Sadaf Bukhari et al. 2024. Dynamic Fine-grained SLA Management for 6G eMBB-plus Slice using mDNN & Smart Contracts. *IEEE Transactions on Services Computing* (2024), 1–14.
[25] California State Legislature. 2018. California Consumer Privacy Act (CCPA) – Assembly Bill No. 375. https://oag.ca.gov/privacy/ccpa Accessed: 2024-02-19.
[26] Xingjian Cao et al. 2023. PerFED-GAN: Personalized Federated Learning via Generative Adversarial Networks. *IEEE Internet of Things Journal* 10, 5 (March 2023), 3749–3762.
[27] Chuan Chen et al. 2019. A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles. *IEEE Transactions on Vehicular Technology* 68, 9 (Sept. 2019), 9110–9121.
[28] Chen Chen et al. 2021. An Edge Traffic Flow Detection Scheme Based on Deep Learning in an Intelligent Transportation System. *IEEE Transactions on Intelligent Transportation Systems* 22, 3 (March 2021), 1840–1852.
[29] Chien-Ming Chen et al. 2019. A Secure Authentication Protocol for Internet of Vehicles. *IEEE Access* 7 (2019), 12047–12057.
[30] Jiageng Chen et al. 2018. Special Issue on Advanced Persistent Threat. *Future Generation Computer Systems* 79 (Feb. 2018), 243–246.
[31] Jiasi Chen et al. 2019. Deep Learning With Edge Computing: A Review. *Proc. IEEE* 107, 8 (Aug. 2019), 1655–1674.
[32] Yanjiao Chen et al. 2020. Deep Learning on Mobile and Embedded Devices: State-of-the-art, Challenges, and Future Directions. *Comput. Surveys* 53, 4 (Aug. 2020), 1–37.
[33] Xiongwen Cheng et al. 2019. Space/Aerial-Assisted Computing Offloading for IoT Applications: A Learning-Based Approach. *IEEE Journal on Selected Areas in Communications* 37, 5 (May 2019), 1117–1129.
[34] Haruna Chiroma et al. 2021. Deep Learning-Based Big Data Analytics for Internet of Vehicles: Taxonomy, Challenges, and Research Directions. *Mathematical Problems in Engineering* 2021 (Nov. 2021), 1–20.
[35] Young-June Choi et al. 2017. Special issue on V2X communications and networks. *Journal of Communications and Networks* 19, 3 (2017), 205–208.
[36] Cities Forum. 2023. What Made Shanghai the World's No. 1 Smart City. https://www.citiesforum.org/news/what-made-shanghai-the-worlds-no-1-smart-city Accessed: 2024-08-03.
[37] Mauro Conti et al. 2016. A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials* 18, 3 (2016), 2027–2051.
[38] Gianpiero Costantino et al. 2022. In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards. *IEEE Communications Standards Magazine* 6, 1 (March 2022), 84–92.

Just Accepted

[39] Guangming Cui et al. 2022. Efficient Verification of Edge Data Integrity in Edge Computing Environment. *IEEE Transactions on Services Computing* 15, 6 (Nov. 2022), 3233–3244.
[40] Jie Cui et al. 2018. Privacy-Preserving Authentication Using a Double Pseudonym for Internet of Vehicles. *Sensors* 18, 5 (May 2018), 1453.
[41] Laizhong Cui et al. 2020. A Decentralized and Trusted Edge Computing Platform for Internet of Things. *IEEE Internet of Things Journal* 7, 5 (May 2020), 3910–3922.
[42] Laizhong Cui et al. 2021. A Blockchain-Based Containerized Edge Computing Platform for the Internet of Vehicles. *IEEE Internet of Things Journal* 8, 4 (Feb. 2021), 2395–2408.
[43] Cheng Dai et al. 2020. A Low-Latency Object Detection Algorithm for the Edge Devices of IoV Systems. *IEEE Transactions on Vehicular Technology* 69, 10 (Oct. 2020), 11169–11178.
[44] Wenbin Dai et al. 2019. Industrial Edge Computing: Enabling Embedded Intelligence. *IEEE Industrial Electronics Magazine* 13, 4 (Dec. 2019), 48–56.
[45] Yueyue Dai et al. 2019. Artificial Intelligence Empowered Edge Computing and Caching for Internet of Vehicles. *IEEE Wireless Communications* 26, 3 (June 2019), 12–18.
[46] Tasneem S. J. Darwish et al. 2018. Fog Based Intelligent Transportation Big Data Analytics in The Internet of Vehicles Environment: Motivations, Architecture, Challenges, and Critical Issues. *IEEE Access* 6 (2018), 15679–15701.
[47] Sagar Dasgupta et al. 2022. A Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles. *IEEE Transactions on Intelligent Transportation Systems* 23, 12 (Dec. 2022), 23559–23572.
[48] Shuiguang Deng et al. 2020. Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence. *IEEE Internet of Things Journal* 7, 8 (2020), 7457–7469.
[49] Hamza Djigal et al. 2022. Machine and Deep Learning for Resource Allocation in Multi-Access Edge Computing: A Survey. *IEEE Communications Surveys & Tutorials* 24, 4 (2022), 2449–2494.
[50] Shi Dong et al. 2021. Network Abnormal Traffic Detection Model Based on Semi-Supervised Deep Reinforcement Learning. *IEEE Transactions on Network and Service Management* 18, 4 (Dec. 2021), 4197–4212.
[51] Marwa A. Elsayed et al. 2020. PredictDeep: Security Analytics as a Service for Anomaly Detection and Prediction. *IEEE Access* 8 (2020), 45184–45197.
[52] European Parliament and Council of the European Union. 2016. General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679. https://gdpr-info.eu/ Accessed: 2024-02-19.
[53] Yuqi Fan et al. 2021. DR-BFT: A consensus algorithm for blockchain-based multi-layer data integrity framework in dynamic edge computing system. *Future Generation Computer Systems* 124 (Nov. 2021), 33–48.
[54] Cherine Fathy et al. 2022. Integrating Deep Learning-Based IoT and Fog Computing with Software-Defined Networking for Detecting Weapons in Video Surveillance Systems. *Sensors* 22, 14 (July 2022), 5075. doi:10.3390/s22145075
[55] Tiago M. Fernandez-Carames. 2020. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet of Things Journal* 7, 7 (July 2020), 6457–6480.
[56] Mohamed Amine Ferrag et al. 2021. Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis. *IEEE Access* 9 (2021), 138509–138542.
[57] Mohamed Amine Ferrag et al. 2022. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access* 10 (2022), 40281–40306.
[58] Wenliang Fu et al. 2016. A practical intrusion detection system for Internet of vehicles. *China Communications* 13, 10 (Oct. 2016), 263–275.
[59] Ying Gao et al. 2018. A Novel Semi-Supervised Learning Approach for Network Intrusion Detection on Cloud-Based Robotic System. *IEEE Access* 6 (2018), 50927–50938.
[60] Ivan Garcia-Magarino et al. 2019. Security in Vehicles With IoT by Prioritization Rules, Vehicle Certificates, and Trust Management. *IEEE Internet of Things Journal* 6, 4 (Aug. 2019), 5927–5934.
[61] Sahil Garg et al. 2021. Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities. *IEEE Network* 35, 5 (Sept. 2021), 298–305.
[62] Maoguo Gong et al. 2023. Self-Paced Co-Training of Graph Neural Networks for Semi-Supervised Node Classification. *IEEE Transactions on Neural Networks and Learning Systems* 34, 11 (Nov. 2023), 9234–9247.
[63] PTV Group. 2024. AI in traffic management systems: How Artificial Intelligence is Shaping the Future of Mobility. https://www.ptvgroup.com/en/application-areas/ai-in-transportation Accessed: 2024-08.
[64] Harsh Grover et al. 2021. Edge Computing and Deep Learning Enabled Secure Multitier Network for Internet of Vehicles. *IEEE Internet of Things Journal* 8, 19 (Oct. 2021), 14787–14796.
[65] Li Guo et al. 2021. Optimal Allocation of False Data Injection Attacks for Networked Control Systems With Two Communication Channels. *IEEE Transactions on Control of Network Systems* 8, 1 (March 2021), 2–14.

Just Accepted

[66] Daya Sagar Gupta et al. 2022. Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles. *IEEE Transactions on Vehicular Technology* 71, 3 (March 2022), 3255–3266.
[67] Sohan Gyawali et al. 2020. Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks. *IEEE Transactions on Vehicular Technology* 69, 8 (Aug. 2020), 8871–8885.
[68] Mohammad Hamad et al. 2024. REACT: Autonomous intrusion response system for intelligent vehicles. *Computers & Security* 145 (2024), 104008.
[69] Brian Haugli. 2023. Electric vehicles are taking over. Hackers are waiting. https://www.securitymagazine.com/articles/97461-electric-vehicles-are-taking-over-hackers-are-waiting Accessed: 2024-08.
[70] Ying He et al. 2021. Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning Approach. *IEEE Internet of Things Journal* 8, 4 (Feb. 2021), 2226–2237.
[71] Xiangwang Hou et al. 2020. Reliable Computation Offloading for Edge-Computing-Enabled Software-Defined IoV. *IEEE Internet of Things Journal* 7, 8 (Aug. 2020), 7097–7111.
[72] Rui Huang et al. 2022. Quantum Federated Learning With Decentralized Data. *IEEE Journal of Selected Topics in Quantum Electronics* 28, 4 (July 2022), 1–10.
[73] Xumin Huang et al. 2018. Secure Roadside Unit Hotspot Against Eavesdropping Based Traffic Analysis in Edge Computing Based Internet of Vehicles. *IEEE Access* 6 (2018), 62371–62383.
[74] Mamoona Humayun et al. 2021. Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal* 22, 1 (March 2021), 105–117.
[75] Fatima Hussain et al. 2020. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials* 22, 3 (2020), 1686–1721.
[76] IEEE. 2024. IEEE Draft Guide for Blockchain in Power and Energy Systems. *IEEE P2418.5/D1.0, May 2024* (2024), 1–98.
[77] MohammadNoor Injadat et al. 2021. Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection. *IEEE Transactions on Network and Service Management* 18, 2 (June 2021), 1803–1816.
[78] International Organization for Standardization (ISO). 2024. ISO/TC 307: Blockchain and Distributed Ledger Technologies Committee. https://www.iso.org/committee/6266604.html Accessed: 2024-02-19.
[79] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 2022. ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en Accessed: 2024-02-19.
[80] International Organization for Standardization (ISO) and Society of Automotive Engineers (SAE). 2021. ISO/SAE 21434: Road Vehicles – Cybersecurity Engineering. https://www.iso.org/obp/ui/en/#iso:std:iso-sae:21434:ed-1:v1:en Accessed: 2024-02-19.
[81] Uzair Javaid et al. 2021. A Secure and Scalable Framework for Blockchain Based Edge Computation Offloading in Social Internet of Vehicles. *IEEE Transactions on Vehicular Technology* 70, 5 (May 2021), 4022–4036.
[82] Daniel Jiang and Luca Delgrossi. 2008. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In *VTC Spring 2008-IEEE vehicular technology conference*. IEEE, 2036–2040.
[83] Tigang Jiang et al. 2019. Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis. *IEEE Internet of Things Journal* 6, 3 (June 2019), 4640–4649.
[84] Zhiyang Ju et al. 2020. Distributed Deception Attack Detection in Platoon-Based Connected Vehicle Systems. *IEEE Transactions on Vehicular Technology* 69, 5 (May 2020), 4609–4620.
[85] Satya Katragadda et al. 2020. Detecting Low-Rate Replay-Based Injection Attacks on In-Vehicle Networks. *IEEE Access* 8 (2020), 54979–54993.
[86] Eshaan Khanapuri et al. 2023. Learning Based Longitudinal Vehicle Platooning Threat Detection, Identification and Mitigation. *IEEE Transactions on Intelligent Vehicles* 8, 1 (Jan. 2023), 290–300.
[87] Xiangjie Kong et al. 2022. Edge Computing for Internet of Everything: A Survey. *IEEE Internet of Things Journal* 9, 23 (Dec. 2022), 23472–23485.
[88] Yann LeCun et al. 2015. Deep learning. *Nature* 521, 7553 (May 2015), 436–444.
[89] Lenovo. 2021. Inside Barcelona, the 5G Smart City of the Future. https://www.lenovo.com/us/en/servers-storage/smart-city-barcelona/ Accessed: 2024-08.
[90] Bo Li et al. 2021. Auditing Cache Data Integrity in the Edge Computing Environment. *IEEE Transactions on Parallel and Distributed Systems* 32, 5 (May 2021), 1210–1223.
[91] Bo Li et al. 2022. Inspecting Edge Data Integrity With Aggregate Signature in Distributed Edge Computing Environment. *IEEE Transactions on Cloud Computing* 10, 4 (Oct. 2022), 2691–2703.
[92] Fangyu Li et al. 2019. System Statistics Learning-Based IoT Security: Feasibility and Suitability. *IEEE Internet of Things Journal* 6, 4 (Aug. 2019), 6396–6403.
[93] Jiabin Li et al. 2021. RTED-SD: A Real-Time Edge Detection Scheme for Sybil DDoS in the Internet of Vehicles. *IEEE Access* 9 (2021), 11296–11305.

Just Accepted

[94] Xinghua Li et al. 2021. Transfer learning based intrusion detection scheme for Internet of vehicles. *Information Sciences* 547 (Feb. 2021), 119–135.
[95] Xinghua Li et al. 2022. CAN Bus Messages Abnormal Detection Using Improved SVDD in Internet of Vehicles. *IEEE Internet of Things Journal* 9, 5 (March 2022), 3359–3371.
[96] Tailin Liang et al. 2021. Pruning and quantization for deep neural network acceleration: A survey. *Neurocomputing* 461 (Oct. 2021), 370–403.
[97] Wei Yang Bryan Lim et al. 2021. Towards Federated Learning in UAV-Enabled Internet of Vehicles: A Multi-Dimensional Contract-Matching Approach. *IEEE Transactions on Intelligent Transportation Systems* 22, 8 (Aug. 2021), 5140–5154.
[98] Li Lin et al. 2019. Computation Offloading Toward Edge Computing. *Proc. IEEE* 107, 8 (Aug. 2019), 1584–1607.
[99] Qiang Liu et al. 2018. A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View. *IEEE Access* 6 (2018), 12103–12117.
[100] Rui Liu et al. 2024. CRS: A Privacy-Preserving Two-Layered Distributed Machine Learning Framework for IoV. *IEEE Internet of Things Journal* 11, 1 (Jan. 2024), 1080–1095.
[101] Shaoshan Liu et al. 2019. Edge Computing for Autonomous Driving: Opportunities and Challenges. *Proc. IEEE* 107, 8 (Aug. 2019), 1697–1716.
[102] Xiaolan Liu et al. 2020. Resource Allocation With Edge Computing in IoT Networks via Machine Learning. *IEEE Internet of Things Journal* 7, 4 (April 2020), 3415–3426.
[103] Yaqiong Liu et al. 2020. Toward Edge Intelligence: Multiaccess Edge Computing for 5G and Internet of Things. *IEEE Internet of Things Journal* 7, 8 (Aug. 2020), 6722–6747.
[104] Yunlong Lu et al. 2020. Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles. *IEEE Transactions on Vehicular Technology* 69, 4 (April 2020), 4298–4311.
[105] Feng Luo et al. 2025. An anomaly detection model for in-vehicle networks based on lightweight convolution with spectral residuals. *Computers & Security* 151 (2025), 104304.
[106] Rishikesh Magar et al. 2022. Crystal twins: self-supervised learning for crystalline material property prediction. *npj Computational Materials* 8, 1 (Nov. 2022), 1–8.
[107] Shalaka S Mahadik et al. 2023. Edge-HetIoT defense against DDoS attack using learning techniques. *Computers & Security* 132 (2023), 103347.
[108] Alessandro Mantelero et al. 2020. The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology* 28, 4 (Dec. 2020), 297–328.
[109] Dimitra Markopoulou et al. 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review* 35, 6 (Nov. 2019), 105336.
[110] Mario Merone et al. 2022. A Practical Approach to the Analysis and Optimization of Neural Networks on Embedded Systems. *Sensors* 22, 20 (Oct. 2022), 7807.
[111] Alekha Kumar Mishra et al. 2019. Analytical Model for Sybil Attack Phases in Internet of Things. *IEEE Internet of Things Journal* 6, 1 (Feb. 2019), 379–387.
[112] Muhammad Baqer Mollah et al. 2021. Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey. *IEEE Internet of Things Journal* 8, 6 (March 2021), 4157–4185.
[113] Viraaji Mothukuri et al. 2022. Federated-Learning-Based Anomaly Detection for IoT Security Attacks. *IEEE Internet of Things Journal* 9, 4 (Feb. 2022), 2545–2554.
[114] M. G. Sarwar Murshed et al. 2021. Machine Learning at the Network Edge: A Survey. *Comput. Surveys* 54, 8 (Oct. 2021), 1–37.
[115] National Institute of Standards and Technology (NIST). 2020. *NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations.* Technical Report. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf Accessed: 2024-02-19.
[116] National Institute of Standards and Technology (NIST). 2023. *NIST Cybersecurity White Paper: IoT Device Cybersecurity Guidance for the Federal Government.* Technical Report. National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf Accessed: 2024-08.
[117] Yuanzhi Ni et al. 2020. Toward Reliable and Scalable Internet of Vehicles: Performance Analysis and Resource Management. *Proc. IEEE* 108, 2 (Feb. 2020), 324–340.
[118] Laisen Nie et al. 2020. Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method. *IEEE Transactions on Network Science and Engineering* 7, 4 (Oct. 2020), 2219–2230.
[119] Zhaolong Ning et al. 2019. Deep Learning in Edge of Vehicles: Exploring Trirelationship for Data Transmission. *IEEE Transactions on Industrial Informatics* 15, 10 (Oct. 2019), 5737–5746.
[120] Zhaolong Ning et al. 2021. Intelligent Edge Computing in Internet of Vehicles: A Joint Computation Offloading and Caching Solution. *IEEE Transactions on Intelligent Transportation Systems* 22, 4 (April 2021), 2212–2225.

Just Accepted

[121] Zhaolong Ning et al. 2021. Joint Computing and Caching in 5G-Envisioned Internet of Vehicles: A Deep Reinforcement Learning-Based Traffic Control System. *IEEE Transactions on Intelligent Transportation Systems* 22, 8 (Aug. 2021), 5201–5212.
[122] NIO Inc. 2023. NIO Inc. Promptly Responds to Data Leakage. https://ir.nio.com/news-events/news-releases/news-release-details/nio-inc-promptly-responds-data-leakage/ Accessed: 2024-08.
[123] Weina Niu et al. 2021. Malware on Internet of UAVs Detection Combining String Matching and Fourier Transformation. *IEEE Internet of Things Journal* 8, 12 (June 2021), 9905–9919.
[124] Ahmad Nsouli et al. 2023. Reinforcement learning based scheme for on-demand vehicular fog formation. *Vehicular Communications* 40 (2023), 100571.
[125] Felix O. Olowononi et al. 2021. Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS. *IEEE Communications Surveys & Tutorials* 23, 1 (2021), 524–552.
[126] Ayodeji Oseni et al. 2023. An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks. *IEEE Transactions on Intelligent Transportation Systems* 24, 1 (Jan. 2023), 1000–1014.
[127] Quoc-Viet Pham et al. 2020. A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art. *IEEE Access* 8 (2020), 116974–117017.
[128] Segun I. Popoola et al. 2022. Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT-Edge Devices. *IEEE Internet of Things Journal* 9, 5 (March 2022), 3930–3944.
[129] Porsche AG. 2019. Porsche Uses Edge Computing to Enhance Vehicle Performance. https://newsroom.porsche.com/en/2019/digital/porsche-edge-computing-19509.html Accessed: 2024-08.
[130] Pavana Prakash et al. 2022. IoT Device Friendly and Communication-Efficient Federated Learning via Joint Model Pruning and Quantization. *IEEE Internet of Things Journal* 9, 15 (Aug. 2022), 13638–13650.
[131] Gopika Premsankar et al. 2018. Edge Computing for the Internet of Things: A Case Study. *IEEE Internet of Things Journal* 5, 2 (April 2018), 1275–1284.
[132] Adnan Qayyum et al. 2020. Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and the Way Forward. *IEEE Communications Surveys & Tutorials* 22, 2 (2020), 998–1026.
[133] Qi Qi et al. 2020. Scalable Parallel Task Scheduling for Autonomous Driving Using Multi-Task Deep Reinforcement Learning. *IEEE Transactions on Vehicular Technology* 69, 11 (Nov. 2020), 13861–13874.
[134] Kanwal Rashid et al. 2023. An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs). *Sensors* 23, 5 (Feb. 2023), 2594.
[135] Jinke Ren et al. 2019. Collaborative Cloud and Edge Computing for Latency Minimization. *IEEE Transactions on Vehicular Technology* 68, 5 (May 2019), 5031–5044.
[136] E. Rescorla. 2018. *The Transport Layer Security (TLS) Protocol Version 1.3*. Vol. 8446. IETF. 1–160 pages. doi:10.17487/rfc8446
[137] Carlos Resende et al. 2021. TIP4.0: Industrial Internet of Things Platform for Predictive Maintenance. *Sensors* 21, 14 (July 2021), 4676.
[138] Alessio Sacco et al. 2020. An architecture for adaptive task planning in support of IoT-based machine learning applications for disaster scenarios. *Computer Communications* 160 (July 2020), 769–778.
[139] Christian Sanders et al. 2020. Localizing Spoofing Attacks on Vehicular GPS Using Vehicle-to-Vehicle Communications. *IEEE Transactions on Vehicular Technology* 69, 12 (Dec. 2020), 15656–15667.
[140] Yuris Mulya Saputra et al. 2023. Dynamic Federated Learning-Based Economic Framework for Internet-of-Vehicles. *IEEE Transactions on Mobile Computing* 22, 4 (April 2023), 2100–2115.
[141] Prinkle Sharma et al. 2021. A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles. *IEEE Internet of Things Journal* 8, 6 (March 2021), 4991–4999.
[142] Meng Shen et al. 2019. Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT Data in Smart Cities. *IEEE Internet of Things Journal* 6, 5 (Oct. 2019), 7702–7712.
[143] Hafiz Husnain Raza Sherazi et al. 2019. DDoS attack detection: A key enabler for sustainable communication in internet of vehicles. *Sustainable Computing: Informatics and Systems* 23 (Sept. 2019), 13–20.
[144] Weisong Shi et al. 2016. Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal* 3, 5 (Oct. 2016), 637–646.
[145] Yuanming Shi et al. 2020. Communication-Efficient Edge AI: Algorithms and Systems. *IEEE Communications Surveys & Tutorials* 22, 4 (2020), 2167–2191.
[146] Md. Maruf Hossain Shuvo et al. 2023. Efficient Acceleration of Deep Learning Inference on Resource-Constrained Edge Devices: A Review. *Proc. IEEE* 111, 1 (Jan. 2023), 42–91.
[147] Pavel Sikora et al. 2021. Artificial Intelligence-Based Surveillance System for Railway Crossing Traffic. *IEEE Sensors Journal* 21, 14 (July 2021), 15515–15526.
[148] Shivani Singh et al. 2022. Machine-Learning-Assisted Security and Privacy Provisioning for Edge Computing: A Survey. *IEEE Internet of Things Journal* 9, 1 (Jan. 2022), 236–260.
[149] Arunan Sivanathan et al. 2020. Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning. *IEEE Transactions on Network and Service Management* 17, 1 (March 2020), 60–74.

Just Accepted

[150] Liangjun Song et al. 2020. FBIA: A Fog-Based Identity Authentication Scheme for Privacy Preservation in Internet of Vehicles. *IEEE Transactions on Vehicular Technology* 69, 5 (May 2020), 5403–5415.
[151] Cagatay Sonmez et al. 2021. Machine Learning-Based Workload Orchestrator for Vehicular Edge Computing. *IEEE Transactions on Intelligent Transportation Systems* 22, 4 (April 2021), 2239–2251.
[152] Clare Sullivan. 2019. EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *Computer Law & Security Review* 35, 4 (Aug. 2019), 380–397.
[153] Frost & Sullivan. 2023. Tesla's Dojo Supercomputer: A Game-Changer in the Quest for Fully Autonomous Vehicles. https://www.frost.com/frost-perspectives/teslas-dojo-supercomputer-a-game-changer-in-the-quest-for-fully-autonomous-vehicles/ Accessed: 2024-08.
[154] Yaohua Sun et al. 2019. Application of Machine Learning in Wireless Networks: Key Techniques and Open Issues. *IEEE Communications Surveys & Tutorials* 21, 4 (2019), 3072–3108.
[155] Anil Kumar Sutrala et al. 2020. On the Design of Conditional Privacy Preserving Batch Verification-Based Authentication Scheme for Internet of Vehicles Deployment. *IEEE Transactions on Vehicular Technology* 69, 5 (May 2020), 5535–5548.
[156] Anum Talpur et al. 2022. Machine Learning for Security in Vehicular Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials* 24, 1 (2022), 346–379.
[157] Fengxiao Tang et al. 2020. Future Intelligent and Secure Vehicular Network Toward 6G: Machine-Learning Approaches. *Proc. IEEE* 108, 2 (Feb. 2020), 292–307.
[158] The Business Research Company. 2023. Connected Cars Global Market Report. https://www.thebusinessresearchcompany.com/report/connected-cars-global-market-report Accessed: 2024-08.
[159] Zhihong Tian et al. 2020. A Distributed Deep Learning System for Web Attack Detection on Edge Devices. *IEEE Transactions on Industrial Informatics* 16, 3 (March 2020), 1963–1971.
[160] Shreshth Tuli et al. 2020. HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. *Future Generation Computer Systems* 104 (March 2020), 187–200.
[161] Frederick Tung et al. 2020. Deep Neural Network Compression by In-Parallel Pruning-Quantization. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 42, 3 (March 2020), 568–579.
[162] Safi Ullah et al. 2022. HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles. *Sensors* 22, 4 (Feb. 2022), 1340.
[163] United Nations Economic Commission for Europe. 2024. Vehicle Regulations. https://unece.org/transport/vehicle-regulations Accessed: 2024-08.
[164] Upstream Auto. 2024. Global Automotive Cybersecurity Report. https://upstream.auto/reports/global-automotive-cybersecurity-report/ Accessed: 2024-07.
[165] Veeramanikandan et al. 2020. Data Flow and Distributed Deep Neural Network based low latency IoT-Edge computation model for big data environment. *Engineering Applications of Artificial Intelligence* 94 (Sept. 2020), 103785.
[166] Parag Verma et al. 2022. FETCH: A Deep Learning-Based Fog Computing and IoT Integrated Environment for Healthcare Monitoring and Diagnosis. *IEEE Access* 10 (2022), 12548–12563.
[167] Volvo Cars. 2021. Volvo Cars to Harness Real-Time Data from Customer Cars to Set New Safety Standards. https://www.media.volvocars.com/global/en-gb/media/pressreleases/283544/volvo-cars-to-harness-real-time-data-from-customer-cars-to-set-new-safety-standards Accessed: 2024-08.
[168] Fangxin Wang et al. 2020. Deep Learning for Edge Computing Applications: A State-of-the-Art Survey. *IEEE Access* 8 (2020), 58322–58336.
[169] Jitian Wang et al. 2018. Vehicle Type Recognition in Surveillance Images From Labeled Web-Nature Data Using Deep Transfer Learning. *IEEE Transactions on Intelligent Transportation Systems* 19, 9 (Sept. 2018), 2913–2922.
[170] Jiadai Wang et al. 2020. Topology Poisoning Attack in SDN-Enabled Vehicular Edge Network. *IEEE Internet of Things Journal* 7, 10 (Oct. 2020), 9563–9574.
[171] Junhua Wang et al. 2022. Green Internet of Vehicles (IoV) in the 6G Era: Toward Sustainable Vehicular Communications and Networking. *IEEE Transactions on Green Communications and Networking* 6, 1 (March 2022), 391–423.
[172] Xiaojie Wang et al. 2019. A deep learning based energy-efficient computational offloading method in Internet of vehicles. *China Communications* 16, 3 (2019), 81–91.
[173] Xiaofei Wang et al. 2020. Convergence of Edge Computing and Deep Learning: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials* 22, 2 (2020), 869–904.
[174] Xiaojie Wang et al. 2022. Deep Learning-Based Network Traffic Prediction for Secure Backbone Networks in Internet of Vehicles. *ACM Transactions on Internet Technology* 22, 4 (Nov. 2022), 1–20.
[175] Xiaojie Wang et al. 2023. Blockchain Intelligence for Internet of Vehicles: Challenges and Solutions. *IEEE Communications Surveys & Tutorials* 25, 4 (2023), 2325–2355.
[176] Yingqing Wang et al. 2025. A reliability anomaly detection method based on enhanced GRU-Autoencoder for Vehicular Fog Computing services. *Computers & Security* 150 (2025), 104217.

Just Accepted

[177] Waymo. 2020. Seeing is Knowing: Advances in search and image recognition train Waymo's self-driving technology for any encounter. https://waymo.com/blog/2020/02/content-search/ Accessed: 2024-08.
[178] Mohammad Wazid et al. 2019. AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment. *IEEE Internet of Things Journal* 6, 5 (Oct. 2019), 8804–8817.
[179] Chathurika S Wickramasinghe et al. 2021. Explainable Unsupervised Machine Learning for Cyber-Physical Systems. *IEEE Access* 9 (2021), 131824–131843.
[180] Yu Wu et al. 2019. Mobility Management through Scalable C/U-Plane Decoupling in IoV Networks. *IEEE Communications Magazine* 57, 2 (Feb. 2019), 122–129.
[181] Shunyuan Xiao et al. 2022. Secure Distributed Adaptive Platooning Control of Automated Vehicles Over Vehicular Ad-Hoc Networks Under Denial-of-Service Attacks. *IEEE Transactions on Cybernetics* 52, 11 (Nov. 2022), 12003–12015.
[182] Zhan Xie et al. 2022. Efficient and secure certificateless signcryption without pairing for edge computing-based Internet of Vehicles. *IEEE Transactions on Vehicular Technology* 72, 5 (2022), 5642–5653.
[183] Chugui Xu et al. 2019. GANobfuscator: Mitigating Information Leakage Under GAN via Differential Privacy. *IEEE Transactions on Information Forensics and Security* 14, 9 (Sept. 2019), 2358–2371.
[184] Minrui Xu et al. 2022. Secure and Reliable Transfer Learning Framework for 6G-Enabled Internet of Vehicles. *IEEE Wireless Communications* 29, 4 (Aug. 2022), 132–139.
[185] Xiaolong Xu et al. 2019. An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. *Future Generation Computer Systems* 96 (2019), 89–100.
[186] Xiaolong Xu et al. 2019. An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. *Future Generation Computer Systems* 96 (July 2019), 89–100.
[187] Xiaolong Xu et al. 2021. Secure Service Offloading for Internet of Vehicles in SDN-Enabled Mobile Edge Computing. *IEEE Transactions on Intelligent Transportation Systems* 22, 6 (June 2021), 3720–3729.
[188] Xiaolong Xu et al. 2021. Trust-Aware Service Offloading for Video Surveillance in Edge Computing Enabled Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems* 22, 3 (March 2021), 1787–1796.
[189] Xiaolong Xu et al. 2023. Safe: Synergic Data Filtering for Federated Learning in Cloud-Edge Computing. *IEEE Transactions on Industrial Informatics* 19, 2 (Feb. 2023), 1655–1665.
[190] Waleed Yamany et al. 2023. OQFL: An Optimized Quantum-Based Federated Learning Framework for Defending Against Adversarial Attacks in Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems* 24, 1 (Jan. 2023), 893–903.
[191] Bo Yang et al. 2020. Offloading optimization in edge computing for deep-learning-enabled target tracking by internet of UAVs. *IEEE Internet of Things Journal* 8, 12 (2020), 9878–9893.
[192] Helin Yang et al. 2020. Machine Learning Techniques and A Case Study for Intelligent Wireless Networks. *IEEE Network* 34, 3 (May 2020), 208–215.
[193] Janghoon Yang. 2021. A Controllable False Data Injection Attack for a Cyber Physical System. *IEEE Access* 9 (2021), 6721–6728.
[194] Ya-Ting Yang et al. 2023. Edge–IoT Computing and Networking Resource Allocation for Decomposable Deep Learning Inference. *IEEE Internet of Things Journal* 10, 6 (March 2023), 5178–5193.
[195] Shuai Yu et al. 2022. EC-SAGINs: Edge-Computing-Enhanced Space–Air–Ground-Integrated Networks for Internet of Vehicles. *IEEE Internet of Things Journal* 9, 8 (April 2022), 5742–5754.
[196] Mehmet Fatih Yuce et al. 2024. Misbehavior detection with spatio-temporal graph neural networks. *Computers and Electrical Engineering* 116 (2024), 109198.
[197] Kailin Zeng et al. 2022. APD: Learning Diverse Behaviors for Reinforcement Learning Through Unsupervised Active Pre-Training. *IEEE Robotics and Automation Letters* 7, 4 (Oct. 2022), 12251–12258.
[198] Chuan Zhang et al. 2019. LPTD: Achieving lightweight and privacy-preserving truth discovery in CIoT. *Future Generation Computer Systems* 90 (Jan. 2019), 175–184.
[199] Can Zhang et al. 2020. BSFP: Blockchain-Enabled Smart Parking With Fairness, Reliability and Privacy Protection. *IEEE Transactions on Vehicular Technology* 69, 6 (June 2020), 6578–6591.
[200] Can Zhang et al. 2021. PRVB: Achieving Privacy-Preserving and Reliable Vehicular Crowdsensing via Blockchain Oracle. *IEEE Transactions on Vehicular Technology* 70, 1 (Jan. 2021), 831–843.
[201] Chuan Zhang et al. 2022. TPPR: A Trust-Based and Privacy-Preserving Platoon Recommendation Scheme in VANET. *IEEE Transactions on Services Computing* 15, 2 (March 2022), 806–818.
[202] Dajun Zhang et al. 2022. Multiaccess Edge Integrated Networking for Internet of Vehicles: A Blockchain-Based Deep Compressed Cooperative Learning Approach. *IEEE Transactions on Intelligent Transportation Systems* 23, 11 (Nov. 2022), 21593–21607.
[203] Haichun Zhang et al. 2020. CANsec: A Practical in-Vehicle Controller Area Network Security Evaluation Tool. *Sensors* 20, 17 (Aug. 2020), 4900.
[204] Jiale Zhang et al. 2020. LVPDA: A Lightweight and Verifiable Privacy-Preserving Data Aggregation Scheme for Edge-Enabled IoT. *IEEE Internet of Things Journal* 7, 5 (May 2020), 4016–4027.

Just Accepted

[205] Jun Zhang et al. 2020. Mobile Edge Intelligence and Computing for the Internet of Vehicles. *Proc. IEEE* 108, 2 (Feb. 2020), 246–261.
[206] Qikun Zhang et al. 2020. Blockchain-based asymmetric group key agreement protocol for internet of vehicles. *Computers & Electrical Engineering* 86 (Sept. 2020), 106713.
[207] Junhui Zhao et al. 2021. Edge Caching and Computation Management for Real-Time Internet of Vehicles: An Online and Distributed Approach. *IEEE Transactions on Intelligent Transportation Systems* 22, 4 (April 2021), 2183–2197.
[208] Yang Zhao et al. 2021. Local Differential Privacy-Based Federated Learning for Internet of Things. *IEEE Internet of Things Journal* 8, 11 (June 2021), 8836–8853.
[209] Zhiwei Zhao et al. 2018. Deploying Edge Computing Nodes for Large-Scale IoT: A Diversity Aware Approach. *IEEE Internet of Things Journal* 5, 5 (Oct. 2018), 3606–3614.
[210] Xuan Zhou et al. 2021. When Intelligent Transportation Systems Sensing Meets Edge Computing: Vision and Challenges. *Applied Sciences* 11, 20 (2021), 9680. doi:10.3390/app11209680
[211] Zhi Zhou et al. 2019. Edge Intelligence: Paving the Last Mile of Artificial Intelligence With Edge Computing. *Proc. IEEE* 107, 8 (Aug. 2019), 1738–1762.
[212] Hongfeng Zhu et al. 2020. Two novel semi-quantum-reflection protocols applied in connected vehicle systems with blockchain. *Computers & Electrical Engineering* 86 (Sept. 2020), 106714.
[213] Liehuang Zhu et al. 2025. Towards Robust Internet of Vehicles Security: An Edge Node-Based Machine Learning Framework for Attack Classification. In *Wireless Artificial Intelligent Computing Systems and Applications*, Zhipeng Cai et al. (Eds.). Springer Nature Switzerland, Cham, 78–89.
[214] Yuedi Zhu et al. 2025. FC-Trans: Deep learning methods for network intrusion detection in big data environments. *Computers & Security* (2025), 104392.

Received 20 May 2025; revised 3 May 2026; accepted 7 May 2026

Just Accepted