IEEE Open Journal of
Intelligent Transportation
Systems

Received 13 February 2025; revised 20 August 2025 and 22 November 2025; accepted 24 November 2025. Date of publication 26 November 2025; date of current version 9 December 2025.

Digital Object Identifier 10.1109/OJITS.2025.3637333

Interplay Between Security, Privacy and Trust in 6G-Enabled Intelligent Transportation Systems

AHMED DANLADI ABDULLAHI[1] (Student Member, IEEE), ERFAN BAHRAMI[2], TOOSKA DARGAHI[1] (Member, IEEE), MOHAMMED AL-KHALIDI[1] (Senior Member, IEEE), AND MOHAMMAD HAMMOUDEH[3] (Senior Member, IEEE)

[1]Department of Computing and Mathematics, Manchester Metropolitan University, M15 6BH Manchester, U.K.
[2]Department of Computer Engineering, Sharif University of Technology, Tehran 1458889694, Iran
[3]Department of Information and Computer Science, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

CORRESPONDING AUTHOR: A. D. ABDULLAHI (e-mail: ahmed2.abdullahi@stu.mmu.ac.uk)

ABSTRACT Advancements in sixth-generation (6G) wireless technology are expected to transform the transportation sector by enabling faster, more reliable, and more intelligent mobility services. 6G-enabled Intelligent Transportation Systems (ITS) offer ultra-low-latency communication, massive connectivity, and advanced analytics that support safer, more efficient, and more sustainable mobility. Despite these benefits, 6G-ITS introduces significant security, privacy, and trust challenges that must be addressed to ensure safe deployment and sustained public confidence. This paper reviews the opportunities and challenges of 6G-ITS with a focus on security, privacy, and trust, including the dual role of quantum technologies that strengthen cryptographic mechanisms while introducing novel attack surfaces. The paper highlights the benefits of 6G for transportation, including improved communication performance, enhanced device interoperability, advanced data analytics, and increased automation across transportation management and communication systems. A taxonomy of attack models in 6G-ITS is provided, alongside a comparison of security threats in 5G-ITS and 6G-ITS and corresponding mitigation strategies. The findings highlight the need for a comprehensive, multi-layered security framework that spans physical infrastructure, network protocols, data management, application security, and trust mechanisms to ensure the integrity and resilience of future 6G transportation ecosystems.

INDEX TERMS Intelligent transportation systems, 6G, authentication, cybersecurity, trust, data privacy.

I. INTRODUCTION

As WE approach the 2030s, the wireless communication landscape is poised for another revolutionary leap with the advent of sixth-generation (6G) technology [1]. Whilst fifth-generation (5G) networks are still in their deployment phase and their global adoption and coverage remain incomplete [2], researchers and industry leaders are already envisioning the next frontier of connectivity that will seamlessly integrate communication across terrestrial, aerial, and space levels [2]. 6G represents the next generation of wireless communication technology, designed to surpass the capabilities of 5G in terms of speed, capacity, latency, and connectivity [3]. The emerging 6G architecture combines dense terrestrial cells, aerial platforms, and satellite networks into a unified three-dimensional system that offers continuous and highly reliable coverage [2], [4]. These layers are interconnected through advanced backhaul and fronthaul networks, creating a seamless, three-dimensional coverage ecosystem [5] as shown in Figure 1.

Several groundbreaking features distinguish 6G. It boasts an Artificial Intelligence (AI)-native design, with AI embedded at every network layer, from the physical infrastructure to the application level, enabling autonomous network optimization, predictive resource allocation, and intelligent service provisioning [6], [7]. Quantum technologies are also expected to play a central role, providing quantum key distribution and quantum-resistant cryptography for enhanced security while simultaneously presenting new attack surfaces [6]. Intelligent reflecting surfaces, which are programmable metasurfaces, can dynamically control

The review of this article was arranged by Associate Editor Peter Han Joo Chong.

and optimize electromagnetic wave propagation, enhancing coverage, capacity, and energy efficiency [8]. Using terahertz (THz) frequencies in the 0.1–10 THz range aims to achieve unprecedented data rates and support holographic communications [9]. THz communication refers to ultra-high-frequency bands that offer massive bandwidth for high-capacity links but suffer from severe path loss and require line-of-sight operation, making propagation management essential. Cell-free massive Multiple-Input Multiple-Output (MIMO) technology also provides uniform high-capacity coverage and mitigates the cell-edge issues prevalent in traditional cellular networks, which occur when devices are far from the base station and receive weak signals, resulting in lower data rates and reduced reliability [10]. In contrast to conventional cellular layouts, cell-free MIMO replaces fixed cell boundaries with many distributed access points that cooperatively serve users, leading to more consistent and reliable connectivity.

6G networks are designed to meet unprecedented performance metrics to support ambitious goals. These include peak data rates of up to 1 terabit per second (Tbps), user-experience data rates of 1 gigabit per second (Gbps), spectrum efficiency 3 to 5 times higher than 5G, and network energy efficiency ten to hundred times better than its predecessor [10], [11]. Furthermore, 6G aims to support an area traffic capacity of 1 Gbps/m^2, a connection density of 10 million devices per square kilometre (10^7 devices/km^2), latency below 100 microseconds, mobility up to 1000 kilometres per hour, and centimetre-level positioning accuracy [3], [5], [12]. These requirements are crucial for enabling advanced applications across various sectors, particularly in ITS.

These performance improvements support real-time autonomous driving decisions, allow the exchange of rich sensor data and 3D environmental maps, and enable dense deployments of roadside sensors for continuous monitoring and cooperative perception [13], [14]. Centimetre-level positioning accuracy enhances navigation systems, enabling precise lane-level positioning for autonomous vehicles and more efficient traffic flow management [11]. The AI-native architecture allows for predictive traffic management, adaptive routing based on real-time data analysis, and proactive maintenance of transportation infrastructure [10].

These advancements pave the way for transformative ITS applications such as fully autonomous transportation systems, seamless intermodal mobility, and intelligent traffic management that can adapt in real time to changing conditions [15]. However, the security implications of the increased connectivity and interoperability support of millions of loosely connected heterogeneous devices and vehicles present significant challenges, particularly in terms of security, privacy, and trust [2]. Cyberattacks on autonomous vehicles, roadside units, or control centres pose direct risks to human safety, making robust protection mechanisms a fundamental requirement for future transportation

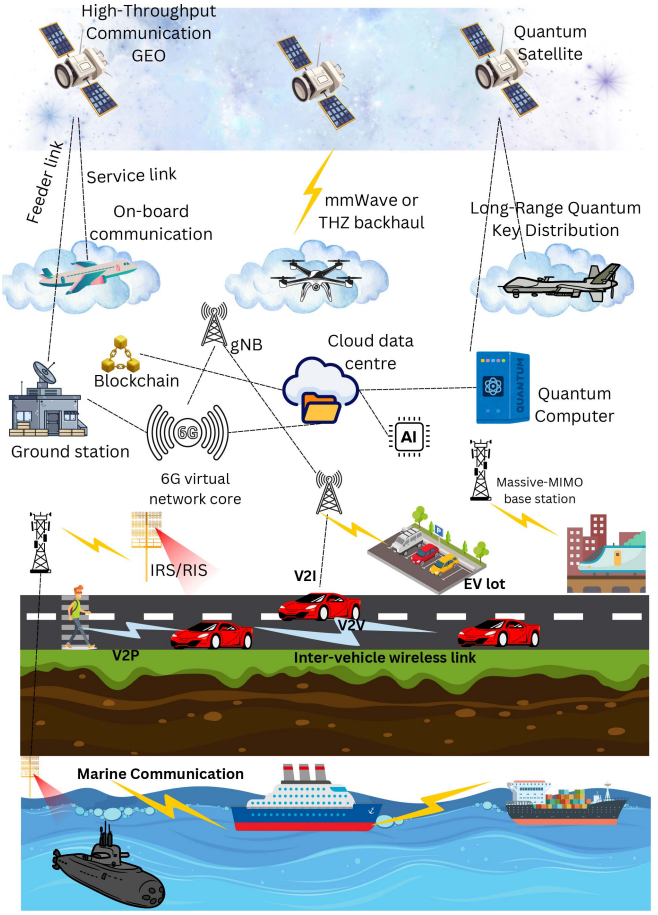

FIGURE 1. Vision of ground, sea, air, and space 6G integrated network with ITS.

systems. The risks associated with security breaches in ITS could have severe consequences beyond financial loss or reputational damage, potentially impacting human safety.

Realizing the transformational potential of 6G-powered ITS critically depends on establishing robust, multi-faceted security and trust between components [2]. Open challenges remain in balancing privacy with vast 6G-generated data to refine usability [16]. The scale and heterogeneity of 6G-ITS mean that billions of devices, vehicles, and infrastructure components must coordinate securely, making trust management and continuous verification essential [17]. Holistic trust and security mechanisms spanning technological, governance, and social dimensions are thus imperative but challenging to achieve.

ITS integrates advanced sensors, communication modules, and data management systems to improve various aspects of transportation. For a more in-depth discussion of the ITS components and their implications on cyber security, refer to [18], [19] and [20]. Figure 1 illustrates 6G's vision for ground, sea, air, and space integrated networks with ITS applications.

This paper aims to answer the research questions highlighted in Table 1. The primary contributions of this research are summarized as follows:

TABLE 1. Research questions.

Research Questions (RQ)	Discussion
RQ1: In the context of 6G-ITS, how can multi-layered security strategies be designed to protect against sophisticated cyberattacks targeting communication networks, devices, and data analytics platforms?	This question addresses the critical aspect of security in 6G-ITS. It recognizes the complexity of potential cyber threats and the need for comprehensive, layered strategies to safeguard essential components of ITS. Addressing this question will provide insights into developing robust security frameworks that can adapt to the evolving threat landscape, ensuring the resilience of ITS infrastructure.
RQ2: What mechanisms can be developed within 6G-ITS to ensure user privacy in the face of extensive data collection required for advanced sensing, automation, and communication systems?	Privacy is a paramount concern in the deployment of ITS, especially with the advent of 6G technologies enabling unprecedented data exchange rates. This question underscores the challenge of balancing the benefits of enhanced data analytics capabilities with the imperative of protecting individual privacy. Solutions to this query are pivotal for fostering user trust and facilitating the wider acceptance of 6G-ITS.
RQ3: How can trust in 6G-ITS be quantified and managed, particularly in systems involving decision-making and autonomous operations?	Quantifying and managing trust in 6G-ITS involves developing metrics to assess the reliability, security, and performance of AI and machine learning (ML) driven technologies, alongside implementing dynamic assessment methods and adaptive protocols for ongoing monitoring and system improvements.

1) Comparison of the security of 5G-enabled ITS and 6G-ITS, analysing how the unique capabilities of 6G pose new security threats that must be addressed.
2) Providing a taxonomy of the main security threats to 6G-ITS, including communication-based attacks, data-based attacks, device-based attacks, application-based attacks, privacy invasion and quantum attacks, and their impact on confidentiality, integrity, availability, and non-repudiation.
3) Providing an in-depth analysis of the privacy risks in 6G-ITS and the impact of emerging privacy-preserving technologies, such as Federated Learning (FL), differential privacy, and secret sharing schemes.
4) Highlighting the key challenges of authentication and trust in 6G-ITS, especially in the context of the increased connectivity density and heterogeneous, decentralized nature of the networks.

The remainder of this paper follows the structure illustrated in Figure 2. Section II discusses existing works. Section III examines the security landscape of 6G-ITS, where the attack model and security requirements are analyzed. Section IV explains the privacy outlook of 6G-ITS, while Section V discusses the trust landscape in 6G-ITS. Section VI explores the differences between 5G-ITS and 6G-ITS. Section VII and VIII answer the research questions and conclude the paper, respectively. Table 2 contains the list of utilized acronyms throughout the paper.

II. RELATED WORK

The emergence of 6G technology sparked significant research interest in its potential applications, challenges, and implications for various sectors, including ITS. The current state of research on 6G-ITS encompasses a wide range of themes, from privacy and security to trust management and emerging technologies.

Several studies outlined the vision and requirements for 6G networks. Jiang et al. [9] provide a comprehensive survey of 6G systems, discussing drivers, use cases, requirements, and enabling technologies. They predict an explosive growth in mobile traffic by 2030 and envision potential use cases and scenarios. Similarly, Zhang et al. [10] present a vision for 6G networks, describing use cases and requirements for multi-terabyte-per-second intelligent networks. They propose a large-dimensional and autonomous network architecture that integrates space, air, ground, and underwater networks. Saad et al. [11] offer a holistic vision of 6G systems, arguing that 6G will be a convergence of technological trends driven by the underlying services rather than the mere exploration of higher frequency bands. They identify the primary drivers of 6G systems and propose new service classes with target performance requirements.

Several researchers explored the application of 6G in ITS. Deng et al. [21] comprehensively review 6G autonomous intelligent transportation systems (6G-AITS), discussing the mechanisms, applications, and challenges. They emphasize the importance of maintaining a human-centric approach in the development of 6G-ITS. Jha et al. [13] investigate the potential of 6G in revolutionizing transportation systems, analyzing the standards, technologies, and challenges associated with its implementation. They discuss novel applications such as autonomous driving, smart traffic management, and cooperative collision avoidance. Nguyen et al. [14] focus on the evolution of vehicular networks towards intelligent vehicular networks in 6G. They highlight why 5G is inadequate for specific vehicular applications and how 6G technologies can fill the gap. The work of Noor-A-Rahim et al. [22] shifts focus to enabling technologies for 6G-V2X communication,

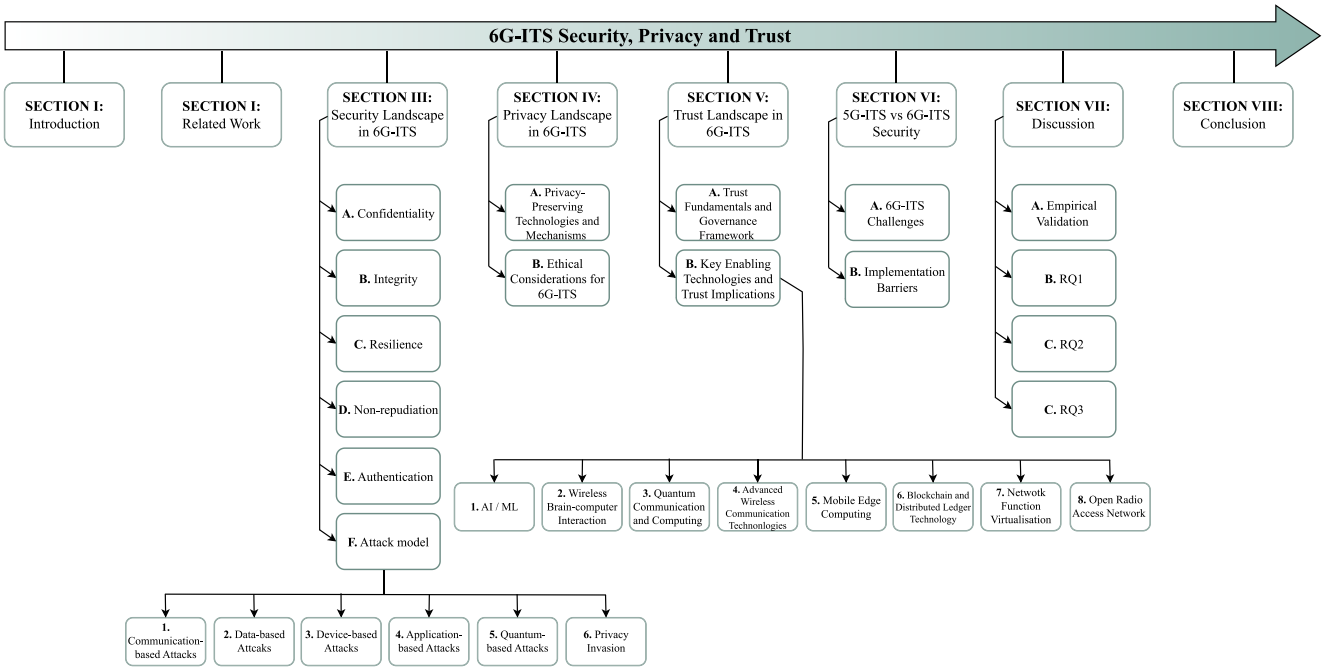

FIGURE 2. Structure and organization of this paper.

touching upon advances in machine learning for vehicular networks. Similarly, Kirubasri et al. [23] survey the broader scope of 6G vehicular technology, its applications, and the challenges it presents, indicating a paradigm shift from smart to intelligent systems.

Security and privacy concerns in 6G-ITS are a significant focus of research. Moya Osorio et al. [24] provide a comprehensive survey on security and privacy in the 6G-enabled Internet of Vehicles (IoV), covering the evolution of V2X communication towards IoV and highlighting security frameworks and privacy concerns. Wang et al. [25] discuss new areas and challenges in security and privacy for 6G networks, including real-time intelligent edge computing, distributed artificial intelligence, intelligent radio, and 3D intercoms. They also explore potential use cases and emerging technologies in each area. Nguyen et al. [26] offer a systematic overview of security and privacy issues based on the prospective technologies for 6G in the physical, connection, and service layers. They highlight new threat vectors from new radio technologies and discuss promising techniques to mitigate the magnitude of attacks and breaches of personal data. The research in [20] focuses on the current security landscape of ITS, particularly considering the integration of the Internet of Things (IoT). It thoroughly examines ITS's security posture, including attacker models and potential vulnerabilities. Complementing this, a survey presented in [18] categorizes the security challenges in ITS, identifying major attack types, such as Distributed Denial of Service (DDoS) and session hijacking.

Trust management in 6G networks has emerged as a crucial research area. Ziegler et al. [17] discuss the evolution of the 5G security paradigm and explore relevant security technology enablers for 6G, including automated software creation, privacy-preserving technologies, and quantum-safe security. Wang et al. [27] introduce a new trust framework called SIX-Trust, made up of three layers that focus on sustainable trust, infrastructure trust, and xenogenesis trust. They demonstrate how these technologies can enhance the trust and security of 6G networks. Veith et al. [28] provide an overview of trust anchor technologies for 6G, describing the requirements for an end-to-end trust building framework and discussing the concept of trust in mobile communications systems.

Several studies explored emerging technologies that could enable 6G-ITS. Akyildiz et al. [7] discuss transformative solutions expected to drive the surge for accommodating a rapidly growing number of intelligent devices and services in 6G and beyond. They highlight technologies such as THz band communications, intelligent communication environments, and pervasive artificial intelligence. Giordani et al. [4] discuss technologies that will evolve wireless networks toward 6G, providing a full-stack, system-level perspective on 6G scenarios and requirements. They focus on technologies that can satisfy these requirements by improving the 5G design or introducing completely new communication paradigms. Yang et al. [29] present an overview of promising techniques evolving to 6G, including physical-layer transmission techniques, network designs, security approaches, and testbed developments. A

TABLE 2. Main acronyms used in this paper.

Acronym	Definition	Acronym	Definition
3D	Three-Dimensional	ML	Machine Learning
3GPP	Third Generation Partnership Project	mmWave	Millimetre Wave
5G	Fifth Generation	NFV	Network Function Virtualization
6G	Sixth Generation	NOMA	Non-Orthogonal Multiple Access
6G-AITS	6G Autonomous Intelligent Transportation Systems	OBUs	On-Board Units
6G-ITS	6G-enabled Intelligent Transportation Systems	O-RAN	Open Radio Access Network
AI	Artificial Intelligence	P2BA	Privacy-preserving Protocol with Batch Authentication
AKA	Authentication and Key Agreement	PCA	Pilot Contamination Attacks
AMF	Access and Mobility Management Function	PKI	Public Key Infrastructure
APs	Access Points	PLS	Physical Layer Security
BCV	Brain-Controlled Vehicles	PQC	Post-Quantum Cryptography
C-FL	Consensus-driven Federated Learning	QKD	Quantum Key Distribution
CA	Central Authority	QoS	Quality of Service
CAV	Connected Autonomous Vehicle	RATs	Radio Access Technologies
DDoS	Distributed Denial of Service	RIC	Radio Intelligent Controller
DLT	Distributed Ledger Technology	RIS	Reconfigurable Intelligent Surface
dMIMO	Distributed Multiple-Input Multiple-Output	RSU	Road Side Unit
DP	Differential Privacy	SADC	Sensor Attack Detection Classification
EEG	Electroencephalography	SAGIN	Space-Air-Ground-Sea Integration Network
ETSI	European Telecommunications Standards Institute	SDN	Software Defined Networking
FL	Federated Learning	SDR	Software Defined Radio
GANs	Generative Adversarial Networks	SMC	Secure Multi-party Computation
Gbps	Gigabits per second	TA	Trusted Authority
GEO	Geostationary Earth Orbit	Tbps	Terabits per second
gNB	Next Generation NodeB	THz	Terahertz
IEEE	Institute of Electrical and Electronics Engineers	TLS	Transport Layer Security
IoT	Internet of Things	TPM	Trusted Platform Module
IoV	Internet of Vehicles	V2G	Vehicle-to-Grid
IRS	Intelligent Reflecting Surface	V2I	Vehicle-to-Infrastructure
ISAC	Integrated Sensing and Communication	V2N	Vehicle-to-Network
ITS	Intelligent Transportation Systems	V2P	Vehicle-to-Pedestrian
LEO	Low Earth Orbit	V2V	Vehicle-to-Vehicle
Li-Fi	Light Fidelity	V2X	Vehicle-to-Everything
Lidar	Light Detection and Ranging	VANET	Vehicular Ad Hoc Network
LSTM	Long Short-Term Memory	VLC	Visible Light Communication
MDI	Measurement-Device-Independent	VNF	Virtual Network Function
MEC	Mobile Edge Computing	VPN	Virtual Private Network
MIMO	Multiple-Input Multiple-Output	xApps	Extensible Applications
MitM	Man-in-the-Middle	ZTA	Zero Trust Architecture

comparison of previous related surveys and how our work fills the existing gap is presented in Table 3.

III. SECURITY LANDSCAPE IN 6G-ITS

Advancements in 6G technology introduce unprecedented challenges to the security landscape of ITS. With its ultra-high bandwidth, massive connectivity, and AI/ML integration at the network core, 6G fundamentally alters the nature and scale of security threats. The 6G-ITS security landscape is complex, connecting diverse components such as vehicles, drones, and several IoT devices. This heterogeneity and high mobility complicate achieving both security and interoperability [18], necessitating advanced authentication and security measures. This section examines how 6G impacts confidentiality, integrity, availability, authentication, and non-repudiation in ITS, exploring evolving security requirements and new attack models. Figure 3 illustrates a high-level overview of the ITS architecture based on an accident emergence scenario.

A. CONFIDENTIALITY

Ensuring security and confidentiality in a 6G-ITS is essential. The massive connectivity of 6G significantly increases the attack surface for data breaches. Confidentiality attacks could include attacks on the communication systems that connect vehicles, infrastructure and control centers or on the data analytics and management tools that process and analyze the data collected by sensors and cameras. Unlike 5G, 6G's integration of AI/ML at the network core introduces new data processing and analysis vulnerabilities, such as adversarial examples and privacy leaks. Secure protocols and quantum-resistant encryption protect communication, alongside robust security measures such as firewalls, intrusion detection systems, and incident response plans [18].

Data breaches pose a significant risk to the security of ITS, particularly as these systems collect sensitive data, such as traffic patterns, weather conditions, and pedestrian movements, which may include personally identifiable

TABLE 3. A comparison of related surveys in the literature.

Annotations: "✓" indicates covered, and "X" indicates not covered

Ref	6G	ITS	Security	Privacy	Trust	Focus	Limitation
[9]	✓	X	X	X	X	Comprehensive survey of 6G systems	Limited focus on ITS and security
[10]	✓	✓	X	X	X	Large-dimensional 6G network architecture	Lacks security and privacy considerations
[11]	✓	X	X	X	X	Holistic vision of 6G systems	Does not address ITS or security challenges
[21]	✓	✓	X	X	X	6G autonomous ITS	Limited security, privacy, and trust focus
[13]	✓	✓	X	X	X	6G in revolutionizing transportation	Lacks in-depth security analysis
[14]	✓	✓	X	X	X	Intelligent vehicular networks in 6G	Inadequate security and privacy coverage
[22]	✓	✓	X	X	X	Enabling technologies for 6G-V2X	Limited security and trust considerations
[23]	✓	✓	X	X	X	Broader scope of 6G vehicular technology	Lacks detailed security analysis
[24]	✓	✓	✓	✓	X	Security and privacy in 6G-IoV	Limited trust management focus
[25]	✓	X	✓	✓	X	Security and privacy in 6G networks	Not specifically focused on ITS
[26]	✓	X	✓	✓	X	Security and privacy in 6G technologies	Lacks ITS-specific considerations
[20]	X	✓	✓	X	X	Security landscape of ITS	Limited focus on 6G and privacy
[18]	X	✓	✓	X	X	Security challenges in ITS	Does not address 6G specifics
[17]	✓	X	✓	✓	✓	6G security paradigm evolution	Not focused on ITS applications
[27]	✓	X	X	X	✓	SIX-Trust framework for 6G	Limited security and privacy coverage
[28]	✓	X	X	X	✓	Trust anchor technologies for 6G	Lacks ITS-specific considerations
[7]	✓	X	X	X	X	Transformative solutions for 6G	Limited security, privacy, trust in ITS
[4]	✓	X	X	X	X	Technologies for 6G networks	Lacks security and ITS considerations
[29]	✓	X	✓	X	X	Promising techniques for 6G	Limited privacy, trust, ITS applications
Our Work	✓	✓	✓	✓	✓	Comprehensive security, privacy, and trust in 6G-ITS	Limited focus on practical implementation challenges and experimental validation

information. Unlike 5G, 6G's integration of AI/ML at the network core introduces new data processing and analysis vulnerabilities, such as adversarial examples and privacy leaks. With 6G enabling more sophisticated AI/ML integrations, enhanced data privacy measures are paramount to protect individual confidentiality. For instance, the trial of AI-powered speed cameras in the U.K. raised privacy concerns due to their invasive imaging capabilities [30]. Maintain public trust hinges in addressing these confidentiality issues as mobile technology evolves. Proper data encryption and management practices protect this data, while access controls ensure that only authorized personnel can view or use it [31]. Physical attacks on the infrastructures, including sensors, cameras, and communication devices. Securing the physical infrastructure requires tamper-proof housing and intrusion detection capabilities, with critical infrastructure well-protected through strictly controlled access [32].

B. INTEGRITY

One of the main concerns for the security integrity in an ITS is maintaining the consistency and accuracy of the data being transmitted, processed, and stored. The sheer volume of data in 6G networks, which could reach zettabytes per year, exponentially increases the challenge of maintaining data integrity. Data protection from unauthorized changes, deletions, or insertions during transmission, processing, and storage requires tampering detection and prevention mechanisms such as digital signatures, authentication, and encryption, which should be implemented to ensure the integrity of the data. Another aspect to consider is the integrity of system components and communication must also be considered. ITS components, such as sensors, cameras, communication devices, and other devices, require security and protection from physical tampering and unauthorized access, including the control system responsible for the decision-making, coordination, and management of the system resources. Additionally, regular updates and patch management address known vulnerabilities and keep the system free from malware. When machine learning and AI techniques are used, the integrity of decision-making processes and algorithms must be maintained through validation and testing of models to ensure their robustness. Maintaining security integrity in 6G-ITS requires a holistic

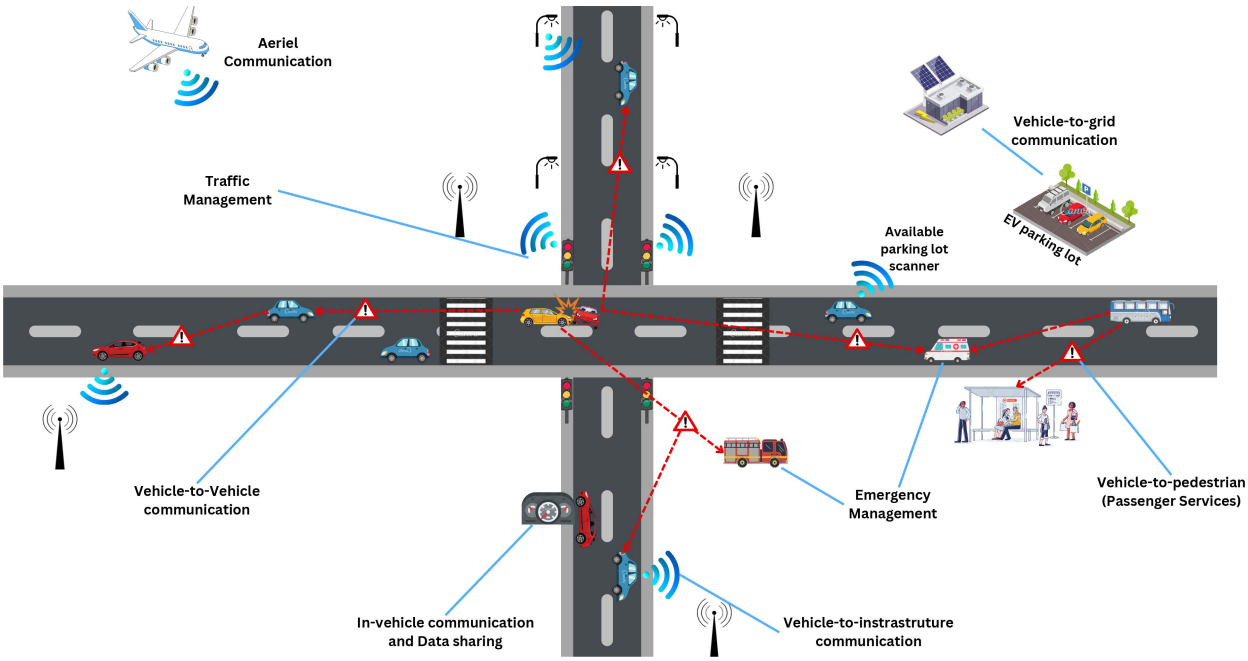

FIGURE 3. High-level overview of ITS architecture.

approach that involves multiple layers of security controls and mechanisms [18].

C. RESILIENCE

Resilience in 6G-ITS is paramount due to the direct link between system availability and public safety. Unlike traditional communication systems where disruptions cause inconvenience, failures in ITS can lead to catastrophic consequences, including traffic accidents, emergency response delays, and cascading infrastructure failures [24]. With 6G's sub-millisecond latency requirements, even brief disruptions can have severe consequences, making resilience a critical concern. A millisecond-level outage in autonomous vehicle coordination systems could result in collisions, whilst disruption to traffic management systems can cause gridlock that affects emergency services' access to critical incidents.

As part of Critical National Infrastructure (CNI), ITS prioritises availability over security–a fundamental departure from conventional IT security paradigms where confidentiality often takes precedence. This prioritization reflects the reality that a secure but unavailable system poses greater risks than a partially compromised but operational one. For instance, during emergency evacuations or disaster response scenarios, maintaining traffic flow and vehicle coordination capabilities supersedes concerns about data confidentiality or perfect authentication. However, this does not diminish security requirements; rather, it necessitates security mechanisms that enhance rather than impede availability [18]. The ability to keep the system running in the face of cyberattacks or other disruptive events is one of the primary problems related to security resilience in an ITS. This involves defending the system against ransomware, DDoS attacks, and other malicious attacks that can render the system inoperable. Another challenge is ensuring the resilience and fault tolerance of the system against hardware or software failures, power outages, or other disruptions [18]. The increased reliance on edge computing in 6G networks introduces new points of failure that must be addressed to maintain system availability.

The safety-critical nature of ITS demands resilience strategies that account for graceful degradation rather than complete failure. When components fail, the system must transition to reduced-capacity operation modes whilst maintaining safety guarantees. For example, if AI-driven traffic optimization fails, the system should revert to traditional signal timing patterns rather than complete shutdown. Similarly, autonomous vehicle systems must maintain basic safety functions even when connectivity to 6G infrastructure is lost [24]. Diverse and redundant systems and network designs, combined with detailed disaster recovery plans, provide rapid response capabilities in the event of an incident. Security measures such as firewalls, intrusion detection and prevention systems, and incident response strategies reduce these risks. The integration of emerging technologies such as AI/ML raises additional concerns regarding the robustness and transparency of decision-making processes. Ensuring security availability in 6G-ITS requires balancing the competing demands of security, safety, and operational continuity–a challenge that distinguishes CNI systems from conventional networks where security considerations may justifiably compromise availability [24].

D. NON-REPUDIATION

Ensuring non-repudiation in 6G-ITS is an important aspect of overall security, as it helps ensure that the authenticity and integrity of data and communications can be verified

and that any actions taken by the system can be traced to their originator [24]. One of the main challenges is ensuring that data and communications are properly authenticated and that the sender's identity can be verified. Techniques such as digital signatures, certificates, and Public Key Infrastructure (PKI), combined with tamper-proof hardware or secure communication protocols, protect data in transit [33]. However, the quantum computing capabilities expected in the 6G era pose a significant threat to traditional PKI systems, necessitating the development of quantum-resistant cryptographic techniques.

Maintaining a tamper-proof log of all actions and events within the system is essential for non-repudiation, though this results in high computational costs. Digital signatures, digital time-stamping, and other technologies that 6G promises to ensure that actions and events can be traced back to their originator, whilst secure data storage and archiving practices preserve logs for future reference [26], [33]. Non-repudiation is also essential for liability and accountability. In case of incidents and accidents, tracing the decisions and actions that led to the incident and holding the responsible parties accountable is vital. This becomes particularly complex in 6G-ITS, where decision-making may involve AI/ML algorithms, raising questions about accountability in automated systems.

E. AUTHENTICATION

Authentication is a crucial aspect of security in 6G-ITS, as it helps to ensure that only authorized entities can access and interact with the system. The heterogeneity and massive scale of devices in 6G networks make authentication a particularly complex challenge. ITS include various types of entities, such as vehicles, roadside infrastructures, control centers, and other devices that must be authenticated before accessing the system [34]. Authentication in 6G-ITS is bidirectional, which means that user devices must authenticate to the system and the 6G infrastructure must authenticate itself to user devices. While this bidirectional authentication helps prevent attacks realized through fake base stations and ensures users connect to legitimate network infrastructure, it also introduces new security vulnerabilities to replay attacks, forgery attacks, and man-in-the-middle attacks [1].

The scalability and flexibility of the system are among the primary difficulties in authentication. Managing and protecting the system becomes increasingly challenging as the number of entities engaging with the system grows, particularly in ensuring that appropriate entities receive access at the appropriate level [5]. Secure and adaptable authentication techniques, such as multi-factor authentication, digital certificates and PKI, can expand to handle many entities without sacrificing security. Authentication in ITS must also maintain the privacy and security of personal information used for authentication [35]. Personal information, such as biometric data, is sensitive and requires protection from unauthorized access and misuse through secure data storage, encryption, and strict access controls. In addition, authentication challenges include the integration of IoT devices with limited resources and computational capabilities making robust authentication methods difficult to implement. Integrating emerging technologies such as AI/ML and other 6G enabling technologies poses additional challenges regarding robustness against advanced attacks and transparency in decision-making [36]. The State-of-the-art authentication schemes and challenges in 6G-ITS are further analyzed in Section VII.

F. ATTACK MODEL FOR 6G-ITS

Security threats in 6G-ITS are classified into six categories based on the Space-Air-Ground-Sea Integration Network (SASGIN) architecture [33]: communication-based, data-based, device-based, application-based, quantum-based attacks, and privacy invasion. Figure 4 illustrates this comprehensive attack taxonomy. Table 4 summarizes mitigation strategies for each attack category.

1) COMMUNICATION-BASED ATTACKS

Communication-based attacks target channels and protocols that transmit data and control information in 6G-ITS. Two critical attack surfaces emerge: the vehicle-to-everything (V2X), which encompasses vehicles-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), and vehicle-to-grid (V2G) communications operating at up to 1 Tbps with sub-millisecond latency, and the intelligent network management systems responsible for resource orchestration, Quality of Service (QoS) management, network slicing, and dynamic spectrum allocation. Ultra-dense deployment, heterogeneous architecture, and real-time safety requirements create numerous entry points for attackers. A common attack model for communication-based attacks in a 6G-ITS would include the following:

- DDoS: Overwhelming communication channels with traffic to prevent legitimate request processing [37].
- Man-in-the-Middle (MitM): Intercepting and manipulating communications between vehicles, infrastructure, and control centers to steal or corrupt data.
- Key management attacks: Targeting the cryptographic infrastructure that underlies secure communications [37].
- Replay attacks: Recording and replaying valid messages to impersonate legitimate entities.
- Protocol injection/: Exploiting protocol vulnerabilities to cause service denial or system compromise [38].
- Eavesdropping: Intercepting sensitive transmissions across 6G's expanded channels; sophisticated beamforming creates new covert data capture opportunities.
- Jamming: Introduce targeted interference to disrupt wireless communications; higher frequency bands enable selective targeting of network segments. Example: relay theft attacks on Land Rover vehicles using key fob jamming [39].

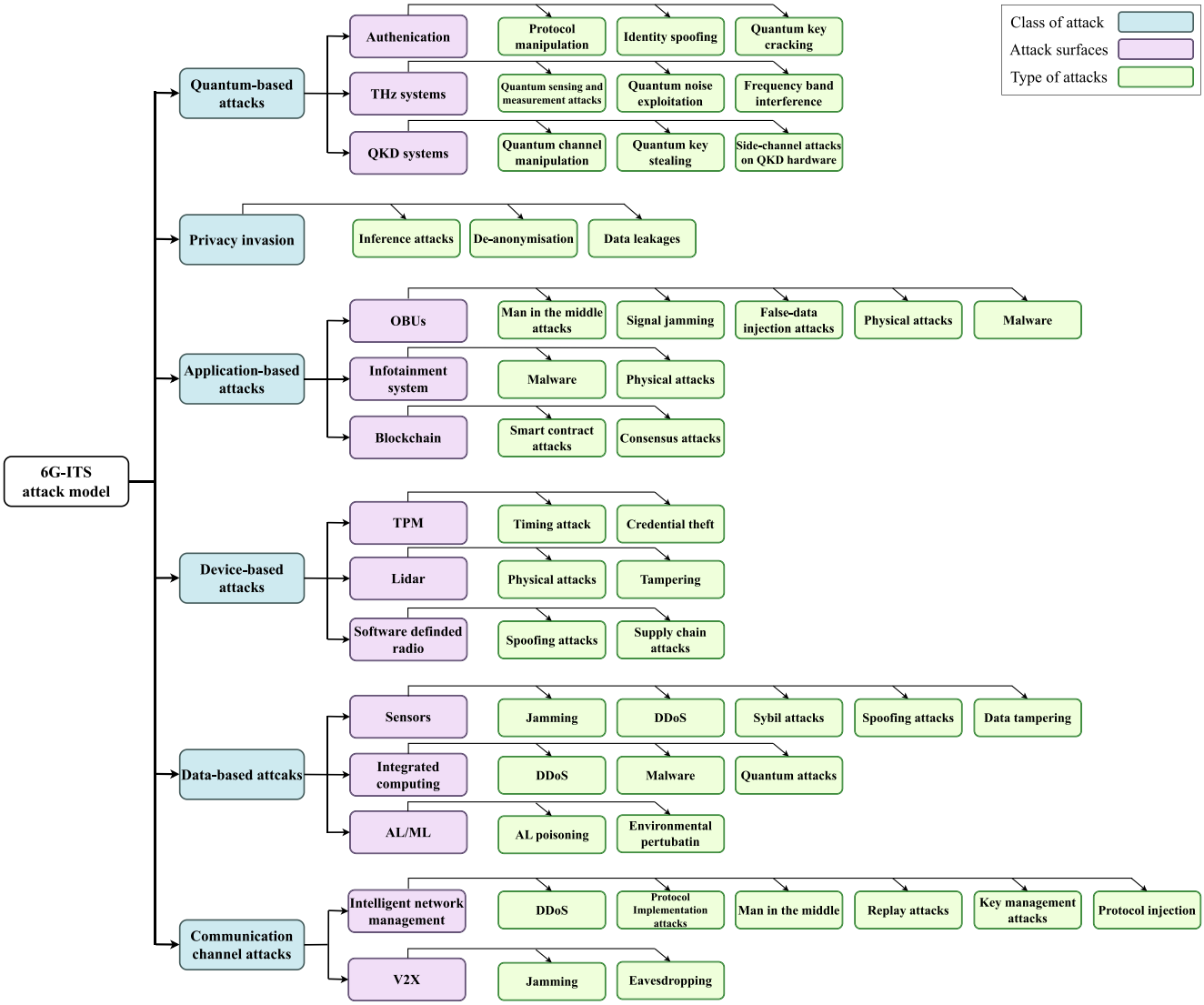

FIGURE 4. Attack model of 6G-ITS.

2) DATA-BASED ATTACKS

The 6G-ITS data processing integrates AI/ML directly into the network core, fundamentally transforming the security landscape. Three interconnected layers form the ecosystem: AI/ML systems serving as the cognitive engine, an integrated computing infrastructure that combines edge and cloud resources, and sensor networks that provide the physical-digital interface. The distributed computing architecture, essential for data generation and processing, introduces numerous entry points for attackers that require security in multiple layers of the 6G-ITS architecture. Examples of typical data-based attacks in a 6G-ITS include the following:

- AI/ML poisoning: Manipulating training data or introducing adversarial examples (i.e., carefully crafted inputs designed to deceive ML models) to compromise autonomous vehicle control and traffic management.
- Environmental perturbation: Refers to unexpected physical conditions such as fog, rain, snow, dust, or glare that distort sensor readings or wireless signals, causing ITS components to misinterpret their surroundings [40]. This introduces physical or electromagnetic interference to manipulate sensor readings.
- Data manipulation /injection: Modification or insertion of false data without authorization [41].
- Quantum attacks: Exploiting quantum computing to compromise cryptographic systems, potentially breaching quantum key distribution (QKD using quantum mechanics to securely distribute encryption keys) implementations [42]. In simple terms, these are attacks that use quantum computers to break encryption that classical computers cannot.
- Sybil attacks: Create multiple fake identities to manipulate data aggregation in V2X communications.
- Spoofing: Compromising the authenticity of the data through unauthorized modifications of sensor readings or vehicle telemetry [41].

TABLE 4. Summary of mitigation strategies for 6G-ITS attack categories.

Attack category	Attack vectors	Main mitigation strategies in 6G-ITS	References
Communication-based	DDoS, MitM, key management attacks, replay, protocol injection / implementation attacks, eavesdropping, jamming	Secure and authenticated communication protocols; robust key management and PKI; quantum-based key distribution; frequency hopping and adaptive beamforming; error-pattern-embedding steganography for covert communication; network-level rate limiting and traffic engineering; distributed intrusion detection and rapid incident response	[31], [37]–[39], [53]
Data-based	AI/ML poisoning, environmental perturbation, data tampering, data injection, quantum attacks on data confidentiality, Sybil, spoofing, data-plane malware	Data validation and sanitization; adversarially robust training and anomaly detection; multi-sensor fusion frameworks (e.g., SADC) for detecting inconsistent sensor readings; tamper-evident logging via blockchain / DLT; post-quantum cryptography and QKD; proof-of-location and trust frameworks for identity validation; AI-driven intrusion detection at edge and cloud	[41], [42], [54]–[60]
Device-based	SDR spoofing, physical tampering, supply-chain insertion, timing / side-channel attacks on TPM and crypto modules	Secure hardware design and attestation; ISAC-based device fingerprinting; PUF-based device authentication; secure boot and signed firmware; post-quantum secure key exchange and firmware signing; constant-time cryptographic implementations and timing randomization (e.g., PerRand); environmental hardening and tamper detection for critical devices	[24], [43], [58], [61]–[63]
Application-based	Smart contract exploits, consensus attacks, false-data injection into applications, evasion and model-stealing attacks on AI models	Formal verification and secure design of smart contracts; multi-signature and role-based controls for critical transactions; resilient hybrid consensus (e.g., PoW–PoS–BFT) for blockchain-based ITS; AI-based anomaly detection and digital twins for behaviour monitoring; adversarially robust model training, input filtering, and output sanity checks; query authentication and rate control to protect ML APIs	[44], [45], [64]–[66]
Quantum-based	Quantum key stealing, coherent and Trojan-horse attacks, MDI attacks, quantum-enabled key cloning	Deployment of post-quantum cryptographic schemes for long-term protection; secure QKD implementations with monitoring of side channels; quantum-safe key management policies; quantum random number generators; continuous monitoring and auditing of quantum channels and devices	[42], [46], [47]
Privacy invasion	Tracking and profiling via location data, sensor fusion, side channels, and metadata; re-identification from aggregated datasets; misuse of monetized vehicular data	End-to-end encryption and strict access control; strong pseudonym management and identity protection schemes tailored to V2X; data minimization and purpose limitation; anonymization and pseudonymization; differential privacy for statistics and model updates; governance and regulation for data marketplaces and cross-border data sharing in ITS	[1], [19], [25], [36], [48]–[52]

- Malware: Enhanced threats employing AI-driven evasion techniques, propagating across edge-to-cloud infrastructure [1].

3) DEVICE-BASED ATTACKS

Device-level attack surfaces encompass interconnected hardware, including Software Defined Radio (SDR) systems providing programmable wireless communications, Lidar systems serving as environmental perception sensors, and Trusted Platform Module (TPM) systems serving as hardware-based security anchors managing increasingly complex responsibilities in 6G environments. The following are some of the attacks in this category:

- Spoofing: Exploiting programmable radio interfaces to forge device identities and manipulate wireless signals.
- Physical attacks: Physical destruction or alteration of devices [24].
- Supply chain attacks: Compromising device integrity during manufacturing by introducing hardware trojans or malicious firmware [43].
- Timing attacks: Exploiting ultra-precise synchronization requirements to disrupt secure protocols and TPM operations.

4) APPLICATION-BASED ATTACKS

The application layer bridges user interactions, vehicle operations, and network services through OBUs managing vehicle-to-6G infrastructure interfaces, vehicle infotainment systems serving as passenger-network gateways, and blockchain technology securing operations through

consensus protocols and smart contracts. The following attack vectors are peculiar to applications in 6G-ITS The following are some of the application-based attacks:

- Smart contract attacks: Exploiting vulnerabilities in automated agreement systems, compromising vehicle services and traffic management [44].
- Consensus attacks: Manipulation of blockchain decision-making to gain control over validation mechanisms.
- Injection of False-data: Introduction of fabricated data in application processes [45].
- Evasion attacks: Create inputs designed to evade AI/ML model detection.
- Model-stealing attacks: Extracting trained models for malicious purposes [44].

5) QUANTUM-BASED ATTACKS

Quantum-based attacks in a 6G-ITS primarily target quantum-based technologies, such as QKD, which might be incorporated into the system to ensure the security of communication and data transmission. These attacks can be categorized as data-based attacks, as they can compromise system security by breaking the cryptographic protection of classical key-based systems, leading to data breaches, safety hazards, and other issues [46]. Furthermore, quantum-based attacks can also affect the security of applications and devices within the 6G-ITS ecosystem, potentially compromising vehicle systems or introducing malicious software [42]. This highlights the cross-cutting nature of quantum-based threats and their ability to impact multiple layers of the 6G-ITS architecture.

Examples of quantum-based attacks include quantum key theft, coherent attacks, Trojan-horse attacks, Measurement-Device-Independent (MDI) attacks, and quantum-safe key cloning attacks [46], [47]. These attacks exploit the vulnerabilities of quantum-based technologies to intercept, manipulate, or clone cryptographic keys, bypassing the security measures meant to protect the 6G-ITS system. Countermeasures against quantum-based attacks include migration to post-quantum cryptography, secure deployment of QKD, quantum-grade randomness, and cross-layer monitoring of quantum channels and devices [42], [46], [47]. Their role across 6G-ITS layers is summarised in Table 4.

6) PRIVACY INVASION

Privacy invasion poses a serious threat to 6G-ITS. The massive amounts of data collected, communicated, and analyzed in ITS can contain sensitive personal information. If exploited by attackers, these data could enable tracking of individuals' movements and routines, profiling of their behaviors and preferences, and other violations of privacy [25]. The ubiquity of sensors and cameras for traffic monitoring and vehicle tracking and enforcement leads to widespread surveillance [19]. The connectivity density in 6G networks enables easy data aggregation [1], whilst data mining techniques can deduce additional intelligence from raw data. Key enablers include visual sensors collecting license plate or facial data, vehicular sensors gathering location and biometric data, and communication interfaces used to track vehicles [19]. Location inference attacks, such as those demonstrated in our work using robust geo-localisation techniques on distorted GAN-based camera datasets [48], side-channel attacks monitoring radio signals, and metadata aggregation from usage patterns all erode privacy when analysed [49]. Additionally, the 6G capabilities allow the monetization of vehicular data [50], where driving patterns, vehicle health, and travel locations could be sold to third parties, posing serious privacy risks without proper anonymization and consent [51]. Mitigating privacy invasion in 6G-ITS requires encryption and access control, strong pseudonym management, data minimisation, anonymisation, and differential privacy, complemented by appropriate regulatory and governance frameworks [36], [50], [51], [52]. Table 4 provides a high-level summary of these measures, while detailed privacy-preserving mechanisms are discussed in Section IV.

IV. PRIVACY LANDSCAPE IN 6G-ITS

Privacy protection in 6G-ITS faces unprecedented challenges as ITS sensors collect vast amounts of personal data through continuous vehicle monitoring, behavioral tracking, and precise location sensing. This section explores privacy-preserving technologies such as federated learning (FL) and differential privacy (DP), examines ethical considerations in data collection and monetization, and discusses frameworks for balancing system functionality with individual privacy rights.

A. PRIVACY-PRESERVING TECHNOLOGIES AND MECHANISMS

ITS uses advanced technologies such as sensors, communication networks, and data analytics to improve the efficiency and safety of transportation. These systems can generate large amounts of data about the movement of people and vehicles, which can be used for various purposes such as traffic management, route optimization, and public safety [25]. Therefore, privacy in ITS can be classified into three categories: identity privacy, behaviour privacy, and location privacy. Identity privacy pertains to the protection of user identification information, behaviour privacy involves safeguarding personal data generated by user actions, and location privacy pertains to the confidentiality of user location data [32], [52]. Privacy protection should be viewed as a crucial performance requirement and a fundamental component of wireless communication in the envisioned 6G era, as 6G systems will offer continuous connectivity approximately 1000 times that of 5G [37].

FL emerged as a promising solution. It is a decentralized machine learning paradigm enabling multiple devices to train a model collaboratively without sharing raw data with a central server [67]. FL offers several benefits, including preserving user privacy, reducing communication

costs, and improving scalability. FL can help mitigate privacy risks by allowing data to be processed locally on user devices while allowing the system to learn from the collective intelligence of all users [68], [69]. In V2X scenarios, FL can be integrated by having vehicles, roadside units, and edge servers train models locally–such as traffic prediction, anomaly detection, or cooperative perception–while only transmitting model updates rather than sensitive driving behaviours or location histories. These updates are aggregated at an edge or cloud coordinator, allowing the global model to improve without exposing raw vehicular data [70]. FL can be used to train predictive models for traffic congestion and accident prediction, route optimization, and other ITS applications. Barbieri et al. [67] explored the potential of the consensus-driven Federated Learning (C-FL) paradigm in V2X networks to provide communication-efficient distributed training services. C-FL typically performs well in dense networks with a large population of interconnected vehicles. However, the main challenges in FL design are device sampling, convergence and statistical heterogeneity, which can highly influence the quality of the trained models [69], [71]. FL convergence refers to how quickly and reliably the distributed learning process reaches a stable global model despite vehicles having different data and participation rates [72].

Future 6G wireless applications are likely to incorporate DP, another emerging privacy-preserving technology [1], [25]. DP offers mathematically proven privacy protection against certain attacks, including inference, linkage, and reconstruction. DP achieves this by adding carefully calibrated random noise–often Laplace or Gaussian–to aggregated outputs or model updates, ensuring that the inclusion or exclusion of any individual record changes the final result by no more than a privacy parameter ϵ. Formally, a mechanism M satisfies ϵ-DP if for any two datasets differing by one record and any output subset S, $\Pr[M(D_1) \in S] \leq e^{\epsilon} \Pr[M(D_2) \in S]$ [73]. This probabilistic bound guarantees that adversaries cannot confidently infer whether a specific driver, vehicle, or location trace contributed to the computation. Its properties, such as quantification of privacy loss, composition, and immunity to post-processing, make it attractive to enhance privacy in analyzing personal information [32]. Lightweight privacy-preserving techniques such as homomorphic encryption can also be used instead of traditional data encryption methods, providing the balance between maintaining the performance of high-accuracy services and protecting of user privacy [74].

Trusted privacy preservation techniques require that communication participants have confidence in a third party to process their data [37]. A Central Authority (CA), which can link and invalidate user certificates used in encrypted communication, could be the independent legal authority. Examples include authentication, VPN/tunnel encryption, anonymization, and pseudonymization [75]. Several other privacy-enhancing technologies, such as Secure Multi-party Computation (SMC) and threshold secret sharing, offer prospective solutions to 6G-ITS privacy preservation [76]. One potential application of SMC in ITS is in the context of accident detection and response. SMC can enable real-time analysis of road conditions and detect accidents by securely aggregating data from different sources, such as vehicle sensors and cameras [77]. This can then inform the deployment of emergency services and traffic rerouting to minimize disruption. Moreover, in threshold secret sharing, a secret is divided into multiple shares, each distributed among different nodes in the network. The secret can only be reconstructed when a certain threshold of shares is collected [76], [78]. This technique ensures that the secret remains secure even if some nodes are compromised.

In the 6G age, there is a greater risk that data collection and accessibility would undermine privacy protection and complicate regulatory issues. At the same time, edge intelligence aided by 6G changed the paradigm in how applications are developed and deployed. As a result, more sophisticated applications are being executed on resource-constrained mobile devices, increasing the risks of security attacks [74]. Consequently, safeguarding users' privacy on such devices has become a critical challenge. Therefore, it is imperative to incorporate lightweight and efficient privacy-preserving mechanisms. Maintaining a balance between the performance of high-accuracy services and user privacy protection is paramount. The realization of many intelligent applications requires access to sensitive user information, such as location and identity data. Hence, it is crucial to carefully consider data access rights and ownership and to establish effective mechanisms for supervision and regulation that ensure privacy protection.

B. ETHICAL CONSIDERATIONS FOR 6G-ITS

The deployment of 6G-ITS raises fundamental ethical concerns that extend beyond traditional cybersecurity and privacy considerations. User consent emerges as a critical challenge, as the unprecedented data collection capabilities of 6G networks will enable continuous monitoring of vehicle occupants, travel patterns, and behavioral characteristics with centimetre-level precision. Traditional opt-in consent mechanisms prove inadequate for dynamic 6G-ITS environments where data usage contexts evolve in real-time based on traffic conditions, emergency situations, and automated decision-making processes [70]. The complexity of explaining AI-driven data processing to users in understandable terms further complicates informed consent, particularly when algorithmic decisions directly impact safety-critical transportation functions.

Algorithmic fairness and bias present additional ethical challenges as 6G-ITS systems increasingly rely on machine learning for traffic optimization, route planning, and resource allocation. These systems risk perpetuating or amplifying existing transportation inequalities if training data reflects historical biases in infrastructure development, service provision, or mobility patterns across different

socioeconomic groups. The automated nature of 6G-ITS decisions makes bias detection and correction particularly challenging, especially when decisions occur within sub-millisecond timeframes that preclude human oversight [79]. Real-world evidence already points to the sensitivity of these issues. Independent investigations, such as the Mozilla Foundation's 2023 report, highlight that modern connected vehicles can collect highly granular personal information, extending in some cases to intimate lifestyle inferences [80]. Although such reports focus on current generation systems, the data collection capabilities in 6G-enabled ITS, combined with enhanced AI-driven analytics, will only amplify these risks if not governed by enforceable ethical frameworks.

Beyond these foundational concerns, emerging 6G-ITS architectures are likely to enable new economic models such as vehicle data marketplaces, where vehicle-generated data, ranging from traffic flows and sensor readings to in-cabin behavioral metrics, are monetized among stakeholders [81]. These models present potential incentives for data sharing and could fund infrastructure improvements or reduce vehicle costs; however, they simultaneously raise ethical and regulatory concerns about user consent, equitable distribution of value, and protection against exploitative practices [70]. The inconsistency of global regulations further complicates these issues, as data monetization policies permissible in one jurisdiction may violate privacy rights in others, creating complex compliance challenges for global transportation systems. Operationalizing ethical frameworks for 6G-ITS requires integration of privacy-by-design at the architectural level, dynamic consent management that allows drivers to granularly approve or revoke specific data uses, and transparent revenue-sharing mechanisms that recognize drivers as active stakeholders rather than passive data sources. Additionally, algorithmic accountability measures must ensure that automated decisions can be audited, explained, and contested, particularly in safety-critical scenarios where system failures could have life-threatening consequences. Embedding these safeguards into the 6G-ITS design ensures that privacy protection moves beyond compliance checklists to a verifiable and enforceable practice that balances innovation with individual rights, even in heterogeneous regulatory and cultural landscapes.

V. TRUST LANDSCAPE IN 6G-ITS

Trust is fundamental to the secure operation of 6G-ITS, where autonomous entities must reliably interact across heterogeneous, decentralized networks. This section explores the theoretical foundations of trust, examines governance frameworks and standardization efforts, and discusses key enabling technologies that shape trust management in next-generation intelligent transportation systems.

A. TRUST FUNDAMENTALS AND GOVERNANCE FRAMEWORK

Trust, while inherently abstract and challenging to define with precision, constitutes a fundamental component of interactions among distinct autonomous entities. In social environments, where individual behavior remains unpredictably variable, trust facilitates action by replacing the overwhelming intricacies of these contexts with predictive representations [6]. Thus, trust effectively reduces the infinite complexity of social scenarios to more manageable expectations about the probable conduct of others [28].

The promise of 6G-powered ITS ecosystems is critical to engendering comprehensive trust spanning the technological, governance, and social spheres. The primary concerns revolve around establishing robust trust in the face of these novel integrations, ensuring reliable and secure communication in a dynamic and heterogeneous network environment [47]. The extensive connectivity and virtualization of 6G systems will require trusted mechanisms to manage service agreements and transactions on a massive scale. For example, blockchain solutions could facilitate decentralized billing and charging without intermediaries, as well as establish reliable service level agreements between virtual slices [82], [83], [84]. However, implementing such large-scale trust networks remains an open challenge [85]. In addition, ubiquitous sensors and data exchange in emerging intelligent transportation use cases raise critical privacy and security concerns. The sheer volume of spatial, visual, and contextual data from vehicle sensors enables unprecedented tracking and profiling [86]. If not protected properly, this data could enable harassment or stalking. Furthermore, manipulated sensor data injection could severely impact safety systems and trigger accidents. As such, stakeholders in the 6G ecosystem need stringent and resilient trust frameworks to preserve privacy, guarantee authenticity, and prevent misuse along the physical-digital boundary between vehicles, edge networks, and central clouds.

Decentralized networks such as VANET mobile networks require resilient trust management mechanisms that can function effectively despite vulnerabilities from within the network itself [28]. Traditional centralized methods of ensuring trust falter in such contexts. To enable robust decision-making at the node level, trust and reputation models must ingest direct evidence from local interactions and indirect inputs gathered through peer recommendations [16]. A trust calculation subsequently combines these multi-faceted evidence sources to determine a confidence score. In practice, many ITS trust models quantify trust using normalized scores between 0 and 1, where values above 0.7 denote high-trust nodes suitable for routing or data fusion, while nodes falling below 0.3 may be isolated or quarantined [87]. Bootstrapping schemes handle the cold start problem by initializing new entities with neutral scores that get refined over time [28]. Various computational approaches power this evidence-gathering and trust calculation pipeline, including neural networks [6], Bayesian [88], entropy or probability-based methods [89]. For example, Bayesian trust methods update a vehicle's trust score using likelihood ratios, where consistent behavior over time strengthens posterior trust, while erratic or malicious

TABLE 5. Trust aspects and considerations in 6G-ITS.

Aspect	Key technologies	Trust challenges	Trust solutions	Application scenarios
Technological trust	• AI/ML • Blockchain / DLT • Quantum Computing • Advanced Wireless (THz, VLC, MIMO, IRS)	• Interoperability • System-wide robustness • AI bias and explainability • Quantum-safe cryptography integration	• Rigorous evaluation frameworks • Quantum-resistant algorithms • Federated learning • Physical layer security	• Autonomous vehicle coordination • Smart traffic management • Predictive maintenance
Network trust	• NFV • VLC • MEC • ISAC • dMIMO • IRS	• Expanded attack surface • Resource isolation • Edge node security • Frequency interference and jamming	• Network slice isolation • Distributed ledger for configurations • Zero-trust architecture	• V2X communication • Remote surgery • Augmented reality navigation
Data trust	• Blockchain • Federated Learning • Homomorphic Encryption	• Data privacy • Data integrity • Unauthorized access	• Differential privacy • Secure multi-party computation • Blockchain for data provenance	• Vehicular data monetization • Personalized traffic services • Collaborative sensing
Governance trust	• Smart Contracts • Decentralized Identity	• Regulatory compliance • Cross-border interoperability • Liability attribution	• Standardization (e.g., ETSI TS 102 941) • Regulatory frameworks (e.g., GDPR for 6G) • Automated compliance checking	• Automated insurance claims • Dynamic road pricing • Cross-border vehicle authentication
Social trust	• Explainable AI • Privacy-Enhancing Technologies • Human-Machine Interfaces	• Public perception • Ethical considerations • User acceptance	• Transparent AI decision-making • User-centric design • Ethical guidelines and frameworks	• Trust-based ride-sharing • Ethical routing choices • Community-based traffic reporting

behavior causes rapid score decay. The fusion of direct and indirect trust inputs lends hybrid resilience to decisions in decentralized environments. Operationalizing these schemes, however, remains an open research challenge.

As a result of these challenges, standardization bodies such as the Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI) formulated specifications around security and trust assurances in ITS. Notable among these efforts is ETSI TS 102 941 [90], which outlines a comprehensive trust framework spanning identities, cryptographic policies, and certification roots tailored to the automotive context. In its second iteration, this standard delineates trust relationships between ecosystem entities, stipulates protocols for maintaining verified credentials necessary for secure communication, and establishes collaborative trust anchor models, allowing multiple certificate authorities to interoperate within the same Web of trust. The accompanying ETSI TS 102 940 guideline consolidates these specifications into a reference architecture that codifies best practices for trust establishment, maintenance, and cryptography for integrity and resilience. As ITS components become mainstream, rigorous adoption of such standards will be pivotal to managing trust across the complex partnerships between vehicles, infrastructure, networking components, and mobility service providers. Table 5 describes the trust aspects and their considerations regarding the 6G-ITS ecosystem.

B. KEY ENABLING TECHNOLOGIES AND TRUST IMPLICATIONS

While the technical details of 6G systems are still being researched and standardized, several key technology enablers have become clear. The emergence of the 6G network will provide breakthrough advances in speed, capacity, security, and intelligence compared to existing 5G infrastructure. These capabilities have significant potential to foster trust in next-gen ITS.

1) ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TECHNOLOGY

Integrating AI/ML into the design and orchestration of next-generation 6G wireless networks is poised to revolutionize intelligent transportation. The era of self-driving vehicles, fully connected infrastructure, and intelligent fleet coordination promises an unprecedented change in the way humans and goods travel - driven by the unique capabilities of AI/ML [91].

At its core, the explosive advancement of AI, especially deep neural networks, was driven by the availability of enormous data volumes, computational muscle, and ingenious algorithms modeled after human cognition [51], [91]. 6G unlocks the mammoth connectivity bandwidth and ultra-low latency required to realize a fully AI-first future. Autonomous systems powered by reinforcement learning, decentralized edge intelligence that ensures lightning-fast response times, and generative models that convert data into realistic environment simulations - all were hitherto constrained by 4G/5G limitations [92], [93].

The breadth of intelligent transportation use cases poised to be revolutionized by AI/ML in 6G networks is immense. Traffic flow optimization will become much more reliable through predictive modeling on rich datasets [12]. Almost new forms of real-time vehicular coordination will be unlocked by AI-assisted V2X communication protocols [87], [94]. Self-driving technology could achieve responsiveness, rivaling human drivers through sensor fusion and computer vision [22]. Smart city infrastructure, from adaptive traffic signals to self-diagnosing components to automated parcel-sorting facilities, will become more intelligent and efficient [95]. Recent advances demonstrate that fuzzy-logic-assisted Q-learning (FAQ) models can dynamically allocate physical-layer resources to maximize network throughput while maintaining ultra-low latency and high reliability for diverse vehicular applications [96]. This

approach addresses a fundamental challenge in 6G-ITS, specifically how to intelligently distribute limited spectrum resources among concurrent V2X services. These services range from safety-critical collision avoidance, which requires ultra-low latency, to bandwidth-intensive cooperative perception, which demands high data rates, and infrastructure monitoring, which necessitates high reliability. The fuzzy logic component enhances the speed of learning convergence compared to traditional reinforcement learning and facilitates real-time adaptation to the dynamic conditions of vehicular networks.

A key shift is that 6G will enable more decentralized peer-to-peer communication, unlike current client-server models where the server is the presumed reliable component [97]. This requires participants to engage directly with one another through heterogeneous AI systems. Such multifaceted AI integration across smart transportation networks poses emerging challenges around interoperability, system-wide robustness, and auditability [45], [98]. With automotive and transit functions becoming increasingly software-defined, rigorous validation of AI components and their interactions is essential to fostering trust at both the technical and social levels [85].

From a technical perspective, trust establishment begins with rigorous evaluation frameworks to quantify confidence in AI/ML components and multi-agent systems [99]. Quantitative trust metrics and benchmarks are needed, covering performance, robustness, security, explainability, and ethics [100]. Data veracity and integrity are other key trust factors - with decentralized aggregation, ensuring training data comes from reliable sources is imperative [99]. Ongoing trust management entails continuous auditing and adaptation as transportation environments and threats evolve [100].

Standards bodies have a role to play in devising interoperability and certification schemes for trustworthy AI agents to interoperate securely, particularly in safety-critical control functions [86], [101]. Isolating mission-critical communications on verifiably secure network slices can mitigate risks [101]. Cybersecurity measures like encryption and access control remain essential to prevent spoofing, denial-of-service attacks, or hijacking. Several studies, e.g., [27], [83], [84], [85], [89], [102], [103], proposed methods to enhance trustworthiness in a 6G heterogeneous network. The authors of [84] proposed a scheme, “6blocks”, where trust is managed and enhanced through a combination of blockchain technology, 6G sensors, and NFV. Blockchain ensures decentralized and transparent transactions, enhancing trust and security. The 6G sensors contribute to secure data aggregation, while NFV aids in efficient data processing and resource provisioning. Additionally, the system uses smart contracts for management operations, further ensuring security and trustworthiness in the network.

The integration of AI, specifically Generative Adversarial Networks (GANs), into trust management for 6G networks is explored in [89]. It introduces a novel framework combining fuzzy logic and adversarial learning for intelligent trust management. The paper reviews existing AI-based trust management schemes, proposes a GAN-based trust decision-making model, and applies it to secure clustering for reliable and real-time communication.

The requirement of incorporating trust into the 6G network’s design is examined in [89]. It emphasizes the importance of trust in the merger of the digital and physical worlds, highlighting security risks and the need for robust security measures. The paper proposes a framework for embedding trust into the network, focusing on end-to-end connectivity and reputation-based trust management. It also compares current Internet communication patterns with the proposed 6G framework, emphasizing the need for a paradigm shift in network trust and security approaches.

Beyond technical factors, public trust relies on responsible and ethical development practices [85]. Humans tend to calibrate risks in AI failures, causing distrust [99]. Regulations addressing liability attribution, safety standards, and transparency requirements around the use of personal data are thus crucial. Social and legal frameworks, such as the General Data Protection Regulation (GDPR), that protect public trust regarding digital privacy must be scaled to cover the additional use cases and business opportunities that 6G will birth. For example, data monetization platforms will need guidelines on who owns the generated data and who can sell and profit from processing such data. Also, insurance companies must determine who is liable if autonomous driving fails, resulting in a claim incident. Achieving these regulatory oversights and manufacturer liability provides accountability if mishaps occur. Therefore, AI/ML technologies promise to revolutionize 6G-ITS. Their success will largely depend on achieving a delicate balance between technical innovation and ethical, transparent practices. It is imperative to foster an environment where trust in delegating operations for AL/ML in 6G-ITS is as strong as the technology itself.

2) WIRELESS BRAIN-COMPUTER INTERACTION

The concept of wireless brain-computer communication is a topic of interest in the context of 6G-ITS. Wireless brain-computer communication involves using electroencephalography (EEG) signals to enable direct communication between the human brain and computer systems [24]. This technology can provide a more natural and intuitive way of interacting with technology, particularly in applications related to ITS. For example, wireless brain-computer communication could control various functions through brain signals, such as steering or braking. This emerging technology has the potential to revolutionize the way we interact with technology and our environment. With the development of 6G networks, there is an opportunity to explore the integration of wireless brain-computer communication in ITS applications [22]. Wireless brain-computer technology will enable brain-controlled vehicles (BCV) to help people with disabilities experience increased independence [104].

However, implementing wireless brain-computer communication in 6G-ITS applications also presents significant security, privacy, and ethical challenges. Given the sensitive and personal nature of the data involved, appropriate security measures are needed to protect against unauthorized access or manipulation. Additionally, ethical concerns must be considered, such as issues related to consent and the potential for unintended consequences [22], [104].

3) QUANTUM COMMUNICATION AND COMPUTING FOR 6G-ITS

Quantum computing holds significant promise for bolstering trusted communications in 6G-ITS. By harnessing quantum mechanical phenomena like superposition and entanglement, quantum algorithms can enable cryptography to resist attacks from powerful future quantum computers [42]. Exploiting quantum parallelism and entanglement, quantum algorithms can break cryptography long considered unassailable, jeopardizing legacy security protocols [105], [106]. Quantum key distribution offers a path to trusted communications that are resistant even to quantum attacks [107]. However, seamless integration with classical networks and devices remains an open challenge [47].

On the flip side, quantum computing could bolster security and trust mechanisms with new capabilities. Quantum machine learning shows potential for anomaly detection in complex real-time data, identifying early indicators of malfunction or intrusion [108]. Entangled quantum sensor networks may achieve orders of magnitude enhancement in sensitivity for integrity checks on critical infrastructure [109]. And post-quantum cryptographic primitives theoretically outside the reach of quantum brute forcing are rapidly maturing [42], [107]. Navigating this quantum computing nexus requires a multilayered approach balancing legacy compatibility, future-proofing, and pragmatic transition. Hybrid asymmetric schemes mixing quantum-safe and conventional cryptography provide a migration path as post-quantum standards co-evolve with the technology. Isolating security-critical applications like V2X coordination onto verifiably secure network slices can contain risks [107]. Blockchain-based consensus offers decentralized trust roots that are less dependent on computational hardness assumptions [109].

The quantum paradigm necessitates upgrading computational trust protections for 6G transportation foundations. But judiciously leveraged, quantum techniques can also significantly improve resilience, confidentiality, and reliability - promoting user acceptance. Collaborative efforts between automotive, telecom and quantum stakeholders provide the ideal environment for co-designing trusted mobility networks. The duality of quantum computing's impact means that while it can greatly improve the efficiency and security of 6G-ITS it also necessitates a proactive approach to updating and fortifying current cryptographic standards to maintain network integrity and trust.

4) ADVANCED WIRELESS COMMUNICATION TECHNOLOGIES

The development of advanced wireless communication technologies like terahertz [110], light fidelity (Li-Fi) [111], cell-free massive multiple input multiple outputs (MIMO) [12], and intelligent reflecting surfaces (IRS) [112] will enable ultra-fast, secure, and reliable connectivity for future 6G-ITS.

Terahertz band communication is a promising wireless technology for 6G that can enable the high data rates and wide bandwidths needed for real-time coordination between vehicles, infrastructure, and devices in ITS [110]. By operating at frequencies between the mmWave and infrared bands, terahertz provides far greater spectrum resources than existing wireless technology. This vast bandwidth can satisfy the capacity demands of future mobility ecosystems, potentially reaching transmission speeds up to terabits per second [12], [110]. The tiny wavelengths of terahertz signals also permit the integration of thousands of antenna elements into compact base station arrays [12]. This massive MIMO capability allows the forming of highly directional beams to service many simultaneous users while minimizing co-channel interference reliably [22].

From a trust and security perspective, the focused energy and limited penetration of terahertz beams inherently resist eavesdropping, enhancing privacy [24]. This prevention of unauthorized access aligns with integrity goals for safety-critical vehicle-to-everything communication. However, designing efficient components like antennas and transceivers at such high frequencies remains challenging [22]. Further research is needed to make terahertz systems economically viable at scale. And seamless integration with networks at lower frequencies will be crucial for ubiquitous coverage across transportation infrastructure. Suppose the complexity and power efficiency barriers can be overcome. In that case, terahertz communication promises to provide the secure ultra-high capacity connectivity required to unlock 6G's potential for next-generation intelligent mobility.

Visible light communication (VLC) is an emerging wireless technology that uses LED light sources for high-speed wireless data transmission [111]. By modulating visible light signals, VLC can offer fibre-optic-like bandwidth without requiring the installation of physical cables [22]. This makes it highly promising for vehicle-to-vehicle and vehicle-to-infrastructure communication within intelligent transportation ecosystems.

Since VLC signals do not penetrate opaque objects, connections are inherently confined to intended recipients within direct line-of-sight [111]. This localization enhances security and privacy compared to RF links [26]. Interference is also avoided by spatial reuse of frequencies [111]. With thousands of LEDs integrated into vehicles and smart infrastructure, VLC could enable terabit aggregate data rates for real-time coordination and content sharing as required by future

autonomous mobility services. However, some challenges remain in efficiently harnessing VLC for transportation. Commercial LEDs have narrow modulation bandwidths, requiring enhancement [111]. Robust multi-input multi-output techniques must be developed to overcome limited diversity vulnerabilities [26]. Seamless integration with RF networks is needed where line-of-sight is obstructed. VLC promises to provide the speed, security, and reliability needed to establish trusted links between myriad intelligent devices across 6G transportation ecosystems.

Massive MIMO beamforming is an emerging wireless technique that utilizes large antenna arrays for highly directional signal transmission and reception [24], [111]. By steering focused energy beams, massive MIMO enables spatial reuse where multiple users can simultaneously utilize the same frequencies without interference [113]. This significantly enhances spectral efficiency and capacity compared to omnidirectional broadcasts.

For 6G intelligent transportation, massive MIMO beamforming offers important trust and security advantages. Focused directional beams provide reliable, ultra-high-speed links between vehicles, infrastructure, and devices by confining signals only where needed. This resists eavesdropping or data interception, enhancing privacy [94], [113]. The high gain also compensates for path loss at higher frequencies like mmWave and terahertz, which are envisioned for 6G [94]. Additionally, interference is minimized as directional transmissions avoid overlapping with other links [2]. While promising, real-world mobility environments pose challenges. Maintaining precise beam alignment requires tracking mobile nodes and adapting beams dynamically [112]. Blockage from buildings or vehicles can disrupt links [112]. Scaling up low-cost antenna arrays with reliable phase synchronization is non-trivial. And seamless integration with omnidirectional networks is necessary to prevent coverage gaps [113]. If these hurdles can be overcome, massive MIMO beamforming is poised to deliver the speed, security, and scalability needed to realize the trusted connectivity potential of 6G transportation.

Distributed MIMO (dMIMO) extends traditional MIMO systems by decentralizing antenna arrays across multiple access points (APs) [114]. This architecture enhances signal reliability, coverage, and capacity, making it suitable for 6G-ITS [115]. dMIMO's cooperative nature enables dynamic adaptation to channel variations, ensuring efficient resource use and mitigation of interference. dMIMO can support high-density vehicular networks by providing more uniform coverage and reducing the impact of signal blockages. By strategically placing antenna elements throughout the transportation infrastructure, dMIMO can ensure reliable vehicle connectivity, even in challenging environments like urban canyons or tunnels [116], [117]. The distributed nature of dMIMO also allows for more efficient use of power, as antenna elements can be dynamically activated or deactivated based on traffic demands and vehicle locations [118].

ISAC is a crucial enabler in 6G networks, integrating sensing with communication infrastructure for efficient spectrum use and enhanced data accuracy in ITS operations [119]. This integration reduces the attack surface by having fewer points of potential compromise compared to separate systems [120]. ISAC employs advanced encryption and secure signal processing to protect data integrity and prevent eavesdropping, though it must also guard against spoofing attacks that could mislead sensing functions [121]. The environmental data collected by ISAC can potentially be exploited for unauthorized tracking. Ensuring privacy requires robust data anonymization and strict access controls. Designing ISAC systems with privacy-by-design principles, such as minimal data collection and end-to-end encryption, helps mitigate privacy concerns [122], [123]. Trust in ISAC is built on system reliability and data accuracy. Bidirectional authentication ensures that devices and infrastructure verify each other's identities, preventing attacks from fake base stations [118], [123]. Additionally, machine learning algorithms can detect anomalies and security threats in real-time, further enhancing trust [120].

Intelligent reflecting surfaces (IRS) are an emerging technology comprised of software-controlled metamaterials that can dynamically alter how impinging radio waves are reflected and directed []. By adjusting the phase shifts applied by a dense array of IRS elements, wireless signals can be precisely steered to intended recipients while minimizing undesired scattering. This allows wireless environments to be reconfigured and optimized in real-time based on changing conditions [124].

In 6G-ITS, IRS offers promising opportunities to isolate trusted device groups selectively, reinforce signal strength only where needed, and null interference or eavesdroppers [112]. IRS could also enable rapid beam retargeting for reliable vehicle-to-infrastructure links during high-speed mobility [124]. Integration of IRS with AI/ML and massive MIMO techniques can further augment adaptivity, tuning propagation intelligently. However, seamless coordination across large dynamic IRS networks poses challenges, including channel modelling, optimal phase configuration, mobility management, and cost-effective fabrication [112], [124]. The software-defined nature of the IRS also introduces potential vulnerabilities if not properly secured. Failures or misconfigurations could disrupt critical links [112]. Moreover, the complexity of unpredictable signal interactions in complex transportation environments may limit real-world deployments [124]. Several papers [8], [125], [126] highlighted the security threats and vulnerabilities associated with IRS-aided networks. These threats include jamming attacks using adversarial IRSs, pilot contamination attacks (PCA) exploiting IRS to enhance eavesdropping capabilities, and metasurface manipulation attacks (MSMA) manipulating metasurface behaviour for malicious purposes. The implications of these threats on the IRS are substantial, as they expose the vulnerability of IRS-aided wireless systems to various forms of attacks that can compromise

the security, privacy, and reliability of communications, highlighting the need for developing robust security measures and countermeasures specifically designed for IRS-aided networks. While still in a developmental phase, IRS represents a revolutionary paradigm shift that could give 6G communications unprecedented control over the wireless medium.

The advanced wireless communication technologies discussed above, such as terahertz, VLC, massive MIMO beamforming, dMIMO, ISAC, and IRS, offer promising solutions for ultra-fast, secure, and reliable connectivity in 6G-ITS. However, as these technologies evolve and become more complex, ensuring the security, privacy, and trust of the transmitted information becomes increasingly critical. Physical layer security (PLS) emerges as a crucial first line of defence, exploiting the inherent randomness of wireless channels to secure communications without relying solely on traditional cryptographic methods [127]. PLS schemes were proposed for various 5G and beyond technologies, aiming to enhance the security performance of heterogeneous networks, device-2-device (D2D) communications, IoT, and other aspects of 6G-ITS [128]. The integration of PLS with advanced techniques such as non-orthogonal multiple access (NOMA), IRS, and machine learning showed great potential to achieve better security performance [128], [129]. One promising approach to improving spectrum and energy efficiency in 6G networks is the integration of NOMA and Reconfigurable Intelligent Surface (RIS) techniques. Studies investigated the PLS for RIS-aided NOMA 6G networks, considering both internal and external eavesdropping scenarios. Researchers proposed joint beamforming and power allocation schemes to improve system PLS when dealing with untrusted near-end users attempting to intercept far-end user information. In both internal and external eavesdropping scenarios, noise beamforming and optimal power allocation schemes were introduced to enhance the system's physical security, even without channel state information (CSI) for the eavesdroppers [130]. However, the practical implementation of PLS in 6G-ITS faces challenges, such as managing security across diverse devices, efficient resource allocation, and adapting to dynamic environments [129], [131]. Future research should focus on addressing these challenges and developing comprehensive security frameworks that integrate PLS with higher-layer security measures to ensure the trustworthiness of 6G-enabled intelligent transportation systems.

5) MOBILE EDGE COMPUTING (MEC)

The proliferation of intelligent mobility applications relying on immense volumes of latency-sensitive vehicular data warrants deeper edge computing integration in 6G ecosystems through multi-access edge computing (MEC) platforms [83]. By embedding compute, storage, and analytics closer to autonomous vehicles, drones, and transportation infrastructure, sub-millisecond critical decision-making can be facilitated while smoothing core cloud burdens [132]. MEC's localized intelligence also aids predictive traffic optimization, vehicle coordination, and dynamic network resource allocations to serve native contextual demands better [133]. However, the radically enlarged edge attack surface risks magnifying vulnerabilities [69]. Ensuring reliable hardware roots-of-trust, compartmentalization integrity between slices sharing resources, and securing inter-edge mobility handoffs grows pivotal. With autonomous vehicles bearing lives, prudent threat modelling spanning communication and computing techniques that smartly fuse edge autonomy with cloud supervision minimizes risks.

6) BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY (DLT)

Blockchain and distributed ledger technologies offer promising trust mechanisms for 6G transportation ecosystems by establishing decentralized consensus and immutable transaction records between entities [82]. DLTs provide transparency and prevent data tampering or forgery, aligned with security and integrity goals [83]. Blockchain will facilitate the transition from centralized client-server architectures to trusted peer-to-peer networks for intelligent transportation. As described in [82], [103], blockchain and distributed ledger technologies (DLT) can enable the next generation of distributed sensing and coordination for advanced mobility services based on decentralized trust mechanisms rather than centralized intermediaries.

To fully realize the potential trust benefits, the demanding connectivity requirements of blockchain-based transportation applications will necessitate a synergistic combination of capabilities enabled by 6G networks [84], [103]. Ultra-reliable, low-latency communications will provide the real-time data exchange and consensus needed to foster dynamic trust between vehicles, infrastructure, and other endpoints [103]. Massive machine-type communications will deliver the scalability to support potentially billions of transported entities and infrastructure endpoints within these trust frameworks [134]. There are several opportunities for implementing blockchain and DLT in 6G-ITS:

- Decentralized identity management for vehicles, drivers, and infrastructure components enables authenticated and authorized access to transportation networks. DLTs allow interoperable yet privacy-preserving identification.
- Secure over-the-air software updates, where the integrity of firmware upgrades and vehicle vulnerability patches can be verified through blockchain-based provenance tracing and code attestations.
- Supply chain transparency and efficiency improvements via shared ledgers tracking location, condition and freight handling in real-time across multi-party logistics flows.
- Insurance claim processing can leverage automated execution of coverage rules and payment settlements via smart contracts in case of accidents, delays, and vehicle failures.

- Electric vehicle charging and billing mediated through cryptocurrency payments [135] without a central clearing house using Vehicle-to-Grid integration platforms.
- 5G/6G network slice brokers governed in a decentralized architecture through blockchain for on-demand quality-of-service guaranties to latency-sensitive or high throughput applications.
- Mesh networks and spectrum sharing orchestrated securely between transportation stakeholders, leveraging distributed consensus and incentives for cooperative behaviours.
- Community sensor data exchange platforms to share traffic, weather, or pollution alerts in common ledgers while preserving data ownership rights.
- vehicular data monetization [70] whereby connected vehicle owners can take ownership of their data and trade it in a peer-to-peer manner.

As 6G systems scale exponentially in complexity, blockchain and DLTs can crucially offer transparency, auditability, automation, and coordination across such intricately interconnected ecosystems in a trusted manner. Table 6 enumerates the opportunities, privacy, and security challenges of key 6G enabling technologies and their application in the ITS environment.

7) NETWORK FUNCTION VIRTUALIZATION (NFV)

Regarding infrastructure, NFV is expected to play a significant role in 6G-ITS by enabling the virtualization of network functions traditionally carried out by proprietary physical devices [136]. The flexibility and agility offered by NFV can provide benefits such as efficient computing resource utilization, faster deployments and updates, reduced costs, dynamic scaling to meet fluctuating demands, and enhanced resiliency through virtualized redundancy and failover capabilities [136], [137]. The scalability and flexibility inherent in NFV provide a robust framework for ITS to adapt to varying traffic conditions in real-time [93]. This dynamic allocation of resources enables more efficient use of network capabilities, which is a crucial factor in modern, fast-paced, heterogeneous transportation systems. However, research showed that the vastly expanded attack surface from software pipelines, compatibility challenges posed by multi-vendor virtual network functions (VNFs), and resource isolation needs pose complex trust management challenges [28], [138].

With network slicing, isolated virtual slices can be devoted to specific use cases or tenants. This permits customized trust settings and service levels by logical partition rather than a one-size-fits-all network [16]. Slicing also aids scalability for massive device density. However, the programmability of NFV presents attack vectors like configuration tampering. Hardening virtualized infrastructure against threats is crucial. Distributed ledger-based platforms show promise in establishing immutable configurations and managing trust in software-defined ecosystems [86].

The security of ITS enabled with 6G and enabled with 5G is similar in that both systems must protect the communication and data being transmitted, processed and stored against various threats and attacks. However, there are several key differences between the security of 6G-ITS and 5G-enabled ITS.

One of the main differences between 6G-ITS and 5G-enabled ITS is the level of security required to protect high-speed and low-latency 6G communication [15], [139]. The increased data transmission speeds and low latencies of 6G would require more advanced security measures to protect against sophisticated cyberattacks and ensure the integrity and authenticity of the data. The application of new technologies is also a significant difference. mmWave and THz communications, which are relatively new technologies that are expected to be used in 6G, would present additional security concerns, such as defending communication channels and devices from jamming and spoof attacks [23], [106], [140].

Incorporating quantum-based technology is another distinction, necessitating new and sophisticated security methods like Quantum Key Distribution (QKD) to secure communication channels and quantum-resistant algorithms to thwart quantum-based cyberattacks. 5G technology successfully shaped the development of the next generation of ITS and mapped the demands required for integration and adoption with the cellular network through softwarization; however, there is still concern for security around the 5G architecture [3]. Another significant obstacle to the effectiveness and precision of security controls and monitoring solutions is the high degree of heterogeneity in the 5G-ITS network [140]. 5G-ITS must support various devices and a lot of network traffic. A network of this size can increase the attack surfaces and allow threats to travel to the main areas of the connectivity; this threat is also present in 6G-ITS, as 6G will support devices more loosely connected in a short range than 5G [25]. Consequently, it raises important questions about how to build reliable connections between devices and networks.

Currently, 5G networks are adequate for existing technologies [92]. However, limitations in speed, manual configuration, and network optimization make it unsuitable for supporting future applications and scaling up to accommodate many complex dynamic wireless networks [45], [141]. For example, emergency services in the ITS ecosystem need live feeds in almost real-time to attend to a situation remotely using uncrewed vehicles (UVs). This usually requires information transmission at a latency speed below 1ms; however, 5G offers only a 5ms latency [43]. Furthermore, as ITS services and applications become more integrated, the number of loosely connected nodes that must communicate as a unit is on the rise; therefore, network congestion could be a risk if 5G is unable to link such a number of devices, resulting in further delay in information transmission [132]. To avoid serious CAV connectivity failures, the 5G network topologies will be

TABLE 6. Opportunities and challenges of 6G-enabling technologies for ITS.

6G-enabling technology	Opportunities for ITS	Arising privacy concern	Security challenge	Use cases	Trust issue
Artificial Intelligence (AI)	Enhanced predictive intelligence and real-time decision making for autonomous systems, leveraging 6G's ultra-low latency and massive connectivity	Data collection, Data Anonymization, Data sharing	Increased complexity of AI models in 6G environments, Requiring more sophisticated security measures	Intelligent traffic management, Autonomous driving, Route and planning optimization, AI-driven network optimization and self-healing in 6G ITS infrastructure	Ensuring transparency and accountability of AI systems in ultra-dense, high-speed 6G networks
Wireless Brain-Computer Interactions	Driver Assistance, Accessibility, Cognitive workload management	Data storage and retention, Unauthorized access, Data disclosure	Authentication, Authorization, Integrity	Remote driving, Advanced Driver Assistance Systems (ADAS), Personalized in-vehicle entertainment	Trust in direct brain-computer interfaces, Privacy risks from neural data collection and use. Reliability and accuracy of brain-computer interface interpretations.
Quantum Computing	Optimization, Quantum sensors, Cybersecurity	Privacy-preserving computation, Data ownership	Malware attacks, Access control	Routing and navigation, V2X	Trustworthy integration with classical networks
Terahertz Communication (Thz)	High-speed communication, Improved sensing capabilities, Efficient spectrum utilization	Data retention, Unintentional radiation	Authentication, Interference, Encryption	Advanced driver assistance systems (ADAS), V2V, V2I	Reliability and consistency of Thz communication in diverse environments and maintaining privacy against potential eavesdropping due to its high-frequency signals.
Mobile Edge Computing (MEC)	Ultra-low latency edge processing and analytics, enabled by 6G's increased bandwidth and reduced latency	User profiling, Data breaches	Authentication, Access control and securing the vastly increased number of edge nodes in 6G networks	Real-time, AI-powered traffic management utilizing 6G's massive machine-type communications	Maintaining data integrity and privacy across a highly distributed 6G edge computing environment
Intelligent Reflective Surface (IRS)	Improved signal quality, Energy efficiency, Enhanced communication range	Location tracking, Data collection	authentication, confidentiality	V2I, Smart intersection management, Autonomous vehicle navigation	Secure coordination across large IRS networks
Blockchain and Distributed Ledger Technology (DLT)	Secure and reliable data sharing, Smart contracts for autonomous vehicles, Data security and privacy	Pseudonymity, Linkability	51% attacks, Lack of regulation	Traffic management, Vehicle identity and ownership, Decentralized ride-sharing	Consensus integrity, establishing trust in decentralized systems, reliability in SLA automation
Network Function Virtualization (NFV)	Flexibility, Scalability, Agility, Resiliency	Virtual appliance vulnerabilities	Expanded attack surface, Misconfiguration	On-demand network scaling, Hardware abstraction	Securing virtualized functions and pipelines

significantly based on the applications, quality monitoring, and security of the service providers [141]. Security must be carefully considered with 5G relying on identical mobile network networks and utilizing virtualization and multi-tenancy capabilities. The multiple levels of security and privacy concerns in 5G networks are as follows: The vulnerability between the gNB radio node and the Mobility Management Entity (MME) due to modified nodes exists in backhaul lines [140], core networks are more dynamic and susceptible to attacks due to SDN, NFV and cloud approaches, and edge networks are more vulnerable due to the heterogeneity of nodes and transitions between different access technologies [132], [142].

8) OPEN RADIO ACCESS NETWORK

Open Radio Access Network (O-RAN) is a key architectural enabler for 6G-ITS, offering disaggregated components, open interfaces, and intelligent control that reshape security, privacy, and trust requirements in vehicular environments. Its openness supports multi-vendor deployments but expands the attack surface for highly mobile V2X systems. Hierarchical O-RAN slicing–spanning 3GPP QoS classes, vehicle-type slices, and application-specific slices–creates security boundaries that can isolate safety-critical URLLC traffic but also risk cross-slice propagation if isolation fails [143].

Radio Intelligent Controllers (RICs) optimize V2X connectivity, yet their centralized analytics expose sensitive trajectory and behavioral data, enabling large-scale profiling if not properly protected [143], [144]. Near-RT RICs support millisecond-level xApps for mobility-aware handovers [145], but malicious or compromised xApps could intentionally disrupt emergency vehicle communication or destabilize platoons [146]. Differentiated multi-service scheduling improves Age of Information and throughput [147], yet raises trust concerns when safety-critical messages must be prioritized over infotainment under congestion. Dynamic slicing also requires continuous monitoring of vehicle demand and location, introducing privacy risks related to surveillance and mobility-data monetization [143]. Open interfaces and multi-vendor integration further introduce supply-chain trust challenges [144]. Comprehensive analyses identify over 60 high-risk O-RAN threats, including malicious xApps,

unauthorized RIC data access, and API misuse enabling injection of false V2X messages [148], [149].

Addressing these ITS-specific challenges requires a layered strategy. Zero Trust principles adapted for vehicular mobility mandate continuous re-authentication and context-aware access control tied to velocity, topology, and service criticality [150], [151]. Robust PKI and optimized TLS secure vehicle-to-O-RAN interactions and prevent rogue base-station attacks [152]. xApp vetting frameworks and post-quantum cryptography strengthen control-plane integrity and long-term security [47], [153]. To preserve privacy, federated deep reinforcement learning enables collaborative optimization of handovers and resource allocation while preventing raw trajectory data exposure to RICs [143]. Differential privacy can obscure identifiable mobility statistics while retaining optimization utility. For trust, blockchain-backed service-level commitments provide verifiable guarantees that safety-critical slices are prioritized, and transparent xApp decision logic allows independent auditability [147], [150]. Real-time trust scoring of RIC components supports fallback to distributed modes when anomalies appear, while physical-layer security techniques protect V2X links from eavesdropping [154]. Given sub-millisecond constraints, cryptographic and verification mechanisms must rely on hardware acceleration. Future directions include formal verification of ITS xApps, standardized multi-vendor security frameworks, and AI-based detection of attacks targeting vehicular functions [155], [156].

Table 7 presents a systematic comparison between 5G-enabled ITS and 6G, illustrating how technological advances enable enhanced security capabilities. Each feature comparison is accompanied by its cybersecurity implications and practical application scenarios. For example, while the increase in data transmission speeds from 20 Gbps to 1 Tbps primarily appears as a performance metric, it necessitates new security protocols to ensure data integrity and timely encryption for applications like remote driving. Similarly, the reduction in latency to sub-1 ms creates new security considerations around timing attacks that must be addressed for safe autonomous vehicle coordination. This interconnected analysis demonstrates how 6G's technological foundations both enable and require advanced security measures beyond those in 5G-ITS.

VI. 5G-ITS VS 6G-ITS SECURITY

The progression from 5G to 6G networks in ITS represents a significant evolution in security requirements and capabilities. Table 7 provides a comprehensive comparison of the security implications of 5G and 6G-ITS and application scenarios. This systematic analysis shows how each technological advancement in 6G not only enhances network capabilities but also introduces new security considerations that must be addressed. Building on this comparative foundation, the following section examines the specific challenges that emerge in 6G-ITS environments, particularly focusing on the fundamental issues of authentication and trust establishment in next-generation transportation networks.

A. 6G-ITS CHALLENGES

One of the main challenges that was identified during the survey is the scalability and flexibility of the existing authentication systems and their adaptability to ITS. As the number of entities interacting with the system increases, it becomes more difficult to manage, secure, and ensure that the right level of access is granted to the right components. However, the major contention is the increased number of loosely connected devices that 6G-ITS will support. To address this challenge, it is important to use secure and flexible authentication methods, such as multi-factor authentication, digital certificates, and PKI, that can scale to accommodate many entities without compromising security.

A major drawback for connecting several ITS components in a 6G environment is the authentication method currently being applied in VANET. 6G enabling technologies like IRS, VLC, Terahertz, and intelligent integrated computing (cloud and edge) will create an additional connectivity spectrum for more cyber-physical systems. For example, VLC will enable features such as vehicle headlights and traffic lights to communicate with vehicles and other ITS components within the vehicular network. Also, live traffic update reports to vehicles can be delivered through IRS-enabled communication to base stations and other vehicles in the vehicular network. Therefore, a centralized structure such as the Trusted Authority (TA) scheme, mostly used by current authentication protocols, would prove inefficient and ineffective in maintaining data integrity and privacy security in real-time in such a mobile, geographically distributed and heterogeneous network environment. Likewise, the authentication and key agreement mechanism (AKA) present in third-generation partnership projects (3GPP) in 4G and 5G are insufficient to manage several authentication requests of vehicles at a time. Attempts were made to address this problem.

Ouaissa et al. [157] proposed an enhanced group authentication protocol for vehicular communications in 5G using the 5G-AKA and elliptic curve Diffie-Hellman algorithm. However, the varying security levels of ITS components mean that a symmetric cryptosystem utilized poses an inherent vulnerability of transmitting the same key needed to encrypt and decrypt.

Li et al. [158] proposed a platoon handover authentication scheme in 5G-V2X. The proposed scheme leveraged the Access and Mobility Management function of the 5G core network and created two platoon handover authentication schemes within the Access and Mobility Management Function (AMF) called inter-AMF and intra-AMF. The platoons authenticate with a software network controller when a platoon enters the coverage area of a target gNB from a source gNB and achieves the handover threshold. The gNBs in the 5G-Radio Access Network (5G-RAN) carry out the platoon handover authentication. This scheme can

TABLE 7. Comparison of 5G and 6G-ITS security implications and application scenarios.

Feature	5G	6G	Key differences in 6G	Cybersecurity implications of 6G	Application scenarios for 6G-ITS
Data Transmission Speeds	Up to 20 Gbps	Up to 1 Tbps and beyond	6G enhances speeds by over 50x, which is crucial for massive ITS data needs.	Increased speeds require new protocols to ensure data integrity and timely encryption.	Remote Driving and Real-Time Telematics: Real-time vehicle data handling for autonomous control.
Latency	Around 1 ms	Sub-1 ms	Reduction in latency by up to 90%, crucial for safety-critical operations in ITS.	Lower latency may expose systems to timing attacks unless security is adapted to operate within tighter time frames.	Autonomous Vehicle Coordination: Enables instant decision-making necessary for vehicle platooning.
Network Density	1 million devices/km²	10 million devices/km²	10x increase in device connectivity, supporting dense urban ITS deployments.	Higher device density intensifies the risk of DDoS attacks, necessitating more robust network defences.	Smart City Infrastructure: Comprehensive ITS deployment integrating traffic, safety, and emergency services.
Spectrum Efficiency	Utilizes up to 30 GHz	Expands to sub-terahertz bands (above 300 GHz)	Higher frequency bands increase bandwidth and connection density.	The expanded spectrum introduces a potential for more sophisticated eavesdropping and interference techniques.	AR and VR Services: Enhanced traffic management and navigation aids for drivers and public systems.
Reliability	99.999% availability	99.99999% availability	Enhanced network reliability through advanced technologies and AI integration.	Improved reliability reduces the risk of connection drops, which is crucial for maintaining continuous ITS operations.	Critical Emergency Response: Reliable communication for real-time coordination during safety incidents.
Security and Privacy	AES encryption standard	Quantum cryptography solutions	Implementation of quantum-resistant technologies ensuring superior security levels.	The introduction of quantum cryptography enhances security but requires updates to existing security frameworks to address new vulnerabilities.	Secure V2X Communication: More secure vehicle-to-everything communications for safer transportation systems.
Edge Computing	Latency-dependent processing	Edge AI with real-time processing capabilities	Improved processing capabilities at the edge are crucial for immediate data handling.	Enhanced edge computing capabilities necessitate advanced localized security measures to protect data at the edge.	Localized Data Processing: Real-time traffic data management to enhance flow and reduce congestion.
Device-to-Device Communication	Standard direct connectivity	Ultra-reliable direct device communications	Facilitates more robust and efficient device-to-device interactions.	Improved direct communications reduce reliance on central servers, shifting security focus to endpoint integrity.	Peer-to-Peer Networks for ITS: Direct vehicle communication enhances efficiency and reduces central dependency.
Interference Management	Managed with beamforming	Advanced AI-driven dynamic interference management	AI dynamically adapts to interference, enhancing communication quality.	Dynamic interference management may introduce vulnerabilities if AI systems are compromised.	Dynamic Spectrum Management: Active spectrum management to minimize interference in urban areas.
Network Slicing	Static slices tailored for specific services	Dynamic slicing with AI-driven adjustments	More adaptable network slices dynamically meet changing ITS demands.	Dynamic slicing increases the complexity of security management, requiring continuous monitoring and adaptation of security policies.	Dedicated Slices for Public Transit: High-priority network resources for transit systems ensure reliability and efficiency.

prevent man-in-the-middle and replay attacks since messages carry timestamps. However, protecting the privacy of platoon members and streamlining the signalling process while the SDN controller monitors the platoon's position is one of the issues associated with the proposed approach because it may be using untrustworthy third-party applications. How platoons maintain seamless handover authentication between gNB and eNB or non-3GPP network access points is another issue. Authentication on other components of ITS, such as RSU, was also investigated.

Feng et al. [74] introduced a protocol known as P2BA, which emphasizes privacy and incorporates batch authentication against semi-trusted RSUs. When a registered vehicle communicates a traffic-related message and its concealed certificate to an RSU, the latter, using non-interactive zero-knowledge proof techniques, can independently ascertain the message's validity. Compared to anonymous authentication systems, P2BA demonstrated a remarkable reduction in both computational time and storage requirements. A salient feature of this protocol is its ability to ensure message integrity and nonrepudiation. In cases of disputes, only law enforcement can unveil the vehicle linked to the verification message, thus disclosing its real identity. Nevertheless, there might be efficiency challenges in heterogeneous networks.

Recently, Kovalev and Agafonov [159] investigated an authentication mechanism for VANETs reliant on RSU infrastructure. This mechanism authenticates message signatures in RSUs utilising elliptic curve cryptography. While it potentially reduces computational overhead and the amount of data exchanged, it carries risks such as a single point of failure and possible delays in communications between RSUs and core networks or among RSUs.

More recently, Yang et al. [133] proposed a decentralized mutual authentication protocol with edge assistance. This protocol enables a swift, one-round, interaction-based authentication between vehicles and edge nodes. Several edge nodes can collaboratively validate each vehicle during the initial phase. These nodes subsequently provide an access token based on the vehicle's unique threshold signature, which can be used later for rapid handover authentication. This approach appears promising for highly mobile and dispersed settings, though there might be concerns regarding its computational efficiency.

To address these concerns, Tan et al. [160] proposed a solution that addresses the challenges of authenticating

devices and vehicles in a distributed, infrastructure-less environment. The scheme is based on the idea that vehicles can act as mobile authentication servers and assist in authenticating other vehicles and devices in the network. The scheme begins with the registration of vehicles and devices, which includes the generation and distribution of digital certificates for the devices. During the authentication process, vehicles broadcast a challenge message and request a response from other devices in the network. The devices then use their digital certificates to respond to the challenge and prove their identity to the vehicle-assisted authentication server. The scheme also includes a trust management mechanism, which allows the authentication server to establish trust relationships with other vehicles and devices in the network based on their previous authentication history and reputation. This scheme is particularly useful in infrastructure-less environments such as rural or disaster-stricken areas, where the traditional fixed infrastructure is unavailable or damaged. The scheme enables the vehicles to act as a moving infrastructure, providing authentication and secure communication in a distributed environment.

Implementation of intelligent zero-trust technology in 6G-ITS can equally provide authentication solutions to components. Even after ITS components are authenticated and authorized, zero trust architecture continues to deliver network confidentiality and integrity under the presumption that no entity or component requesting connectivity or access to the network is considered safe and trusted [75]. Every access request is uniquely considered and approved in guidance with the security policy requirements for the trust evaluation.

Critical communication and tactile edge networks comprising heterogeneous and ubiquitous devices require next-generation networks like 6G [161]. Through a variety of new radio access technologies (RATs), including space air and ground integrated network (SAGIN), 6G can provide the required computational resources (through cloud computing) and seamless, dependable, and resilient connection [33]. Meng et al. [162] work on a continuous authentication protocol without trust authority for zero-trust architecture that can be adapted to vehicular networks and other ITS. The paper employed blockchain to eliminate the trusted node, thereby decentralising the authentication, particularly for device-to-device continuous authentication. Additionally, Song et al. [163] proposed a new zero-trust-aided smart key authentication scheme on the IoV. The scheme proposed a smart key for users to unlock vehicles. The scheme proposed a continuous authentication system based on fingerprint, NFC, and facial data to authenticate the driver while driving. It should be noted that the scheme has not yet been implemented on a large scale, and this approach is still being researched. Before implementing in real-world scenarios, further studies should be conducted on security, scalability, and fault tolerance. Figure 5 shows that the authentication, security, privacy, and blockchain are the keywords most discussed in the papers surveyed for this paper.

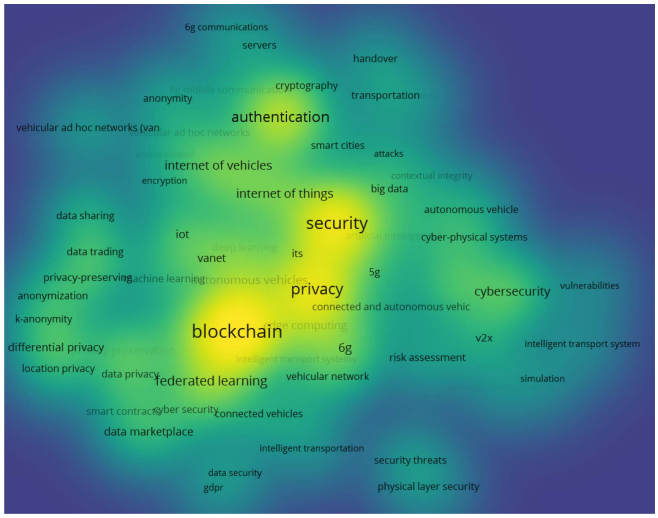

FIGURE 5. Surveyed paper keywords density.

B. IMPLEMENTATION BARRIERS

The transition from theoretical frameworks to the practical implementation of security, privacy, and trust mechanisms within 6G-ITS faces several implementation barriers. One primary challenge is the inherent complexity of integrating heterogeneous devices and technologies into cohesive, secure systems [164]. The coexistence of legacy systems with emerging technologies such as IRS, VLC, and terahertz communication complicates interoperability and standardization, leading to fragmented security protocols and inconsistent trust enforcement [165]. Furthermore, current authentication and key management schemes are insufficiently scalable or flexible to handle the anticipated density and dynamic interactions of 6G-ITS components. Traditional centralized approaches, such as the TA model, face limitations regarding latency, computational overhead, and vulnerability to single-point failures, necessitating a shift towards decentralized architectures [66].

Decentralized approaches, such as blockchain-based identity management and distributed authentication protocols, address these traditional limitations, introducing new challenges that contribute to implementation barriers. These include increased communication overhead due to consensus mechanisms, synchronization difficulties in highly mobile environments, and scalability issues in real-time scenarios [56]. Moreover, the computational and storage demands of decentralized solutions can strain the resource-constrained edge devices commonly used in ITS. Importantly, many of these decentralized frameworks have only been validated in controlled simulation environments, and their performance can degrade or behave unpredictably under real-world conditions, where factors such as network instability, node failure, and physical interference are more difficult to control [165].

Regulatory and governance issues present another critical barrier, particularly concerning data privacy compliance and cross-border interoperability. Differences in global

regulations on data protection, such as GDPR in Europe, create complexities in the design of universally compliant privacy preservation mechanisms [166]. Furthermore, implementing sophisticated cryptographic techniques, including quantum-resistant algorithms, requires substantial computational resources and incurs significant deployment costs [36]. Real-world constraints, such as limited computational power and energy resources in edge devices, exacerbate these challenges, posing practical difficulties in achieving the desired security levels without degrading system performance.

Lastly, societal acceptance and ethics are subtle but influential obstacles. Public trust in autonomous transportation systems is highly dependent on transparent decision-making [167]. Ethical issues related to AI decisions, such as the trade-off between privacy and safety, and the accountability of automation, remain unresolved, potentially causing delays in the adoption of technology. Comprehensive research, international standards, and clear ethical guidelines are essential for the successful deployment and acceptance of secure 6G-enabled ITS.

VII. DISCUSSION

This section examines the findings of our analysis and maps them to the original research questions. Much of the current discourse around 6G-ITS remains conceptual. We critically explore how the frameworks for security, privacy, and trust have been validated in recent empirical studies. Drawing from both simulations and early-stage deployments, we assess the translation of theoretical models into practical implementations and identify instances where empirical evidence supports or contradicts design assumptions. This approach allows us to highlight both the maturity of certain technologies and the areas where real-world applicability is limited.

A. EMPIRICAL VALIDATION

The theoretical foundations of the 6G-ITS security, privacy, and trust frameworks are extensively developed in the academic literature; however, empirical validation is relatively sparse. Most studies rely predominantly on high-fidelity simulations instead of deployment-grade field trials, resulting in a persistent gap between conceptual models and practical implementation [31], [94], [106], [167], [168], [169], [170], [171], [172]. This limitation is of particular importance for ITS, as real-world operational complexity, mobility patterns, and environmental variability can considerably affect the effectiveness of proposed mechanisms.

Several advanced testbeds provide partial empirical insight. The VIAVI GPU-Powered Real-Time 6G Testbed, developed in collaboration with the Institute for Wireless Internet of Things and the Open6G Cooperative Research Center at Northeastern University, integrates a city-scale digital twin to evaluate the 6G network capabilities [173]. Similarly, the IEEE 5G/6G Innovation Testbed offers a cloud-based platform to assess emerging services in domains such as smart cities, industrial automation, and transportation [174]. However, these environments primarily validate communication performance, such as throughput, latency, and reliability, rather than conducting end-to-end assessments of security, privacy, and trust mechanisms.

Empirical studies focused on security for ITS remain focused on 5G and VANET environments. For example, standalone core servers combined with software-defined radio (SDR) cards have been used to identify vulnerabilities through fuzzing operations, and the performance of the V2X protocol has been benchmarked in terms of latency and computational overhead [175]. However, there is little equivalent work for ITS enabled by 6G, particularly in the areas of quantum-resistant cryptography, zero-trust architectures, and AI-driven intrusion detection in vehicular contexts [150]. Validations of the existing trust models in vehicular ad hoc networks have been carried out using simulators such as MobiSim and NS-2, typically with limited mobility scenarios and without the integration of specific features of 6G, including submillisecond latency and ultra-dense connectivity [27], [75], [108], [161], [176].

For privacy, empirical work is sparse. Machine learning–based channel estimation in simulated 6G conditions has achieved over 92% accuracy in differentiating simultaneous users under moderate turbulence, and bidirectional LSTM models have reached 99.99% accuracy in detecting DoS / DDoS attacks in 5G network slices [89]. Although these findings are promising for privacy-preserving federated learning and AI-driven intrusion detection, comprehensive evaluations of differential privacy, homomorphic encryption, and secure multiparty computation in vehicular networks remain confined to controlled simulations [130]. Trust frameworks for autonomous decision making also lack empirical implementation, with no large-scale evaluation of verifiable AI models in safety-critical ITS scenarios.

The current empirical landscape therefore reveals three critical gaps: (i) the absence of large-scale field trials that jointly validate security, privacy, and trust mechanisms under realistic 6G-ITS conditions, (ii) the lack of standardized benchmarks and metrics for consistent cross-scenario evaluation, and (iii) insufficient real-world testing of emerging technologies such as quantum-safe V2X authentication, verifiable AI, and longitudinal trust adaptation in adversarial multiagent environments. Furthermore, most validation efforts are siloed, focusing on either communication performance or isolated security features, without addressing their combined effects in integrated ITS deployments. These limitations highlight the urgent need for coordinated industry–academia efforts to establish empirical frameworks capable of bridging the theory–practice divide. Beyond empirical validation, practical deployment faces challenges in resource-constrained edge devices, backward compatibility with legacy infrastructure, and the computational overhead of quantum-resistant cryptography and zero-trust architectures, all of which introduce scalability concerns that must be addressed through phased implementation strategies [22]. As

TABLE 8. Open problems in 6G-ITS security, privacy, and trust.

Category	Open problem	Description
Security	Zero-trust enforcement for O-RAN-based ITS	Applying zero-trust models at the RIC and edge nodes is still an open challenge due to latency constraints and difficulty in synchronising dynamic policies across distributed components.
	Quantum-safe V2X authentication	Post-quantum V2X protocols remain underdeveloped for real-time, mobile vehicular environments, with limited field validation of algorithm performance under sub-millisecond latency requirements.
Privacy	Cross-domain data minimization	Balancing data utility and privacy across ITS, telecom, and cloud domains—particularly under federated learning constraints—remains unresolved in real-world deployments.
	Differential privacy for real-time sensor data	Most differential privacy mechanisms degrade performance or fail to meet latency requirements for safety-critical 6G-ITS applications.
Trust	Verifiable AI in safety-critical decisions	ITS lacks verifiable and interpretable ML models that maintain robustness under adversarial conditions while providing real-time decision assurance in safety-critical contexts.
	Dynamic trust computation in multi-agent systems	Computing and adapting trust scores for vehicles in dynamic, adversarial, and high-mobility settings remains underexplored, particularly for large-scale, real-world ITS deployments.

a result, several open problems remain, as summarized in Table 8.

B. RQ1:IN THE CONTEXT OF 6G-ITS, HOW CAN MULTI-LAYERED SECURITY STRATEGIES BE DESIGNED TO PROTECT AGAINST SOPHISTICATED CYBERATTACKS TARGETING COMMUNICATION NETWORKS, DEVICES, AND DATA ANALYTICS PLATFORMS?

Addressing the challenge of crafting multi-layered security strategies for 6G-ITS, our investigation highlighted the necessity for robust frameworks capable of safeguarding these systems against an evolving landscape of cyber threats. The advent of 6G technology brings forth enhanced data rates, connectivity, and reduced latency, marking significant advancements in transportation efficiency and safety. However, these benefits also introduce complex security vulnerabilities, from increased attack surfaces due to the sheer volume of connected devices to sophisticated cyberattacks that disrupt transportation systems' integrity and availability. Our discussion on multi-layered security strategies underscored the integration of cutting-edge encryption techniques, secure communication protocols, and stringent access controls, all tailored to shield ITS against potential breaches. Notably, the prospect of quantum computing necessitates a forward-looking approach to ITS security, prompting the inclusion of quantum-resistant algorithms in the strategic defence matrix. By synthesizing theoretical models with real-world case studies, the paper presents actionable solutions, detailed in Section III and summarized in Table 4, that fortify the security posture of ITS, ensuring a resilient infrastructure capable of withstanding future cyber threats. Practical implementation, however, requires balancing the computational demands of these advanced security mechanisms against the latency constraints of safety-critical ITS applications and the resource limitations of edge devices, presenting scalability challenges that necessitate careful deployment planning and infrastructure investment.

C. RQ2: WHAT MECHANISMS CAN BE DEVELOPED WITHIN 6G-ITS TO ENSURE USER PRIVACY IN THE FACE OF EXTENSIVE DATA COLLECTION REQUIRED FOR ADVANCED SENSING, AUTOMATION, AND COMMUNICATION SYSTEMS?

The discourse on privacy-preserving mechanisms within 6G-ITS illuminated the critical balance between leveraging extensive data for system optimization and safeguarding individual privacy. With the advent of 6G, ITS is poised to benefit from unprecedented data collection and processing levels, enhancing traffic management and vehicle-to-everything communications. However, this capability raises significant privacy concerns, necessitating the adoption of technologies like federated learning and differential privacy. These methodologies enable the decentralized analysis of data, minimizing the exposure of sensitive information while maintaining system efficacy. The paper further explores the regulatory and ethical frameworks essential to embedding privacy considerations into ITS design and operation. It advocates for a privacy-centric approach that aligns with global standards and public expectations.

D. RQ3: HOW CAN TRUST IN 6G-ITS BE QUANTIFIED AND MANAGED, PARTICULARLY IN SYSTEMS INVOLVING DECISION-MAKING AND AUTONOMOUS OPERATIONS?

Lastly, our inquiry into quantifying and managing trust in AI/ML-driven ITS systems revealed the complexities involved in ensuring the public perceives these technologies as reliable and safe. The deployment of AI/ML in autonomous vehicle operations and decision-making processes introduces a layer of opacity that can hinder trust. This research underscores the importance of developing transparent and verifiable methods to evaluate the reliability

of AI/ML algorithms and their output. Establishing trust in ITS extends beyond technical solutions to encompass ethical considerations, stakeholder participation, and adherence to the principles of responsible AI usage. The paper advocates for a comprehensive trust management framework, incorporating standardized metrics for trust quantification alongside adaptive strategies that evolve with technological advancements and societal values.

VIII. CONCLUSION

This comprehensive survey reveals that while 6G-ITS promises transformative improvements in connectivity, automation, and safety, significant challenges in security, privacy, and trust must be resolved before widespread deployment. Our analysis identifies critical gaps between theoretical frameworks and practical implementation, particularly in empirical validation, quantum-safe integration, and real-world scalability testing. The evolution from 5G to 6G fundamentally alters the security paradigm, requiring distributed defense mechanisms, quantum-resistant cryptography, and AI-driven threat detection that current approaches cannot adequately address.

In summary, the findings collectively demonstrate how the proposed multi-layered security strategies (RQ1), privacy-preserving mechanisms for large-scale data ecosystems (RQ2), and trust management models suitable for autonomous and cooperative ITS environments (RQ3) form a coherent foundation for securing next-generation transportation systems. Together, these insights outline the technical direction required to align 6G capabilities with the safety, privacy, and reliability expectations of future mobility infrastructures.

To bridge these gaps, coordinated action between stakeholders is essential. Regulators must establish standardized security-by-design mandates with clear post-quantum migration timelines and cross-border data governance frameworks. The industry must embed zero-trust architectures, hardware security foundations, and privacy-preserving analytics throughout its development lifecycles. Network operators require end-to-end protection that combines slice isolation, confidential computing, and robust incident response capabilities. Research institutions must advance measurable trust metrics, formal verification methods, and empirical validation through joint pilot programs that bridge the gaps between lab and field implementation. Success in 6G-ITS deployment depends on establishing technically rigorous, privacy-preserving security baselines that are validated through comprehensive real-world testing and supported by adaptive governance frameworks that evolve in response to emerging threats.

REFERENCES

[1] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[2] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6G technologies and applications," *Sensors*, vol. 22, p. 1969, Mar. 2022.

[3] G. K. Munasinghe and M. Murtaza, "Analyzing vehicle-to-everything communication for intelligent transportation system: Journey from IEEE 802.11p to 5G and finally towards 6G," in *Proc. 5th Int. Conf. Innov. Technol. Intell. Syst. Ind. Appl. (CITISIA)*, Nov. 2020, pp. 1–7.

[4] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, Mar. 2020.

[5] Z. Zhou, A. Gaurav, B. B. Gupta, M. D. Lytras, and I. Razzak, "A fine-grained access control and security approach for intelligent vehicular transport in 6G communication system," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9726–9735, Jul. 2022.

[6] W. Guo, "Explainable artificial intelligence for 6G: Improving trust between human and machine," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 39–45, Jun. 2020.

[7] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020.

[8] H. Alakoca et al., "Metasurface manipulation attacks: Potential security threats of RIS-aided 6G communications," *IEEE Wireless Commun. Mag.*, vol. 61, no. 1, pp. 24–30, Jan. 2023.

[9] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 334–366, 2021.

[10] Z. Zhang et al., "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.

[11] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[12] Z. Lv, L. Qiao, and I. You, "6G-enabled network in box for Internet of Connected Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5275–5282, Aug. 2021.

[13] A. V. Jha, B. Appasani, M. S. Khan, S. Zeadally, and I. Katib, "6G for intelligent transportation systems: standards, technologies, and challenges," *Telecommun. Syst.*, vol. 86, pp. 241–268, Mar. 2024.

[14] V.-L. Nguyen, R.-H. Hwang, P.-C. Lin, A. Vyas, and V.-T. Nguyen, "Toward the age of intelligent vehicular networks for connected and autonomous vehicles in 6G," *IEEE Netw.*, vol. 37, no. 3, pp. 44–51, May 2023.

[15] R. Liu, A. Liu, Z. Qu, and N. N. Xiong, "An UAV-enabled intelligent connected transportation system with 6G communications for Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2045–2059, Feb. 2023.

[16] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, "A survey on trust models in heterogeneous networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2127–2162, 4th Quart., 2022.

[17] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and trust in the 6G era," *IEEE Access*, vol. 9, pp. 142314–142327, 2021.

[18] J. Harvey and S. Kumar, "A survey of intelligent transportation systems security: Challenges and solutions," in *Proc. IEEE 6th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), IEEE Int. Conf. High Perform. Smart Comput. (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2020, pp. 263–268.

[19] D. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges," *IEEE Intell. Transp. Syst. Mag.*, vol. 13, no. 1, pp. 181–196, Apr. 2021.

[20] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, pp. 9180–9208, 2021.

[21] X. Deng et al., "A review of 6G autonomous intelligent transportation systems: Mechanisms, applications and challenges," *J. Syst. Archit.*, vol. 142, Sep. 2023, Art. no. 102929.

[22] M. Noor-A-Rahim et al., "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proc. IEEE*, vol. 110, no. 6, pp. 712–734, Jun. 2022.

[23] G. Kirubasri, S. Sankar, D. Pandey, B. K. Pandey, H. Singh, and R. Anand, "A recent survey on 6G vehicular technology, applications and challenges," in *Proc. 9th Int. Conf. Rel., Infocom Technol. Optim. (ICRITO)*, Sep. 2021, pp. 1–5.

[24] D. P. Moya Osorio et al., "Towards 6G-enabled Internet of Vehicles: Security and privacy," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 82–105, 2022.

[25] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digit. Commun. Netw.*, vol. 6, pp. 281–291, Aug. 2020.

[26] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[27] Y. Wang, X. Kang, T. Li, H. Wang, C.-K. Chu, and Z. Lei, "SIX-Trust for 6G: Toward a secure and trustworthy future network," *IEEE Access*, vol. 11, pp. 107657–107668, 2023.

[28] B. Veith, D. Krummacker, and H. D. Schotten, "The road to trustworthy 6G: A survey on trust anchor technologies," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 581–595, 2023.

[29] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul. 2019.

[30] H. Visavadia. "Drivers rage new artificial intelligence cameras not fit for U.K. roads as they 'invade' privacy." Jun. 2024. [Online]. Available: https://www.gbnews.com/lifestyle/cars/drivers-rage-new-artificial-intelligence-cameras-not-fit-for-uk-roads-they-invade-privacy

[31] L. Ming, G. Zhao, M. Huang, X. Kuang, H. Li, and M. Zhang, "Security analysis of intelligent transportation systems based on simulation data," in *Proc. 1st Int. Conf. Data Intell. Secur. (ICDIS)*, Apr. 2018, pp. 184–187.

[32] A. Jolfaei and K. Kant, "Privacy and security of connected vehicles in intelligent transportation system," in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN-S)*, Jun. 2019, pp. 9–10.

[33] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 53–87, 1st Quart., 2022.

[34] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, Dec. 2017.

[35] W. Hathal, H. Cruickshank, Z. Sun, and C. Maple, "Certificateless and lightweight authentication scheme for vehicular communication networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 16110–16125, Dec. 2020.

[36] H. Fang, X. Wang, Z. Xiao, and L. Hanzo, "Autonomous collaborative authentication with privacy preservation in 6G: From homogeneity to heterogeneity," *IEEE Netw.*, vol. 36, no. 6, pp. 28–36, Nov./Dec. 2022.

[37] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[38] P. Porambage, G. Gur, D. P. Moya Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 622–627.

[39] A. English. "How range rovers became virtually uninsurable." The Telegraph. 2024. [Online]. Available: https://www.telegraph.co.uk/cars/land-rover/land-rovers-thefts-expensive-insurance/January 2024

[40] T. Hong, J. Cao, C. Fang, and D. Li, "6G based intelligent charging management for autonomous electric vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7574–7585, Jul. 2023.

[41] B. Zeddini, M. Maachaoui, and Y. Inedjaren, "Security threats in intelligent transportation systems and their risk levels," *Risks*, vol. 10, p. 91, Apr. 2022.

[42] K.-A. Shim, "A survey on post-quantum public-key signature schemes for secure vehicular communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 14025–14042, Sep. 2022.

[43] M. Visan, S. L. Negrea, and F. Mone, "Towards intelligent public transport systems in smart cities; collaborative decisions to be made," *Procedia Comput. Sci.*, vol. 199, pp. 1221–1228, Feb. 2022.

[44] M. Kamal, M. Tariq, G. Srivastava, and L. Malina, "Optimized security algorithms for intelligent and autonomous vehicular transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2038–2044, Feb. 2023.

[45] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar. 2020.

[46] H. Guo, X. Zhou, J. Liu, and Y. Zhang, "Vehicular intelligence in 6G: Networking, communications, and computing," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100399.

[47] C. Wang and A. Rahman, "Quantum-enabled 6G wireless networks: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 58–69, Feb. 2022.

[48] O. Adeboye, A. Abdullahi, T. Dargahi, M. Babaie, and M. Saraee, "LIFT the AV: Location inference attack on autonomous vehicle camera data," in *Proc. IEEE 20th Consumer Commun. Netw. Conf. (CCNC)*, Jan. 2023, pp. 1–6.

[49] Z. Xiong, W. Li, Q. Han, and Z. Cai, "Privacy-preserving auto-driving: A GAN-based approach to protect vehicular camera data," in *Proc. IEEE Int. Conf. Data Min. (ICDM)*, Nov. 2019, pp. 668–677.

[50] A. Taeihagh and H. S. M. Lim, "Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks," *Transp. Rev.*, vol. 39, pp. 103–128, Jul. 2018.

[51] B. Keller, M. Eling, H. Schmeiser, M. Christen, and M. Loi, *Big Data and Insurance: Implications for Innovation, Competition and Privacy*. Zürich, Switzerland: Geneva Assoc., Mar. 2018, pp. 1–48.

[52] S. Johar, N. Ahmad, A. Durrani, and G. Ali, "Proof of pseudonym: Blockchain-based privacy preserving protocol for intelligent transport system," *IEEE Access*, vol. 9, pp. 163625–163639, 2021.

[53] Y. Jang et al., "Optimization of error pattern embedding steganography within error-correcting code frameworks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2024, pp. 1094–1099.

[54] Y. Salmi and H. Bogucka, "Poisoning attacks against communication and computing task classification and detection techniques," *Sensors*, vol. 24, p. 338, Jan. 2024.

[55] M. Begum, G. Raja, and M. Guizani, "AI-based sensor attack detection and classification for autonomous vehicles in 6G-V2X environment," *IEEE Trans. Veh. Technol.*, vol. 73, no. 4, pp. 5054–5063, Apr. 2024.

[56] M. Kim, I. Oh, K. Yim, M. Sahlabadi, and Z. Shukur, "Security of 6G-enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies," *IEEE Access*, vol. 12, pp. 33972–34001, 2024.

[57] M. Alwakeel, "Neuro-driven agent-based security for quantum-safe 6G networks," *Mathematics*, vol. 13, p. 2074, Jun. 2025.

[58] F. Zaman, A. Farooq, M. A. Ullah, H. Jung, H. Shin, and M. Z. Win, "Quantum machine intelligence for 6G URLLC," *IEEE Wireless Commun.*, vol. 30, no. 2, pp. 22–30, Apr. 2023.

[59] N. Khatri, S. Lee, and S. Y. Nam, "Sybil attack-resistant blockchain-based proof-of-location mechanism with privacy protection in VANET," *Sensors*, vol. 24, p. 8140, Dec. 2024.

[60] N. Kaur and L. Gupta, "Securing the 6G–IoT environment: A framework for enhancing transparency in artificial intelligence decision-making through explainable artificial intelligence," *Sensors*, vol. 25, p. 854, Jan. 2025.

[61] A. Krayani, G. Barabino, L. Marcenaro, and C. Regazzoni, "Integrated sensing and communication for joint GPS spoofing and jamming detection in vehicular V2X networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2023, pp. 1–7.

[62] Z. T. A. Tang, K.-W. Yu, K. Yuta, T.-Y. Chen, and A. Karati, "Enhancing security of a PUF-based remote keyless entry system using machine learning approach," in *Proc. 6th Int. Electron. Commun. Conf.*, Jul. 2024, pp. 66–74.

[63] D. Berardi, N. O. Tippenhauer, A. Melis, M. Prandini, and F. Callegati, "Time sensitive networking security: Issues of precision time protocol and its implementation," *Cybersecurity*, vol. 6, p. 8, Apr. 2023.

[64] S. Zidi, B. Alaya, T. Moulahi, A. Al-Shargabi, and S. E. Khediri, "Fault prediction and recovery using machine learning techniques and the HTM algorithm in vehicular network environment," *IEEE Open J. Intell. Transp. Syst.*, vol. 5, pp. 132–145, 2024.

[65] B. Ashutosh Holla, M. M. M. Pai, U. Verma, and R. M. Pai, "Vehicle re-identification and tracking: Algorithmic approach, challenges and future directions," *IEEE Open J. Intell. Transp. Syst.*, vol. 6, pp. 155–183, 2025.

[66] T. Li, M. Shang, S. Wang, and R. Stern, "Detecting subtle cyberattacks on adaptive cruise control vehicles: A machine learning approach," *IEEE Open J. Intell. Transp. Syst.*, vol. 6, pp. 11–23, 2025.

[67] L. Barbieri, S. Savazzi, M. Brambilla, and M. Nicoli, "Decentralized federated learning for extended sensing in 6G connected vehicles," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100396.

[68] W. Song, S. Rajak, S. Dang, R. Liu, J. Li, and S. Chinnadurai, "Deep learning enabled IRS for 6G intelligent transportation systems: A comprehensive study," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 11, pp. 12973–12990, Nov. 2023.

[69] Q. Xia, W. Ye, Z. Tao, J. Wu, and Q. Li, "A survey of federated learning for edge computing: Research problems and solutions," *High-Confid. Comput.*, vol. 1, Jun. 2021, Art. no. 100008.

[70] E. Bahrami, A. Abdullahi, and T. Dargahi, "SoK: Privacy, security, and ethical considerations in vehicular data monetization," in *Proc. 7th ACM Int. Symp. Blockchain Secure Crit. Infrast.*, 2025, pp. 1–14.

[71] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb, "Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1342–1397, 2nd Quart., 2021.

[72] H. Hafi, B. Brik, P. A. Frangoudis, A. Ksentini, and M. Bagaa, "Split federated learning for 6G enabled-networks: Requirements, challenges, and future directions," *IEEE Access*, vol. 12, pp. 9890–9930, 2024.

[73] J. A. Alonso-Lupez et al., "Level of trust and privacy management in 6G intent-based networks for vertical scenarios," in *Proc. 1st Int. Conf. 6G Netw. (6GNet)*, Jul. 2022, pp. 1–4.

[74] X. Feng, Q. Shi, Q. Xie, and L. Wang, "P2BA: A privacy-preserving protocol with batch authentication against semi-trusted RSUs in vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3888–3899, 2021.

[75] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wireless Commun. Mobile Comput.*, vol. 2022, Jan. 2022, Art. no. 6476274.

[76] M. De Ree, G. Mantas, J. Rodriguez, and I. E. Otung, "DECENT: Decentralized and efficient key management to secure communication in dense and dynamic environments," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7586–7598, Jul. 2023.

[77] X. Huo and M. Liu, "Distributed privacy-preserving electric vehicle charging control based on secret sharing," *Electr. Power Syst. Res.*, vol. 211, Oct. 2022, Art. no. 108357.

[78] O. O. Olakanmi and K. O. Odeyemi, "Trust-aware and incentive-based offloading scheme for secure multi-party computation in Internet of Things," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100527.

[79] P. Bossauer, T. Neifer, G. Stevens, and C. Pakusch, "Trust versus privacy: Using connected car data in peer-to-peer carsharing," in *Proc. CHI Conf. Human Factors Comput. Syst.*, Apr. 2020, pp. 1–13.

[80] J. Caltrider, M. Rykov, and Z. MacDonald. "It's official: Cars are the worst product category we have ever reviewed for privacy." Sep. 2023. Accessed: Aug. 8, 2025. [Online]. Available: https://www.mozillafoundation.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

[81] D. Suo, J. Siegel, and A. Soley, "Driving data dissemination: The 'term' governing connected car information," *IEEE Intell. Transp. Syst. Mag.*, vol. 13, no. 1, pp. 20–30, Mar. 2021.

[82] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Toward blockchain-based trust and reputation management for trustworthy 6G networks," *IEEE Netw.*, vol. 36, no. 4, pp. 112–119, Jul. 2022.

[83] X. Wang, H. Zhu, H. Xiao, Z. Zhou, S. Yang, and L. Sun, "Blockchain-enhanced trust management for mobile edge computing-enabled intelligent vehicular collaboration in the 6G era," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 7, May 2023, Art. no. e4791.

[84] P. Bhattacharya, A. Shukla, S. Tanwar, N. Kumar, and R. Sharma, "6Blocks: 6G-enabled trust management scheme for decentralized autonomous vehicles," *Comput. Commun.*, vol. 191, pp. 53–68, Jul. 2022.

[85] M. Maier, "6G as if people mattered: From industry 4.0 toward society 5.0: (Invited paper)," in *Proc. Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2021, pp. 1–10.

[86] T. Gazdar, A. Belghith, and H. Abutair, "An enhanced distributed trust computing protocol for VANETs," *IEEE Access*, vol. 6, pp. 380–392, 2018.

[87] K. Haseeb, A. Rehman, T. Saba, S. A. Bahaj, H. Wang, and H. Song, "Efficient and trusted autonomous vehicle routing protocol for 6G networks with computational intelligence," *ISA Trans.*, vol. 132, pp. 61–68, Jan. 2023.

[88] C. Li, W. Guo, S. C. Sun, S. Al-Rubaye, and A. Tsourdos, "Trustworthy deep learning in 6G-enabled mass autonomy: From concept to quality-of-trust key performance indicators," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 112–121, Dec. 2020.

[89] L. Yang, Y. Li, S. X. Yang, Y. Lu, T. Guo, and K. Yu, "Generative adversarial learning for intelligent trust management in 6G wireless networks," *IEEE Netw.*, vol. 36, no. 4, pp. 134–140, Jul. 2022.

[90] *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*, ETSI Standard TS 102 941, Jun. 2012.

[91] A. M. Algarni and V. Thayananthan, "Autonomous vehicles with a 6G-based intelligent cybersecurity model," *IEEE Access*, vol. 11, pp. 15284–15296, 2023.

[92] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, Feb. 2020.

[93] S. Gajewski, "5G technologies in intelligent transport systems-architectures, virtualization and network slicing," *Arch. Transp. Syst. Telemat.*, vol. 12, no. 1, pp. 9–16, 2019.

[94] I. Rasheed, F. Hu, Y.-K. Hong, and B. Balasubramanian, "Intelligent vehicle network routing with adaptive 3D beam alignment for mmWave 5G-based V2X communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2706–2718, May 2021.

[95] Y. Zhang, W. Zhao, P. Dong, X. Du, W. Qiao, and M. Guizani, "Improve the reliability of 6G vehicular communication through skip network coding," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100400.

[96] M. Zhang, Y. Dou, V. Marojevic, P. H. J. Chong, and H. C. B. Chan, "FAQ: A fuzzy-logic-assisted Q-learning model for resource allocation in 6G V2X," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 2472–2489, Jan. 2024.

[97] C. Patsakis, K. Dellios, and M. Bouroche, "Towards a distributed secure in-vehicle communication architecture for modern vehicles," *Comput. Secur.*, vol. 40, pp. 60–74, Feb. 2014.

[98] H. Chen, J. Liu, J. Wang, and Y. Xun, "Towards secure intra-vehicle communications in 5G advanced and beyond: Vulnerabilities, attacks and countermeasures," *Veh. Commun.*, vol. 39, Feb. 2023, Art. no. 100548.

[99] G. P. Fettweis and H. Boche, "On 6G and trustworthiness," *Commun. ACM*, vol. 65, pp. 48–49, Mar. 2022.

[100] C. Li et al., "Quality-of-trust in 6G: Combining emotional and physical trust through explainable AI," in *Proc. IEEE 98th Veh. Technol. Conf.*, Oct. 2023, pp. 1–7.

[101] M. R. Sama, W. Kiess, R. Guerzoni, S. Thakolsri, and J. Jurjens, "Redefining the trust model for the internet of everything in the 6G era," in *Proc. IEEE 33rd Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2022, pp. 1400–1406.

[102] R. Kantola, "6G network needs to support embedded trust," in *Proc. 14th Int. Conf. Avail., Rel. Secur.*, Aug. 2019, pp. 1–5.

[103] T. Wang et al., "Building trust via blockchain in UAV-assisted ultra-dense 6G cellular networks," *IET Blockchain*, vol. 2, pp. 67–76, Sep. 2022.

[104] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, 2020.

[105] A. R. Nair, N. K. Jadav, R. Gupta, and S. Tanwar, "AI-empowered secure data communication in V2X environment with 6G network," in *Proc. IEEE Conf. Comput. Commun. Workshops*, May 2022, pp. 1–6.

[106] Z. Zhou, M. Wang, J. Huang, S. Lin, and Z. Lv, "Blockchain in big data security for intelligent transportation with 6G," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9736–9746, Jul. 2022.

[107] H. A. Al-Mohammed and E. Yaacoub, "On the use of quantum communications for securing IoT devices in the 6G era," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6.

[108] X. Chen, J. Ding, and Z. Lu, "A decentralized trust management system for intelligent transportation environments," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 1, pp. 558–571, Jan. 2022.

[109] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.

[110] C.-X. Wang, J. Wang, S. Hu, Z. H. Jiang, J. Tao, and F. Yan, "Key technologies in 6G terahertz wireless communication systems: A survey," *IEEE Veh. Technol. Mag.*, vol. 16, no. 4, pp. 27–37, Dec. 2021.

[111] M. A. Arfaoui et al., "Physical layer security for visible light communication systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1887–1908, 3rd Quart., 2020.

[112] Y. Zhu, B. Mao, and N. Kato, "Intelligent reflecting surface in 6G vehicular communications: A survey," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 266–277, 2022.

[113] Y. Lu and X. Zheng, "6G: A survey on technologies, scenarios, challenges, and the related issues," *J. Ind. Inf. Integr.*, vol. 19, Sep. 2020, Art. no. 100158.

[114] S. F. Islam, "Distributed massive MIMO in millimetre wave communication," Ph.D. dissertation, Dept. Electron. Eng., Univ. York, York, U.K., Apr. 2022.

[115] H. Guo et al., "Integrated communication, localization, and sensing in 6G D-MIMO networks," *IEEE Wireless Commun.*, vol. 32, no. 2, pp. 214–221, Apr. 2025.

[116] O. Haliloglu et al., "Distributed MIMO systems for 6G," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2023, pp. 156–161.

[117] I. Ahmed, M. Z. Hasan, A. Rubaai, K. Hasan, C. Pu, and J. H. Reed, "Deep learning assisted channel estimation for cell-free distributed MIMO networks," in *Proc. 19th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Jun. 2023, pp. 344–349.

[118] Y. Cui, F. Liu, X. Jing, and J. Mu, "Integrating sensing and communications for ubiquitous IoT: Applications, trends, and challenges," *IEEE Netw.*, vol. 35, no. 5, pp. 158–167, Sep./Oct. 2021.

[119] P. Rosemann et al., "Enabling mobility-oriented JCAS in 6G networks: An architecture proposal," 2023, *arXiv:2311.11623*.

[120] M. A. Hossain, A. Xiang, A. Kiani, T. Saboorian, J. Kaippallimalil, and N. Ansari, "AI-assisted E2E network slicing for integrated sensing and communication in 6G networks," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 10627–10634, Mar. 2024.

[121] Y. Cui, F. Liu, C. Masouros, J. Xu, T. X. Han, and Y. C. Eldar, *Integrated Sensing and Communications: Background and Applications*. Singapore: Springer Nat., 2023, pp. 3–21. [Online]. Available: https://citation-needed.springer.com/v2/references/10.1007/978-981-99-2501-8_1?format=bibtex&flavour=citation

[122] S. Roger, C. Botella-Mascarell, D. Martín-Sacristán, D. García-Roger, J. F. Monserrat, and T. Svensson, "Sustainable mobility in B5G/6G: V2X technology trends and use cases," *IEEE Open J. Veh. Technol.*, vol. 5, pp. 459–472, 2024.

[123] H. Taghvaee, M. Khodadadi, G. Gradoni, and M. Khalily, "Fully autonomous reconfigurable metasurfaces with integrated sensing and communication," in *Proc. 18th Eur. Conf. Antennas Propag. (EuCAP)*, Mar. 2024, pp. 1–5.

[124] Y. Zhu, B. Mao, Y. Kawamoto, and N. Kato, "Intelligent reflecting surface-aided vehicular networks toward 6G: Vision, proposal, and future directions," *IEEE Veh. Technol. Mag.*, vol. 16, no. 4, pp. 48–56, Dec. 2021.

[125] K.-W. Huang and H.-M. Wang, "Intelligent reflecting surface aided pilot contamination attack and its countermeasure," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 345–359, Jan. 2021.

[126] H. Huang, Y. Zhang, H. Zhang, Y. Cai, A. L. Swindlehurst, and Z. Han, "Disco intelligent reflecting surfaces: Active channel aging for fully-passive jamming attack," *IEEE Trans. Wireless Commun.*, vol. 23, no. 1, pp. 806–819, Jan. 2024.

[127] L. Mucchi et al., "Physical-layer security in 6G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021.

[128] F. Irram, M. Ali, M. Naeem, and S. Mumtaz, "Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions," *J. Netw. Comput. Appl.*, vol. 206, Oct. 2022, Art. no. 103431.

[129] H. Ayaz et al., "Physical layer security analysis using radio frequency-fingerprinting in cellular-V2X for 6G communication," *IET Signal Process.*, vol. 17, May 2023, Art. no. e12225.

[130] X. Lu et al., "Reinforcement learning-based physical cross-layer security and privacy in 6G," *IEEE Wireless Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 425–466, 1st Quart., 2023.

[131] S. Kavaiya and D. K. Patel, "Restricting passive attacks in 6G vehicular networks: A physical layer security perspective," *Wireless Netw.*, vol. 29, pp. 1355–1365, Apr. 2023.

[132] P. Arthurs, L. Gillam, P. Krause, N. Wang, K. Halder, and A. Mouzakitis, "A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6206–6221, Jul. 2022.

[133] A. Yang, J. Weng, K. Yang, C. Huang, and X. Shen, "Delegating authentication to edge: A decentralized authentication architecture for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1284–1298, Feb. 2022.

[134] K. Yan, W. Ma, Q. Yang, S. Sun, and W. Wang, "Info-chain: Reputation-based blockchain for secure information sharing in 6G intelligent transportation systems," *IEEE Internet Things J.*, vol. 11, no. 5, p. 9198–9212, Mar. 2024.

[135] E. Bahrami, A. M. Aghapour, and M. Amini, "LIoTning: A peer-supervised payment channel approach for secure micropayments in IoT ecosystem," *IEEE Access*, vol. 13, pp. 134080–134112, 2025.

[136] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Wireless Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.

[137] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236–262, 1st Quart., 2016.

[138] B. Nogales et al., "Using aerial and vehicular NFV infrastructures to agilely create vertical services," *Sensors*, vol. 21, p. 1342, Feb. 2021.

[139] T. Liu, F. Sabrina, J. Jang-Jaccard, W. Xu, and Y. Wei, "Artificial intelligence-enabled DDoS detection for blockchain-based smart transport systems," *Sensors*, vol. 22, p. 32, Dec. 2021.

[140] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Security assessment in vehicle-to-everything communications with the integration of 5G and 6G networks," in *Proc. Int. Symp. Comput. Sci. Intell. Controls (ISCSIC)*, Nov. 2021, pp. 154–158.

[141] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020.

[142] M. Mizmizi et al., "Fastening the initial access in 5G NR sidelink for 6G V2X networks," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100402.

[143] B. Hazarika, P. Saikia, K. Singh, and C.-P. Li, "Enhancing vehicular networks with hierarchical O-RAN slicing and federated DRL," *IEEE Trans. Green Commun. Netw.*, vol. 8, no. 3, pp. 1099–1117, Sep. 2024.

[144] F. Linsalata, E. Moro, F. Gjeci, M. Magarini, U. Spagnolini, and A. Capone, "Addressing control challenges in vehicular networks through O-RAN: A novel architecture and simulation framework," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 9344–9355, Jul. 2024.

[145] M. Santana and K. L. Dias, "Open RAN-enabled deep learning-assisted mobility management for connected vehicles," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2025, pp. 378–383.

[146] S. D. A. Shah, A. K. Bashir, Y. D. Al-Otaibi, M. M. A. Dabel, and F. Ali, "Dynamic AI-driven network slicing with O-RAN for continuous connectivity in connected vehicles and onboard consumer electronics," *IEEE Trans. Consum. Electron.*, vol. 71, no. 1, pp. 720–733, Feb. 2025.

[147] Y. Cui, X. Yang, P. He, D. Wu, and R. Wang, "O-RAN slicing for multi-service resource allocation in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 73, no. 7, pp. 9272–9283, Jul. 2024.

[148] P. Baguer et al., "Attacking O-RAN interfaces: Threat modeling, analysis and practical experimentation," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 4559–4577, 2024.

[149] *WG11 O-RAN Security Threat Modeling and Remediation Analysis 4.0*, O-RAN Alliance, Alfter, Germany, 2022. Accessed: Aug. 1, 2025.

[150] P. Porambage, M. Christopoulou, B. Han, M. Asif Habibi, H. Bogucka, and P. Kryszkiewicz, "Security, privacy, and trust for open radio access networks in 6G," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 332–361, 2025.

[151] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1376–1411, 2nd Quart., 2023.

[152] V.-D. Nguyen et al., "Network-aided intelligent traffic steering in 6G O-RAN: A multi-layer optimization framework," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 2, pp. 389–405, Feb. 2024.

[153] M. El-Hajj, "Secure and trustworthy open radio access network (O-RAN) optimization: A zero-trust and federated learning framework for 6G networks," *Future Internet*, vol. 17, p. 233, May 2025.

[154] E. Moro, F. Linsalata, M. Magarini, U. Spagnolini, and A. Capone, "Advancing O-RAN to facilitate intelligence in V2X," *IEEE Netw.*, early access, Mar. 21, 2025, doi: 10.1109/MNET.2025.3553581.

[155] S. Soltani, A. Amanloo, M. Shojafar, and R. Tafazolli, "Intelligent control in 6G open ran: Security risk or opportunity?" *IEEE Open J. Commun. Soc.*, vol. 6, pp. 840–880, 2025.

[156] T. Chen, I. Chih-Lin, and T. Melodia, "O-RAN's role in shaping 6G: Industry perspectives on open and smart RAN," *IEEE Wireless Commun.*, vol. 32, no. 1, pp. 10–12, Feb. 2025.

[157] M. Ouaissa, M. Houmer, and M. Ouaissa, "An enhanced authentication protocol based group for vehicular communications over 5G networks," in *Proc. 3rd Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Sep. 2020, pp. 1–8.

[158] G. Li and C. Lai, "Platoon handover authentication in 5G-V2X," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Jun. 2020, pp. 1–2.

[159] K. Kovalev and A. Agafonov, "Authentication scheme in vehicular ad hoc networks based on road side unit infrastructure," in *Proc. Int. Conf. Inf. Technol. Nanotechnol. (ITNT)*, Sep. 2021, pp. 1–4.

[160] H. Tan, W. Zheng, P. Vijayakumar, K. Sakurai, and N. Kumar, "An efficient vehicle-assisted aggregate authentication scheme for infrastructure-less vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 15590–15600, Dec. 2023.

[161] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Comput. Netw.*, vol. 217, Nov. 2022, Art. no. 109358.

[162] L. Meng, D. Huang, J. An, X. Zhou, and F. Lin, "A continuous authentication protocol without trust authority for zero trust architecture," *China Commun.*, vol. 19, no. 8, pp. 198–213, Aug. 2022.

[163] Y. Song, F. Jiang, S. W. Ali Shah, and R. Doss, "A new zero-trust aided smart key authentication scheme in IoV," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops Affil. Events (PerCom Workshops)*, Mar. 2022, pp. 630–636.

[164] J. Vogt, H. D. Schotten, and H. Wieker, "Intelligent transportation system protocol interoperability evaluation," *IEEE Open J. Intell. Transp. Syst.*, vol. 6, pp. 67–94, 2025.

[165] J. Betz et al., "Autonomous vehicles on the edge: A survey on autonomous vehicle racing," *IEEE Open J. Intell. Transp. Syst.*, vol. 3, pp. 458–488, 2022.

[166] M. Nold and F. Corman, "How will the railway look like in 2050? A survey of experts on technologies, challenges and opportunities for the railway system," *IEEE Open J. Intell. Transp. Syst.*, vol. 5, pp. 85–102, 2024.

[167] I. E. Panagiotopoulos, G. J. Dimitrakopoulos, and G. Keraite, "On modelling and investigating user acceptance of highly automated passenger vehicles," *IEEE Open J. Intell. Transp. Syst.*, vol. 5, pp. 70–84, 2024.

[168] F. Qiao, J. Wu, J. Li, A. K. Bashir, S. Mumtaz, and U. Tariq, "Trustworthy edge storage orchestration in intelligent transportation systems using reinforcement learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4443–4456, Jul. 2021. [Online]. Available: https://scholar.google.com/scholar?as_q=Trustworthy+edge+storage+orchestration+in+intelligent+transportation+systems+using+reinforcement+learning&as_occt=title&hl=en&as_sdt=0%2C31

[169] P. Vijayakumar, M. Azees, S. A. Kozlov, and J. J. P. C. Rodrigues, "An anonymous batch authentication and key exchange protocols for 6G enabled VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1630–1638, Feb. 2022.

[170] H.-T. Wu and G.-J. Horng, "Establishing an intelligent transportation system with a network security mechanism in an internet of vehicle environment," *IEEE Access*, vol. 5, pp. 19239–19247, 2017.

[171] O. K. Tonguz and R. Zhang, "Harnessing vehicular broadcast communications: DSRC-actuated traffic control," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 2, pp. 509–520, Feb. 2020.

[172] K. N. Qureshi, A. Alhudhaif, S. W. Haidar, S. Majeed, and G. Jeon, "Secure data communication for wireless mobile nodes in intelligent transportation systems," *Microprocess. Microsyst.*, vol. 90, Apr. 2022, Art. no. 104501.

[173] (VIAVI Solut., Scottsdale, AZ, USA). *6G Forward Research Program*. 2024. Accessed: Aug. 2025. [Online]. Available: https://www.viavisolutions.com/en-uk/solutions/6g-forward

[174] "IEEE 5G/6G innovation testbed: Cloud-based, end-to-end 5G network emulator platform for testing and experimentation." 2023. [Online]. Available: https://testbed.ieee.org/

[175] M. Fujita, "Terahertz accelerates beyond 5G towards 6G," *Osaka Univ. Res. Press Rel.*, Feb. 2021. [Online]. Available: https://resou.osaka-u.ac.jp/en/research/2021/20210201_1

[176] S. A. Chaudhry et al., "A lightweight authentication scheme for 6G-IoT enabled maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2401–2410, Feb. 2023.