Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.077625

REVIEW

IoT-Driven Intelligent Transportation System in the Era of 6G and AI: A Review

Muhammet Ali Karabulut[1], A. F. M. Shahen Shah[2], Al-Sakib Khan Pathan[3,*] and Phillip G. Bradford[4]

[1]Electronics Engineering Department, Turkish Air Force Academy, National Defense University, Istanbul, Türkiye
[2]Electronics and Communication Engineering Department, Yildiz Technical University, Istanbul, Türkiye
[3]Department of Computer Science and Engineering, United International University, Dhaka, Bangladesh
[4]Department of Computing, University of Connecticut, Stamford, CT, USA

*Corresponding Author: Al-Sakib Khan Pathan. Email: sakib.pathan@gmail.com

Received: 13 December 2025; Accepted: 19 March 2026; Published: 08 May 2026

ABSTRACT: Today, technological progress is broad and deep. The next generation networks and systems will integrate features, technologies, and models requiring smooth cooperation between new and old technologies. This survey's uniqueness is that it considers an integrated, hybrid and heterogeneous future where Internet of Things (IoT), Sixth-Generation (6G) mobile communications technology, and Artificial Intelligence (AI) will work together, providing a smart and connected Intelligent Transportation System (ITS). This smart ITS will give better road safety and optimized travel. Currently, there is a scarcity of surveys focusing particularly on smart ITS that is expected soon. In this work, we investigate 6G technology and its enhanced features, then provide an overview of how AI systems will work. We also consider the effectiveness and security of ITS for autonomous driving, traffic management, route optimization, and accident prevention. We discuss how AI techniques evaluate data produced by IoT devices to improve ITS performance. Moreover, a performance analysis is conducted considering different system parameters for secure IoT-based ITS. Before concluding the paper, we outline the potential advantages and drawbacks of 6G and AI-enabled ITS and then offer suggestions for future research.

KEYWORDS: 6G; AI; intelligent transportation systems; IoT; privacy; security

1 Introduction

Transportation systems are essential for the movement of individuals and goods. The Internet of Things (IoT), new innovations in artificial intelligence (AI), and 6G technology promise unprecedented improvements for transportation efficiency, safety, and sustainability [1–5]. The confluence of these technologies hastens the development of smart Intelligent Transportation Systems (ITS). Smart ITS will improve traffic management, safety features, and offer a better travel experience for passengers [6–10]. Fig. 1 shows a high-level example architecture for the confluence of these technologies.

Real-time data sharing can be enabled between cars, other vehicles, and infrastructure, using a combination of IoT devices and transportation infrastructure. Such a networked ecosystem offers many benefits, including traffic flow monitoring, traffic congestion reduction, and accident prevention [11–14]. However, while the benefits are widely acknowledged, numerous drawbacks also come with such combinations or integrations, particularly for data security and privacy [15–18]. The vast amounts of data generated by IoT devices are vulnerable to cyber-attacks and data breaches. This is a major security concern. Therefore, it is very important to build a secure ITS. For example, an ITS may expose an individual's whereabouts in transit or in place. If people's movements are tracked, the attackers can even change the mode of attack on ITS

systems, waiting for individuals or goods to arrive at their destinations, or a plan could be devised for a future attack on the same route. Security is a broad field that also encompasses privacy. Therefore, ensuring system security involves protecting the entire ecosystem against various threats.

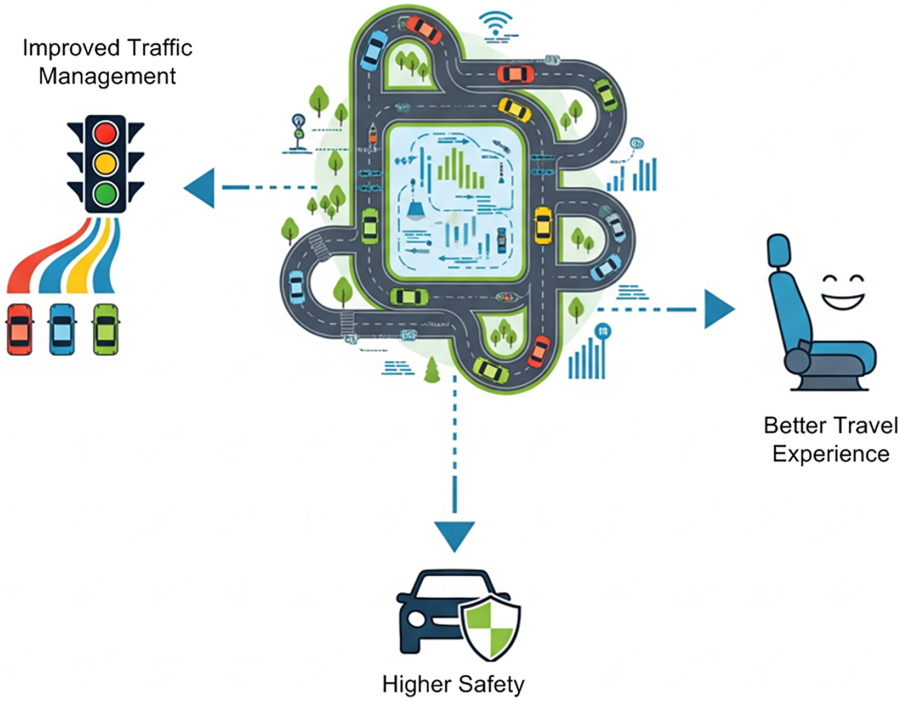

Figure 1: A high-level example architecture showing the confluence of technologies for the development of AI-enabled, IoT and 6G supported ITS.

IoT devices are becoming increasingly capable in terms of processing power and intelligence. Advancing AI technologies can contribute to ITS. 6G can let participating devices communicate with each other more efficiently [19]. Therefore, these devices will need extended capabilities. In such a scenario, much more computation will need to be done in ITS, at the edge, and in the fog. This shift towards localized information processing creates new vulnerabilities because processing critical information at endpoints increases the number of potential entry points for attackers. Hence, security will be critical as the ITS technology advances and gets integrated with other technologies.

Prior to the new advances in ITS, communication was slower, and information was computed upstream in the cloud. Even in that case, securing the cloud and ensuring trust with sufficiently protected communications links was challenging. Consider the new world of more powerful and distributed ITS devices. We will soon have 6G networks [20], and sophisticated AI systems embedded on or near these ITS devices, bringing the computation of critical information to ITS devices [21], the edge, or fog. This means that there will be far more targets for attackers to intrude into the network via various entry points. Hence, this setting adds more security targets by expanding the overall attack surface.

AI is being developed alongside IoT, which could be a potent tool for detecting abnormalities, predicting dangers, and implementing security measures in real-time. Moreover, the enhanced speed, reduced latency, and better security features of 6G may boost the efficacy of AI algorithms [22–26]. Here, we explain how AI may improve the security of IoT-based ITS using 6G technology. While we focus on the interoperability and security problems in these systems, the risks and limitations of IoT-based ITS are also highlighted, followed

by AI-enabled solutions to these issues. Table 1 shows a comparison of current literature in the fields of 6G, IoT, and ITS.

Table 1: A comparison of current literature in the fields of 6G, IoT and ITS.

Ref.	Key Themes in Survey	Key Findings
[27]	6G enabling technologies and use cases overview	This work focuses on 6G in transportation, specifically examines its impact on secured IoT-based ITS using AI.
[28]	IoT Architecture, Technologies, Security, Privacy, Applications	This survey provides a general overview of IoT.
[29]	Edge AI, 6G, Enabling Technologies, Applications	This work specifically looks at AI for security in IoT-based ITS with 6G, and mentions edge computing as a future direction.
[30]	Machine Learning, Deep Learning, IoT Security	The provided article integrates 6G as an enabler for these AI algorithms in ITS.
[31]	6G Security Requirements, Challenges, Applications	The provided article specifically ties 6G security to IoT-based ITS and the role of AI in addressing these challenges.
[32]	IoT, Smart Cities, Technologies, Practices, Challenges	The provided article narrows down to IoT in ITS within the smart city context, emphasizing security with AI and 6G.
[33]	Intelligent Vehicular Networks, 6G, Machine Learning	This survey focuses on machine learning in vehicular networks for 6G, aligning with the provided article's exploration of AI in 6G-enabled ITS.
[34]	IoT, Smart Systems, Challenges, Trends, 5G-IoT	This survey covers general IoT issues for next-gen systems and 5G-IoT.
[35]	AI/Intelligence, IoT, 5G Networks, Opportunities, Challenges	This survey focuses on 5G while our article extends this to 6G and the explicit role of AI in securing IoT-based ITS.
[36]	6G, Internet of Vehicles, Security, Privacy	This survey directly aligns with the our article's focus on 6G, security, and transportation.
[37]	Explainable AI (XAI), 6G Use Cases, Challenges	This article mentions Explainable AI as a future research direction to address trustworthiness in AI for ITS.
[38]	6G Vision, Requirements, Challenges	This survey offers a broad overview of 6G.

(Continued)

Table 1 (continued)

Ref.	Key Themes in Survey	Key Findings
[39]	6G Vision, Requirements, Challenges, Opportunities	This is a general 6G survey. The provided article focuses on the interplay of 6G, AI, and IoT for secure ITS.
[40]	Advanced Deep Learning Models, 6G, Overview, Opportunities, Challenges	This survey focuses on deep learning in 6G.
[41]	6G, Autonomous ITSs, Mechanisms, Applications, Challenges	This survey, specifically addressing 6G and autonomous ITS, highly aligns with the core theme of our article.
Our survey	The combination of IoT, 6G, and AI to build smart, connected, and autonomous ITS; identification and addressing of security threats	While our work shares a somewhat similar theme with other surveys, it specifically focuses on the construction of intelligent and secure IoT-based ITS. We talk about how this is achieved with 6G and AI technologies. We present a theoretical performance analysis based on standard 6G KPIs (Key Performance Indicators), evaluating system parameters such as latency, packet delivery ratio, energy consumption, and security overhead.

Our comparative analysis in Table 1 reveals that the existing literature largely focuses on 5G and basic AI applications. However, the interaction between the ultra-dense network architecture that 6G will bring and AI-powered cyberdefense has not been sufficiently examined. Our study re-evaluates these scattered studies through security, latency, and scalability parameters and contributes to the literature for future ITS architectures. The scope of this work addresses the technological convergence of 6G wireless networks, AI frameworks, and IoT architectures, particularly within the context of ITS. The main objective of this study is to analyze, from a holistic perspective, how 6G wireless networks and AI frameworks transform the security and performance parameters of IoT-based ITS. All sections of the study are structured to support this main objective, addressing security risks, AI solutions and how 6G infrastructure optimizes these solutions. While IoT and AI have broad applications across various sectors, this work limits its analysis to transportation-related use cases mainly, such as autonomous driving, intelligent traffic management, and infrastructure monitoring. When it comes to the issue of network analysis, it focuses specifically on the 6G paradigm, which is characterized by its THz capabilities and ultra-low latency. In fact, the previous studies focused solely or mainly on 5G or 4G infrastructure.

1.1 Major Contributions of This Survey

This work not only lists existing technologies but also analytically reveals the critical impact of 6G's ultra-low latency on AI-based safety protocols in ITS. Unlike literature reviews, it fills a significant gap in the literature by addressing the balance between security and performance from a 6G and AI perspective. The key contributions of the paper are as follows:

- ➢ A comprehensive overview of the vulnerabilities and challenges in IoT-based transportation systems.
- ➢ The improvement potentials of 6G technology are examined for the security and interoperability of ITS.
- ➢ AI-based techniques and algorithms are investigated to enhance security and facilitate interoperability.
- ➢ AI applications are discussed for various use cases such as anomaly detection, threat prediction, security measures, etc.
- ➢ Future research directions and challenges have been identified for 6G-enabled AI-based security and interoperability solutions in smart ITS.

1.2 Survey Methodology

During the paper selection process, we were keen to maintain the highest scientific standards and hence, we applied a strict hierarchical inclusion criterion. The priority was given to peer-reviewed journal articles and procedural articles from notable publishers such as IEEE, ACM, and Elsevier, ensuring the inclusion of studies that have undergone rigorous peer-review processes. As 6G and AI, both technologies are rapidly evolving, we have also taken into consideration the high-quality IEEE conference proceedings from prestigious venues. This mechanism has ensured that the latest standardization studies and experimental results have also been incorporated. For each selected study, three quality criteria were considered: (1) technical depth and methodological soundness, (2) relevance to the convergence of 6G, AI, and ITS, and (3) recent impact on the scientific community. It should be mentioned that non-peer-reviewed preprints and technical reports lacking technical validation were systematically excluded to ensure the reliability of the survey findings.

In order to ensure the internal and external validity of this review study, several quality control measures were applied. First, our search and selection process adhered strictly to preferred reporting items for systematic reviews and meta-analyses (PRISMA) guidelines to minimize selection bias (Fig. 2). The PRISMA checklists are available in the supplementary file. Second, data triangulation was performed by synthesizing findings from multiple scientific databases and indexing services like IEEE Xplore, Web of Science, and Scopus, to ensure that the identified trends in 6G and AI-powered ITS were not limited to the perspective of a single publisher. Third, the validity of the technical classification was verified through cross-referencing among independent studies to ensure the accuracy of the taxonomy presented in Tables 1–3. This rigorous approach guarantees that the qualitative insights and theoretical performance analyses presented in subsequent sections are scientifically sound and are representative of the global research environment.

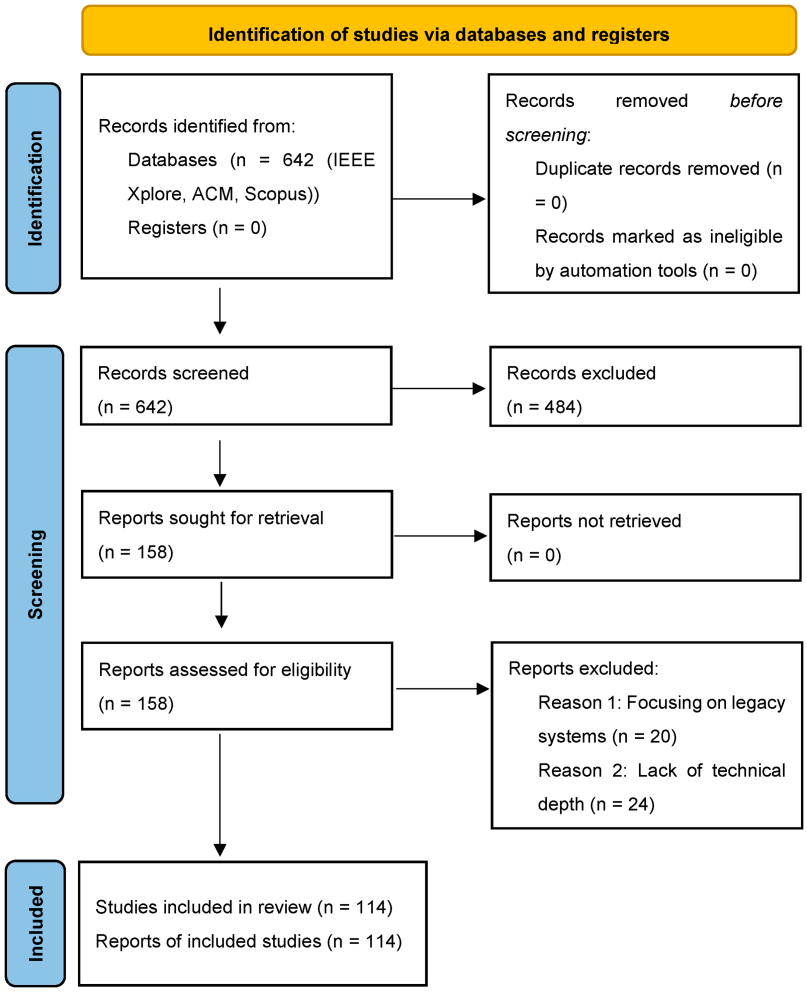

Figure 2: PRISMA flow diagram.

Table 2: IoT applications in ITS with quantitative service requirements.

Application Area	IoT Devices & Technologies	Latency Req.	Data Rate Req.	Reliability Req.	Typical Traffic Pattern
Autonomous driving	Light Detection and Ranging (LiDAR), radar, vehicle-to-everything modules, cameras	<1 ms	>1 Gbps	>99%	Continuous, high-bandwidth
Smart traffic management	Roadside sensors, inductive loops, IP cameras	10–100 ms	10–50 Mbps	>99%	Periodic & event-driven
Fleet management	GPS trackers, OBD-II dongles, RFID tags	Seconds to Minutes	<100 kbps	>99%	Burst, low-volume

(Continued)

Table 2 (continued)

Application Area	IoT Devices & Technologies	Latency Req.	Data Rate Req.	Reliability Req.	Typical Traffic Pattern
Passenger infotainment	4K/8K video streaming, AR/VR headsets	<20 ms	>100 Mbps per user	>99%	Continuous, downlink-heavy
Smart parking	Magnetic/ultrasonic sensors, LPWAN	Tolerant (Seconds)	<1 kbps	>99%	Sporadic
Emergency vehicle preemption	Road Side Units (RSU), sirens, vehicle to infrastructure	<10 ms	<1 Mbps	>99%	Event-driven

Table 3: Taxonomy of security threats in IoT-Based ITS layers with performance impacts.

ITS Layer	Security Threat	Target Component	Countermeasures	Performance Impact/Cost
Perception layer (Edge/Device)	Sensor spoofing & jamming	LiDAR, radar, GPS receivers	Multi-modal sensor fusion, signal strength analysis	High computational latency at the Edge.
Physical tampering	On-Board Units (OBU), RSU	Hardware security modules, physical unclonable functions	Increased hardware cost; Minimal latency impact.	
Network layer (Communication)	Sybil & masquerading attacks	Vehicle to vehicle, V2I communication links	Public key infrastructure, digital signatures	High bandwidth overhead due to certificate exchange.
Man-in-the-Middle (MitM)	6G/5G Wireless interfaces	Quantum-resistant encryption, mutual authentication	High processing load for encryption/decryption.	
Distributed Denial of Service (DDoS)/Jamming	Core Network, Base Stations	Network slicing, spectrum hopping, rate limiting	Throughput degradation; Potential service unavailability.	
Application layer (Cloud/Fog)	AI data poisoning	Traffic prediction models, autonomous driving AI	Federated learning, outlier detection algorithms	Reduced model accuracy; Slower convergence time.

(Continued)

Table 3 (continued)

ITS Layer	Security Threat	Target Component	Countermeasures	Performance Impact/Cost
Ransomware & malware	Central traffic management systems	Sandboxing, regular patching, intrusion detection systems	High storage overhead for logs; Operational downtime risks.	
Privacy leakage	User location data, trajectory logs	Differential privacy, encryption	Significant computational overhead for data processing.	

To ensure comprehensive coverage and scientific quality of the work, the selection of target studies followed a multi-stage systematic screening process. Initially, a broad search was conducted across large databases such as IEEE Xplore, ACM, and Scopus, using defined Boolean queries. In the second stage, the identified 642 records were subjected to title and abstract screening to filter out articles that did not explicitly address the convergence of at least two key areas (6G, artificial intelligence, or IoT-based ITSs). Following this, 158 articles underwent full-text review and were evaluated based on their contributions to safety frameworks, performance analysis, or architectural design in transportation. Studies focusing solely on legacy systems or lacking technical depth were excluded in this phase. As a result, 114 key studies were selected for in-depth analysis based on their ability to provide fundamental data for classifying safety threats and identifying future research directions.

The rest of this paper is structured as follows. IoT in transportation systems is described in Section 2. Secure transportation systems are discussed in Section 3. Section 4 addresses AI in transportation systems. Then, 6G in transportation is explained in Section 5. Numerical analysis is provided in Section 6. Section 7 describes challenges and future research directions, while Section 8 concludes the paper.

2 IoT in Transportation System

IoT refers to the linking of physical things to one another and the larger Internet. These things are outfitted with embedded technology such as sensors, actuators, and other electronic devices, allowing them to collect, share, and act on data. In ITS, IoT facilitates communication and data exchange between cars, infrastructure, and road users. This results in smarter, more efficient, and safer settings [42–45]. Table 2 shows the applications of IoT in ITS.

2.1 Applications of IoT in Transportation Systems

A wide range of functions in the transportation sector can be supported by IoT to enable a broad spectrum of critical use cases. IoT plays a key role in providing continuous connectivity for realization of autonomous vehicles, enabling them to operate with minimal human intervention. IoT devices can facilitate necessary communication between vehicles, infrastructure, and the environment to ensure safe navigation. Beyond navigation operation, IoT sensors enable precise vehicle tracking and fuel monitoring, optimizing fleet management and maintenance schedules. Some real-time metrics can be monitored by IoT, such as a vehicle's speed, braking intensity, and direction changes, providing a comprehensive data profile for detecting reckless driving patterns. Furthermore, the tracking capabilities can help locate stolen vehicles and monitor

passenger movements. Overall, IoT can enhance the user experience by providing real-time data on parking availability and public transport updates, which can be effective in reducing urban traffic congestion and increasing efficiency for various types of journeys, whether long or short.

2.2 Benefits of IoT in Transportation Systems

The integration of IoT with ITS can offer a number of interesting benefits, some of which are:

- ITS can improve fleet management, optimize traffic flow, and cut down on fuel consumption.
- Improvement of road safety is possible by detecting dangerous driving behaviors, preventing accidents, and improving emergency response.
- The environmental impact of transportation systems can be mitigated with the aid of IoT if traffic congestion can be reduced, alongside optimizing fuel consumption.
- Overall, a better travel experience can be provided to the passengers with the help of IoT, as it can provide real-time information, personalized services, and enhanced comfort.

2.3 Challenges of IoT in Transportation Systems

The integration of IoT into ITS also presents several challenges like:

- IoT devices will produce a huge volume of data which would be difficult to protect and may become vulnerable to cyber-attacks and data breaches [46].
- When the general expectation is that the different manufacturers' devices will communicate seamlessly, significant challenges may arise to make it happen. Particularly, there is a need for common standards. It is really a great challenge to develop consensus among many manufacturers.
- Though IoT is envisioned to include millions of things, in reality, increasing numbers of devices and the overall volume of data may pose scalability challenges.
- Power management systems are required so that IoT devices manage their power efficiently. This will allow IoT devices to provide services, remain wake/alive, or participate in the network for a long time.

Despite these challenges, IoT has great potential to shape the future of ITS.

3 Secure Transportation System

This section identifies key vulnerabilities in the ITS ecosystem and outlines the current risk environment necessary for security remediation; this is a key objective of this paper. The security of ITS is crucial for the safety of people, property, and infrastructure. While traditional security measures [47] rely on physical security and human supervision, IoT-based ITS pose new problems that can complicate security threats and vulnerabilities.

The classification of security threats and IoT applications presented in this study is based on the ITS functional multilayer architecture, which is divided into three layers: sensing layer, networking layer, and application layer. This classification was chosen for two main reasons. First, it is consistent with standard architectural models used in the existing literature for classifying IoT-based systems so it ensures that our findings are comparable to current research. Second, this structure provides a logical framework for distinguishing between local physical vulnerabilities and broader communication risks. Using this classification, we can more effectively analyze how 6G's high-speed data transfer improves the network layer and how AI-powered anomaly detection secures the application layer, providing a systematic, evidence-based approach to the taxonomy of the research.

This section takes a deeper look into the security challenges [48–52], in IoT-based ITS to better understand how to address them with a multifaceted approach [53]. In Table 3, we show a layered classification

of security threats, mapping specific vulnerabilities to ITS layers while detailing the associated performance costs of countermeasures.

3.1 Security Risks in IoT-Based Transportation Systems

IoT devices are diverse and have been developed with different technical requirements. Some of these different technical requirements do not require security. This exposes ITS to various kinds of serious security threats as well. As these devices collect sensitive data such as biometric information, speed of objects, and their location, unauthorized access can lead to privacy breaches and identity theft. Rogue actors can exploit the vulnerabilities to take control of system operations, sabotage infrastructure, hijack vehicles, or even alter the timings of traffic signals. Again, the massive scale of IoT networks can be used to launch DDoS attacks that could disrupt emergency communications and fleet management operations in ITS. Another critical risk is false data injection (FDI) or sensor manipulation, which can mislead the autonomous navigation algorithms and cause fatal collisions on the road. In fact, if outdated software runs on the devices, such types of risks are further heightened as that provides the entry points for malware injection and installation.

3.2 An Approach to Secure Transportation Systems

It is not easy to secure IoT-based ITS. Security must be a key design and manufacturing attribute for IoT devices. This may include features such as trusted platform modules, secure boot mechanisms, and hardware-based encryption techniques. Secure coding practices should be used for IoT devices, and software vulnerabilities should be regularly patched. There should be mechanisms for automatic software updates so that the devices are always kept up-to-date to tackle the most recent threats.

A good approach is to deploy IoT devices in separate network segments that are isolated from the rest of the network. This could help limit the spread of an attack to other devices or systems if one of the devices is compromised. Authentication must be performed for every IoT device and user to ensure that only the authorized individuals and devices have access to sensitive data and systems. Some of the advanced authentication methods, such as multi-factor authentication, should be used. Strong encryption mechanisms should be used for protecting the sensitive data both in transit and in storage so that even in the case of a data breach by the malicious entities, sufficient level of protection can be ensured. To prevent unauthorized modifications, data integrity preserving mechanisms should be used.

Regular security testing should be conducted to ensure old vulnerabilities are not revived. Security testing should also be conducted at the preliminary design and setup stage of IoT systems to minimize the vulnerabilities. A crucial task would be collaboration and information sharing between public and private organizations. This can lead to building a common defense strategy against potential threats and rogue actors.

Multi-dimensional approaches to address security risks are needed. Particularly, safe and resilient transportation environments for ITS must be ensured.

4 AI in Transportation Systems

Building on the vulnerabilities identified in the previous section, this section focuses on the main theme of our article by examining the performance and threat prevention capabilities of AI techniques. AI is capable of analyzing large volumes of data and events in real-time. These capabilities allow better detection of threats or abnormal activities well before they can unleash havoc on ITS. AI can also add to understanding the existing system status, its vulnerabilities, and its readiness to cope with any emerging security threats. Current technological trends indicate effective use of AI in transportation systems to improve safety, efficiency, and sustainability. The integration of 6G technologies into ITS offers innovative solutions across a wide range of

areas, from network security to resource management. In this context, trust management mechanisms and physical layer security are addressed as critical focal points in studies [54–56]. Operational efficiency issues. such as traffic flow forecasting, intelligent road maintenance, and data offloading strategies. are detailed in studies [57–61] in the process of developing sustainable smart city infrastructures. Furthermore, deep learning-based resource forecasting, AI applications, federated learning, and AI-embedded network slicing techniques [62–66] are examined to maximize network performance, shedding light on future technical challenges and proposed solutions for the 6G ecosystem. In this section, we discuss issues, aspects, and advantages of AI in ITS. Table 4 lists out the advantages of AI in ITS.

Table 4: Advantages of AI in ITS.

Application Area	Description	AI Techniques	Benefits
Traffic Flow Optimization	Real-time analysis of traffic flow and dynamic adjustment of traffic signals, suggesting alternative routes and optimizing traffic flow.	Machine learning, deep learning, reinforcement learning	- Reduce traffic congestion - Optimize travel times - Increase fuel efficiency - Reduce emissions
Accident Prevention and Safety Improvement	Detecting dangerous driving behaviors and preventing accidents. Identifying potential hazards and warning drivers by analyzing vehicle sensor data.	Computer vision, natural language processing, time series analysis	- Increase road safety - Reduce accidents - Reduce insurance costs
Development of Autonomous Vehicles	Enable autonomous vehicles to perceive their environment, make decisions and move safely. Optimization of vehicle-to-vehicle communication and traffic flow.	Deep learning, reinforcement learning, multi-agent systems	- Reduce human error accidents - Increase traffic efficiency - Increase accessibility for people with disabilities
Optimization of Public Transportation Systems	Optimization of public transport schedules, forecasting passenger demand and improving services. Providing passengers with real-time information and personalized travel recommendations.	Prediction models, time series analysis, optimization algorithms	- Increase public transport use - Increase passenger satisfaction - Increase operational efficiency
Logistics and Supply Chain Management	Planning routes, optimizing deliveries and managing inventory levels.	Optimization algorithms, prediction models, robotic process automation	- Reduce delivery times - Reduce logistics costs - Improve inventory management

(Continued)

Table 4 (continued)

Application Area	Description	AI Techniques	Benefits
Improvement of Infrastructure Maintenance	Monitoring the condition of infrastructure such as bridges and roads for predicting maintenance needs.	Image processing, machine learning, sensor data analysis	- Increase infrastructure safety - Extend infrastructure life - Reduce maintenance costs

4.1 Applications of AI in Transportation Systems

AI algorithms can significantly enhance ITS services [67] by enabling real-time analysis of the traffic flow and adjusting traffic signals dynamically to minimize traffic congestion. Such systems can optimize travel times by suggesting efficient alternative routes. To ensure safety, AI-powered cameras can detect hazardous driving behaviors such as drowsiness or inattentiveness. which can trigger instant warnings. When combined with 6G, AI can facilitate real-time data transmission in the event of accidents, which can allow the vehicles to automatically slow down or find ways to avoid collisions based on live feeds. AI nowadays is a key technology for autonomous systems, which enables vehicles to be aware of their surroundings and navigate independently through various road connections and road conditions. AI can also optimize logistics and supply chain operations using vehicles, improve public transport schedules with passenger demand forecasts, and monitor infrastructure health to recommend proactive maintenance.

4.2 Benefits of AI in Transportation Systems

Some of the notable benefits of AI in the ITS are as follows:

- ➢ By optimizing traffic flow, reducing fuel consumption, and improving logistics operations, AI offers better efficiency for ITS.
- ➢ Road safety can be greatly enhanced by AI-driven active accident prevention mechanisms and the detection of dangerous driving behaviors.
- ➢ The environmental impact of ITS is minimized by the reduction of traffic congestion, optimizing fuel consumption, and as a result, reducing emissions.
- ➢ AI can improve travel experiences. It can even personalize travel experiences by satisfying individual expectations of comfort.
- ➢ AI can reduce the costs of transportation by increasing overall operational efficiency, saving fuel or gas, and lowering maintenance expenses.

4.3 AI and Security

By providing proactive mitigation strategies, AI algorithms enhance the security frameworks discussed earlier in Section 3. While Section 3.1 addresses core risks such as identity theft and data breaches, AI specifically addresses these risks through automated anomaly detection and real-time threat prediction. Table 5 summarizes how specific AI techniques are mapped to these security domains.

Table 5: AI and security.

Security Domain	AI Technique	Description
Anomaly Detection	Machine learning, deep learning (DL)	Identify security breaches by detecting anomalies in network traffic, sensor data, and system logs.
Threat Estimation	Prediction models, time series analysis	Predict potential security threats by analyzing historical data and trends.
Security Measures	Automation, robotic process automation	Automate security systems and take real-time security measures.
Attack surface	Ranking potential attack points and automated analysis of their value	Automate analysis of attack points and the value attackers will see in them.
Physical vulnerabilities	AI for testing ITS devices to ensure they behave properly and are legitimate	Attackers have access to physical aspects of ITS systems up to and including cloning hardware and software.

While the advantages and benefits are lucrative, the actual application of AI in ITS often faces some critical limitations. First, the black-box nature of DL models poses a significant challenge for safety-critical systems. In fact, without XAI, the decision-making process of a vehicle during an emergency situation cannot be fully understood. Again, AI models may be susceptible to data poisoning and hostile attacks. Even subtle manipulations of sensor data can lead an autonomous vehicle astray. There is also a critical challenge of a trade-off between a model's accuracy and processing delay. This is because while more complex neural networks provide better predictions, they can exceed the 10 ms communication time required for real-time collision avoidance in high-speed 6G scenarios.

This study not only discusses theoretical AI-based techniques but also examines their operational efficiency in 6G networks. Specifically, it comparatively evaluates the training and inference times of convolutional neural network (CNN) and recurrent neural network (RNN) architectures used to detect cyber threats in ITS data streams at the high THz data rates offered by 6G. This analysis provides technical evidence demonstrating how AI algorithms can not only enhance security but also meet the millisecond latency requirements of the 6G ecosystem. In examining AI techniques, the compatibility of FL models with the 6G ecosystem was particularly analyzed. Unlike traditional centralized models, it is found that models trained on edge devices reduce the risk of data leakage, and thanks to the high bandwidth offered by 6G, model update times are reduced to milliseconds.

5 6G in Transportation System

The next-generation wireless communication technology, 6G, is expected to surpass 5G in terms of speed, latency, and reliability [68]. If 6G technology is incorporated into ITS, it can significantly enhance its capabilities for a wide range of IoT and AI applications [69,70], which can create a safer and more efficient transportation ecosystem. In this section, we examine the potential benefits of 6G for ITS and analyze how this technology may impact the future of the transportation sector [71–75]. Table 6 presents the quantitative comparison of 5G and 6G capabilities for their requirements, while Table 7 presents the applications of 6G in ITS.

Table 6: Quantitative comparison of 5G and 6G capabilities for ITS requirements.

Key Performance Indicator (KPI)	5G Capability	6G Target	Impact on ITS
Peak Data Rate	20 Gbps	1 Tbps	It provides uncompressed 3D holographic maps and real-time raw sensor sharing between vehicles.
End-to-End Latency	1 ms	0.1 ms	It is critical for high-speed convoys and collision avoidance at speeds above 100 km/h.
Reliability	99%	99%	It is essential for safety-critical Level 5 autonomous driving, where failure is fatal.
Connection Density	10^6 devices/km^2	10^7 devices/km^2	It supports comprehensive IoT deployment in smart cities.
Mobility Support	500 km/h	>1000 km/h	It provides stable connectivity for high-speed trains and flying cars.
Positioning Accuracy	0.2–1 m	1–10 cm	It provides precise lane-level positioning and navigation for autonomous robots/cars.
AI Capability	Cloud-Centric AI	Native AI	It enables in-network intelligence, and the network itself optimizes traffic and safety.

Table 7: Applications of 6G in transportation systems.

Application Area	Description	Contribution of 6G
Advanced Autonomous Driving	Safer and more efficient operation of autonomous vehicles. Real-time data analysis and inter-vehicle communication.	- Ultra-low latency - High reliability - High-speed data transmission
Smart Traffic Management	Real-time monitoring and analysis of traffic flow. Reducing traffic congestion and optimizing travel times.	- High speed and capacity - Wide coverage
Enhanced Passenger Experience	More high-speed internet access, high-resolution video streaming, and immersive augmented reality experiences for passengers.	- High speed and capacity - Low latency
Monitoring and Maintenance of Transportation Infrastructure	Real-time monitoring and analysis of the condition of transportation infrastructure. Identifying and managing maintenance needs.	- High reliability - Wide coverage - Energy efficiency

(Continued)

Table 7 (continued)

Application Area	Description	Contribution of 6G
New Transportation Services	Developing new transportation services such as flying cars and drones.	- High speed and capacity - Ultra-low latency

5.1 What 6G Brings to the Transportation Systems

6G technology [76,77] can effectively transform ITS thanks to its superior performance capabilities. Compared to 5G technology, 6G offers significantly higher speeds and capacities, which will enable simultaneous transmissions of large volumes of data necessary for real-time analysis. This technology offers ultra-low latency, which can provide near-instantaneous communication, which is vital for safety-critical interventions in autonomous driving environments. In addition, 6G enhances system reliability, ensuring uninterrupted connectivity for emergency services and security systems. 6G also offers wider coverage, keeping vehicles connected even in rural areas where infrastructure may be less developed. Again, the energy efficiency in 6G networks allows the IoT devices and vehicles to operate for longer periods. This contributes to the overall sustainability of the smart transportation ecosystem.

However, some complex technical trade-offs [78,79] are required to deploy 6G-enabled smart ITS. While the THz band offers unprecedented bandwidth, its limited propagation range necessitates the large-scale deployment of small cells, which leads to a significant increase in infrastructure costs and energy consumption. Cost of deployment and energy requirements are the two very critical parameters that must be considered. Additionally, there is often a conflict between system security [80] and performance. We talked about using encryption techniques in Section 3; however, implementing robust and multi-layered encryption introduces computational overhead that can increase end-to-end latency as well. Hence, the trade-off for security-latency is critical in such a setting; if encryption operations cause delay for a security-critical message by more than 0.1 ms, the fundamental reliability advantage of 6G would be compromised. Therefore, real-world applications should be supported by lightweight cryptographic protocols that can provide adequate protection without violating the requirements of microsecond latency for the 6G networks.

5.2 Applications of 6G in Transportation Systems

The integration of unmanned aerial vehicles (UAVs) and electric vehicles (EVs) into the 6G-ITS framework addresses both connectivity and sustainability challenges. UAVs may act as airborne base stations to provide on-demand coverage and emergency communications relays, while EVs may focus on green urban mobility. By combining these technologies, 6G networks can optimize energy-efficient route planning and collaborative sensing [81–83]. For instance, UAVs can monitor traffic density from above, providing EVs with real-time charging station availability, effectively reducing urban congestion and energy waste. This synergy enables a more resilient and environment-friendly transportation ecosystem. Table 7 shows the applications of 6G in transportation systems.

5.3 Supporting Electric Vehicles with 6G and IoT

The recent advancements in the fields of EVs give us hope and shows some new possibilities for the future. The future ITS will eventually need to integrate the EVs, which could be the cornerstone of sustainable and environment-friendly transportation system. However, with the growth of the market and use of EVs, new challenges will also be brought into the scenario, such as tackling issues related to efficient management of charging infrastructure, optimizing battery life for the EVs, and balancing the load on the energy grid.

Potential misuse of electricity from a power grid may be disastrous for the regular electricity supply line. However, given this context, the support from 6G and IoT technologies can also be revolutionary for EVs. For instance, IoT sensors can continuously collect data such as the battery lifetime or status, location, and current energy consumption of each electric vehicle (EV) and then this data can be transmitted almost instantaneously to a central AI platform over 6G's ultra-low-latency, high-bandwidth networks [84–87]. This platform will analyze not only the vehicle data but also real-time data from all charging stations, such as occupancy rate, charging speed, pricing, and the current load status of the energy grid. Fig. 3 shows a 6G and IoT-enabled smart electric vehicle ecosystem.

Figure 3: 6G and IoT-supported smart electric vehicle ecosystem.

Future ITS must prioritize sustainable and environment-friendly frameworks to achieve global green mobility goals. Recent studies highlight that overcoming infrastructure and social barriers is essential for the successful adoption of green mobility in urban environments. Furthermore, establishing the key criteria for sustainable urban transportation is critical for balancing the energy grid while promoting a greener future. Integrating these sustainability criteria with the ultra-low latency of 6G enables more efficient management of charging infrastructure and battery life, making it possible to circumvent the complex challenges associated with large-scale EV deployment.

Eventually, this kind of integration makes the following scenarios possible:

- Consider a scenario when an EV driver wants to find the nearest charging station. The system determines the most suitable station by taking into account the driver's route, battery level, and arrival time, minimizes waiting time, and even automatically reserves a charging point before the driver arrives. This is achieved by instantaneously communicating between thousands of vehicles and stations, thanks to 6G's Tbps speed and microsecond latency.
- 6G-enabled EVs are expected to be efficient and have good electricity reserves in their batteries. These features could be used both by the energy consumers and the energy storage units. For instance, during the peak hours for energy demand, energy grid operators can connect to thousands of parked EVs via

the 6G network to request that they temporarily transfer excess energy stored in their batteries back to the energy grid. Thus, the flexibility and resilience of the energy grid can be enhanced.

- 6G can improve performance by accelerating data flow between the vehicle's battery management system and other control units. Again, the collected data can enable predictive maintenance algorithms to detect potential battery failures in advance.

5.4 The Role of UAVs in 6G-Enabled ITS

UAVs [88] hold transformative potential in the evolution of ITS because of their flexibility, rapid deployment, and unique aerial perspectives. UAVs overcome the limitations of traditional ground-based sensors and infrastructure, which open new horizons for ITS. When this technology is combined with the ultra-reliable, low-latency, and high-bandwidth communication capabilities provided by 6G networks [89], real smart and efficient systems can be developed. Fig. 4 depicts a conceptual diagram illustrating how UAVs could be integrated with the future ITS.

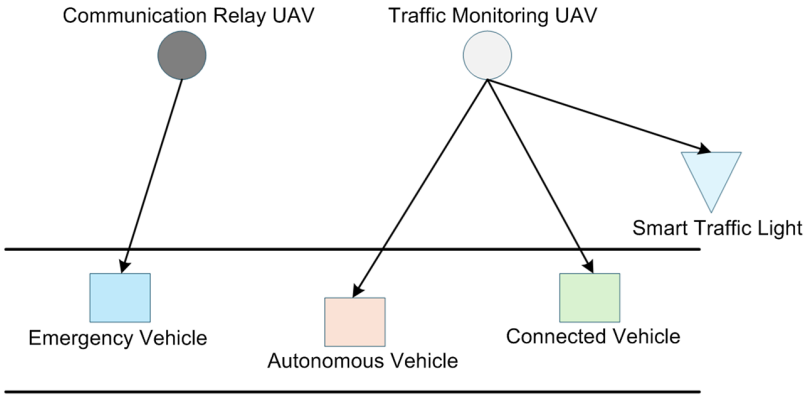

Figure 4: A conceptual diagram showing how UAVs could integrate with future ITSs.

The key areas that can benefit from the integration of UAVs into 6G-enabled ITS are:

- UAVs possess a unique ability to fly over densely populated areas, specific accident sites, or incidents/accidents occurring over a wide area, and provide real-time, high-resolution video streams to traffic management centers. 6G's Tbps data transfer speeds enable the uninterrupted transmission of this large volume of video data. With ultra-low latency, this system allows UAVs to be controlled in complex urban environments in real time. Therefore, it enables dynamic traffic flow optimization and immediate response to incidents.
- Due to the flexibility of movement above the roads, UAVs can reach the accident scenes much faster than ground vehicles constrained by road grids and traffic. Then, these UAVs can assess the severity of the situation and transmit live images to first responders such as the ambulances, emergency crews, fire departments, and police to ensure their preparedness. It is even possible for UAVs to play a lifesaving role by delivering small, critical equipment or medical supplies in critical situations with the support of 6G's highly reliable communication setting.
- UAVs may be equipped with high-resolution cameras, thermal sensors, and LiDAR. This enhances the UAV's capability as it can then autonomously inspect critical transportation infrastructure such as bridges, highways, tunnels, and power lines. When AI-powered algorithms and programs are installed on the UAVs, these can collect data, to detect structural damages, cracks, and analyze that data without explicit human intervention. This kind of system can reduce inspection costs, lower the risks to human life, and lead to proactive maintenance.

- The integration of 6G communication capabilities for UAVs can facilitate the simultaneous management of large delivery fleets without the risk of collisions.
- In some situations, the existing cellular infrastructure can get damaged, for instance, when natural disasters hit like cyclones, tornadoes, earthquakes, etc. In critical emergency scenarios where ground infrastructure is compromised, UAVs can be deployed as mobile base stations to ensure network continuity. These *flying base stations* can provide a temporary 6G communications network for the rescue teams and affected citizens who are using various types of vehicles to ensure the continuity of critical communications.

5.5 6G-Enabled AI Architectures for ITS

It should be noted that initially, 5G technology enabled the deployment of AI in ITS. When sufficient advances were made in the technology, and it reached an appropriate level, AI's integration with 6G makes more sense. Today, 6G is envisioned as an AI-based network or at least a network that would use AI in many of its operations or in its core operations. This integration is expected to fundamentally change how our ITS systems operate by shifting computations from centralized clouds to the edge. Let us now discuss a few important points for 6G-enabled AI-supported ITS:

- Privacy restrictions in ITS typically prevent raw data sharing. Federation Learning (FL) allows vehicles to train local models and share only gradient updates. However, FL experiences communication bottlenecks in 5G due to high latency during parameter collection. 6G's ultra-low latency and THz bandwidth can eliminate this bottleneck, enabling near-real-time global model convergence for collaborative autonomous driving.
- 6G enables the creation of high-accuracy digital twins for entire smart cities. By leveraging 6G's target data rates of 1 Tbps, physical traffic patterns can be projected onto the cyber world with sub-millisecond synchronization. AI algorithms can run simulations on such a cyber twin to predict accidents or optimize traffic flow before sending control commands back to the physical infrastructure.
- A smart and working ITS would require different levels of quality of service (QoS) simultaneously. If AI is directly integrated into the network management layer, 6G can automatically and dynamically resize network slices based on real-time traffic density estimates, which can ensure safety-critical messages to potentially never experience congestion scenarios.

6 Performance Analysis: 5G vs. 6G in ITS

This section presents a theoretical performance analysis comparing 5G and 6G capabilities in the context of ITS. Here, we have not relied on specific simulation experiments, but rather we focus on three critical parameters for the theoretical performance analysis: channel capacity, transmission delay, and security overhead. It should be noted that this analysis is based entirely on fundamental information-theoretical bounds and the 3rd generation partnership project (3GPP) specifications.

6.1 Channel Capacity and Data Rate Limits

We can use the Shannon-Hartley theorem to determine the maximum achievable data rate. The capacity C (in bps) for a secure ITS application can be defined by:

$$C = B \cdot \log_2 (1 + \mathrm{SNR}) \tag{1}$$

where B is the bandwidth and SNR is the Signal-to-Noise Ratio. Let us now take into consideration two scenarios:

- *Scenario for 5G:* It operates in the mmWave band, with a typical bandwidth (B) of 100 to 400 MHz.

➢ *Scenario for 6G:* It operates in the THz band, provides ultra-wide bandwidth ranging from 10 to 100 GHz.

If we consider the same SNR levels, 6G offers an increase of theoretical capacity, of approximately 100x to 1000x, because of its available spectrum alone ($B_{6G} \gg B_{5G}$). This massive pipe is essential for transmitting uncompressed LiDAR point clouds, which typically require greater than 1 Gbps link speeds. This is indeed a feat that would be unattainable with standard 5G at the cell edge.

To ensure the technical rigor of the performance evaluation, a methodological framework was constructed based on a combination of theoretical modeling and 3GPP standardized parameters. Channel capacity analysis uses the Shannon-Hartley theorem, comparing a 5G environment operating at 28 GHz with a 400 MHz bandwidth to a 6G environment operating at 300 GHz with an ultra-wide 50 GHz bandwidth. For latency modeling, a line-of-sight (LoS) propagation environment is assumed to minimize multiple-path fading variables. Security payload calculation specifically models the impact of 256-bit encryption headers on the total packet size. Furthermore, the MATLAB-based simulation environment used for validation assumes a high-density vehicle node distribution consistent with 6G link density targets to evaluate the scalability of the proposed ITS architecture.

Our analysis results clearly show that the encryption overhead, a significant bottleneck in 5G, no longer negatively impacts system performance thanks to 6G's high Tbps data rates. This finding proves that even the most complex AI algorithms can be run in real-time on ITS without compromising security.

6.2 End-to-End Latency Analysis

Delay in ITS is the sum of propagation delay, transmission delay, processing delay, and queuing delay. The most significant improvement in 6G comes from the air interface delay (T_{air}). According to 3GPP Release 16 (5G NR) for 5G networks, the minimum subcarrier spacing (SCS) allows for a transmission time interval (TTI) of approximately 0.5 to 1 ms. In contrast, 6G targets an air interface delay of $T_{air} \cong$ 10–100 μs. The total delay budget (T_{total}) for an autonomous braking decision can be modeled as:

$$T_{total} = T_{air} + T_{sec} + T_{proc} \tag{2}$$

here, T_{sec} represents the security transaction latency. T_{proc} represents general data processing times, excluding security-related periods. 6G's sub-100 μs latency provides a greater time margin for complex cryptographic operations and enables stronger encryption algorithms without violating the strict 10 ms security threshold for vehicle-to-vehicle communications.

6.3 Security Overhead Trade-off

A robust security implementation in an ITS imposes a computational and bandwidth overhead. The security overhead ratio (S_{OH}) can be defined as:

$$S_{OH} = \frac{L_{auth} + L_{enc}}{L_{payload}} \tag{3}$$

L_{auth} and L_{enc} are the lengths of the authentication headers and the encryption padding, respectively. In legacy IoT systems (with low bandwidth), a large S_{OH} would cause packet fragmentation and high latency. However, in 6G-supported ITS, the ultra-high data rate minimizes the transmission time penalty of S_{OH}. Thus, 6G provides intense security with a negligible impact on the overall packet delivery ratio (PDR), addressing the tradeoff often seen in bandwidth-constrained 5G IoT networks.

To verify the theoretical feasibility of the proposed 6G-enabled ITS architecture, a numerical performance evaluation was performed using a MATLAB simulation environment based on fundamental information-theoretic bounds and the 3GPP Release 16 specifications. As shown in Fig. 5, the analysis demonstrates the order-of-magnitude gain provided by the ultra-wide terahertz bandwidth compared to 5G mmWave by modeling the channel capacity using the Shannon-Hartley theorem. The end-to-end delay budget is then decomposed into air interface, processing, and security components to evaluate compliance with the stringent 10 ms security threshold required for autonomous driving. Finally, the transmission penalty of cryptographic overhead was quantitatively calculated at varying data rates, and it has been verified that migrating from Gbps to Tbps speeds renders the delay impact of heavy-duty security protocols as negligible.

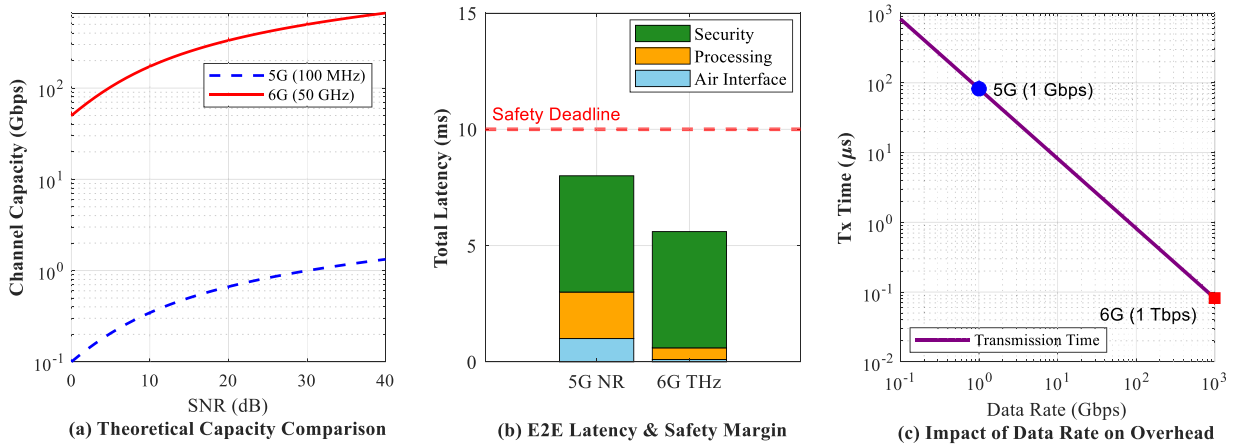

Figure 5: Performance metrics of the ITS vs. SNR.

According to our research findings, AI algorithms used in 6G-enabled smart ITS improve PDR by optimizing data traffic on the network. The examined FL model protects data privacy by allowing vehicles to train their local models without sharing raw data. This significantly reduces model update times compared to traditional 5G networks, thanks to the broad bandwidth provided by 6G infrastructure. These findings demonstrate that AI-based techniques are not just a benefit, but an integral performance component of the 6G-ITS architecture.

7 Challenges and Future Directions

While the combination of IoT, AI, and 6G technologies has the potential to completely transform ITS, there are some critical hurdles to overcome before this vision can become a reality. In particular, data security and privacy protection remain top priorities in IoT-based structures; in this regard, privacy-focused federated learning and blockchain-based authentication models [90,91] stand out in the search for solutions. On one hand, the lack of a standard protocol that ensures full compatibility between devices from different manufacturers remains a serious problem. The extensive studies on the 6G vision and standardization processes [92–96] attempt to shed light on these uncertainties. On the other hand, the ultra-intensive data traffic that 6G will bring will create pressure on scalability, leading to a massive infrastructure need [97–101]. Finally, technical challenges such as the integration of intelligent surfaces into ITS and the use of artificial intelligence in vehicle-to-everything (V2X) communication [102,103] still present significant obstacles to overcome in terms of system sustainability. Moreover, energy efficiency and power management strategies remain critical research areas in this ecosystem where numerous devices are active simultaneously [104–108].

In addition to all these technical requirements, the ethical dimensions of autonomous decisions will play a decisive role in the success of future 6G-enabled ITS [109]. This section highlights the key challenges faced by 6G-enabled AI-based ITS and offers suggestions for future research opportunities.

7.1 Challenges

Previous ITS security studies revealed that the fundamental vulnerability stems from the inability to resolve the negative correlation between security and performance. In previous models, highly secure protocols caused latency, while low-latency models weakened security. Our analysis offers critical insight into how the broad bandwidth offered by 6G can disrupt this zero-sum game and how AI-based lightweight encryption methods can close this gap.

The security and privacy issues present in IoT-based ITS, discussed in detail in Section 3.1, are further amplified in the 6G environment due to increased data volume and more entry points. Therefore, previously established robust security mechanisms and encryption standards must be adapted to meet the ultra-low latency requirements of 6G.

With the evolution of ITS systems integrated with 6G technology, the attack surface also increases and hence, even the attackers will have the same advantage of speed and accessibility. Another issue is that the ITS systems will be relatively easier to access physically for the attackers leading to direct hardware manipulation. A defense mechanism against this could be strong tamper-resistant technology for the ITS devices. Tamper resistant or tamper evident research is still insufficient in this regard.

Table 8 illustrates the challenges and future directions of 6G-enabled AI-based ITS.

Table 8: Challenges and future directions of 6G-enabled AI-based ITS.

Challenges	Description	Future Research Directions
Security and Privacy	Safeguarding the enormous volume of data produced by IoT devices against privacy threats and security lapses.	- Strong authentication and authorization - Data encryption and anonymization - Attack detection and remediation of vulnerabilities - Blockchain technology - Ethics and regulatory frameworks
Physical insecurity and larger attack surfaces	More ITS devices will be physically vulnerable. As ITS devices, the edge, and the fog compute more critical information, ITS attack surfaces will grow.	- Build tamper resistant IoT systems using AI - Securing high value attack points for dynamic ITS devices - Tradeoffs: attack surface growth and quality information in ITS devices, the edge, and fog
Interoperability	Seamlessly communicating and sharing data between IoT devices and systems from different manufacturers.	- Standardized protocols and data formats - Open-source software and platforms - Semantic interoperability
Scalability	As IoT devices and data volumes increase, transportation systems can scale to support this growth.	- Scalability of 6G networks - Scalability of AI algorithms and data analytics platforms - Cloud computing and distributed systems

(Continued)

Table 8 (continued)

Challenges	Description	Future Research Directions
Power Management	Maximizing the energy use of IoT devices.	- Energy efficiency and power management strategies - Energy harvesting and wireless power transfer
Infrastructure and Cost	Infrastructure investments and costs required for the deployment of 6G networks and AI-based systems.	- Cost-effective solutions - Public-private partnerships
Ethics and Social Impact	Addressing the ethical and social impacts of AI-based ITS.	- Ethical decision-making processes for autonomous vehicles - Potential for job loss - Data privacy and discrimination - Social acceptance and trust

One of the biggest challenges for IoT systems and devices is interoperability when different manufacturers do not have commonly agreed-upon standards or policies for connecting their devices and systems to allow data exchange. Interoperability must be enhanced, and data transmission between diverse systems should be facilitated by using standardized protocols and data formats. With the increasing number of IoT devices, ITS must be scalable to support the required growth. The scalability of 6G networks is critical for managing the large number of devices and high data traffic. In addition, AI algorithms and data analytics platforms should also be scalable to meet the demands of increasing data volume and processing.

A key challenge of IoT devices is the increased energy consumption and energy demand, especially when thousands of devices are active at the same time. Hence, advanced energy management strategies must be developed and would be critical to ensure the long-term operation of IoT devices and the sustainability of transportation systems in the future network settings.

The real-life deployment of 6G networks aided by AI-based systems will require significant cost for infrastructure. The existing transportation infrastructure should be integrated with 6G technology as a vital step to accelerate the adoption of these technologies.

While the AI-based ITS offers many benefits, the social and ethical impacts of such systems should be considered carefully. There may be harmful incidents or cases when the autonomous vehicle's decision-making process can create more trouble than benefit in real-life traffic conditions. While human beings employ not only their intelligence but also intuition for making decisions while driving or path-finding, AI-enabled vehicles autonomously running on the roads may not be able to make such quick intuition-based decisions. In connection with the previous point, while data privacy should be at the heart of ethical discussions and standardizing regulations, this kind of system can even cause job losses. Thus, negative social impacts should be sufficiently assessed before deploying such systems.

7.2 Future Research Directions

Investigating the balance between ultra-low latency and computational overhead, particularly for THz band communications and large-scale hardware deployment. Developing XAI models to ensure

transparency in autonomous decision-making and exploring blockchain-based frameworks for decentralized identity management. Designing energy harvesting techniques for IoT sensors and establishing international standards to connect diverse systems and support cross-border interoperability and ethical use of data.

Security and privacy are critical design features for small IoT systems in ITS. These IoT devices may be physically exposed to attacks. So, handling physical attacks as well as other security breaches with low-power sensors is an important area to explore.

Because of their decentralized and dynamic structures, ITS devices cannot fully trust each other, as some may act selfishly or be compromised. Therefore, a distributed consensus mechanism is necessary where blockchain can play a significant role in ITS [110]. However, such blockchain-based systems should also support low power consumption.

ITS system components should be designed and developed based on the pragmatic and real-life data rate support [111]. Sufficient research is needed in this direction. Real-life road traffic conditions need to be studied thoroughly for training of the AI components and tools so that hazardous and conflicting scenarios may be handled when smart ITS might manifest a suboptimal decision-making process. When EVs are to be supported, efficient and secure charging mechanisms should also be developed.

Addressing these challenges and exploring future directions would be critical to fully realize the potential of 6G-enabled AI-based ITS and create a safer, more efficient, and more sustainable transportation future.

8 Conclusions

This study systematically addresses all the research objectives presented in the introduction. Our analyses fill gaps in the literature by identifying critical security vulnerabilities in IoT-based ITS and by providing a comprehensive classification of these risks. Performance evaluations demonstrate that the THz bandwidth offered by 6G technology can maintain millisecond latency despite high encryption overhead, thus fulfilling the promise of secure and high-performance infrastructure. Moreover, the effectiveness of the AI techniques examined in the areas of anomaly detection and proactive threat prediction is validated, and a concrete framework for interoperability between systems is established. The integration of these technologies offers a bright future for green and environment-friendly transportation systems to be used in smart cities. However, we argue that the potential benefits often come with numerous drawbacks as well, especially when data security and privacy are considered. This study has identified the key vulnerabilities and issues in IoT-based and AI-enabled transportation systems. We mentioned that the improved speed, reduced latency, and better security features of 6G have real potential to enhance the efficiency and efficacy of AI algorithms. While AI is emerging as an impactful technology for detecting abnormalities, predicting risks, and implementing security measures in real-time, multifaceted challenges still remain to be tackled in a systematic manner.

Overall, the combination of 6G and AI will offer new possibilities for effective, secure, and dependable IoT-based transportation systems. The core objective of this study is to investigate several AI-based strategies and mechanisms to improve security and interoperability. AI applications for a variety of use cases are covered, including anomaly detection, threat prediction, and security measures. Future research directions may include trustworthiness and explainability aspects of AI, FL, and edge computing in this context.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Muhammet Ali Karabulut and A. F. M. Shahen Shah; writing—original draft preparation, Al-Sakib Khan Pathan; writing—review and editing, Phillip G. Bradford. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Supplementary Materials: The PRISMA checklists are available in the supplementary file. The supplementary material is available online at https://www.techscience.com/doi/10.32604/cmc.2026.077625/s1.

References

1. Liu R, Hua M, Guan K, Wang X, Zhang L, Mao T, et al. 6G enabled advanced transportation systems. IEEE Trans Intell Transport Syst. 2024;25(9):10564–80. doi:10.1109/tits.2024.3362515.
2. Mustari N, Ali Karabulut M, Shah AFMS, Tureli U. Terahertz communication with MIMO-OFDM in FANETs for 6G. Open Transp J. 2023;17(1):e187444782301180. doi:10.2174/18744478-v17-230810-2023-7.
3. Vivek Menon U, Babu Kumaravelu V, Vinoth Kumar C, Rammohan A, Chinnadurai S, Venkatesan R, et al. AI-powered IoT: a survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications. IEEE Access. 2025;13(2):50296–339. doi:10.1109/ACCESS.2025.3551750.
4. Letaief KB, Shi Y, Lu J, Lu J. Edge artificial intelligence for 6G: vision, enabling technologies, and applications. IEEE J Select Areas Commun. 2022;40(1):5–36. doi:10.1109/jsac.2021.3126076.
5. Ali Al-Garadi M, Mohamed A, Al-Ali AK, Du X, Ali I, Guizani M. A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Commun Surv Tutorials. 2020;22(3):1646–85. doi:10.1109/comst.2020.2988293.
6. Abdel Hakeem SA, Hussein HH, Kim H. Security requirements and challenges of 6G technologies and applications. Sensors. 2022;22(5):1969. doi:10.3390/s22051969.
7. Cheng H, Shojafar M, Alazab M, Tafazolli R, Liu Y. PPVF: privacy-preserving protocol for vehicle feedback in cloud-assisted VANET. IEEE Trans Intell Transport Syst. 2022;23(7):9391–403. doi:10.1109/tits.2021.3117950.
8. He Q, Lin J, Fang H, Wang X, Huang M, Yi X, et al. Integrating IoT and 6G: applications of edge intelligence, challenges, and future directions. IEEE Trans Serv Comput. 2025;18(4):2471–88. doi:10.1109/TSC.2025.3586152.
9. Elassy M, Al-Hattab M, Takruri M, Badawi S. Intelligent transportation systems for sustainable smart cities. Transp Eng. 2024;16(17):100252. doi:10.1016/j.treng.2024.100252.
10. Sarwatt DS, Lin Y, Ding J, Sun Y, Ning H. Metaverse for intelligent transportation systems (ITS): a comprehensive review of technologies, applications, implications, challenges and future directions. IEEE Trans Intell Transp Syst. 2024;25(7):6290–308. doi:10.1109/TITS.2023.3347280.
11. Wang C, Shen J, Vijayakumar P, Gupta BB. Attribute-based secure data aggregation for isolated IoT-enabled maritime transportation systems. IEEE Trans Intell Transport Syst. 2023;24(2):2608–17. doi:10.1109/tits.2021.3127436.
12. Gallego-Madrid J, Sanchez-Iborra R, Ortiz J, Santa J. The role of vehicular applications in the design of future 6G infrastructures. ICT Express. 2023;9(4):556–70. doi:10.1016/j.icte.2023.03.011.
13. Mahmood A, Ali Siddiqui S, Sheng QZ, Zhang WE, Suzuki H, Ni W. Trust on wheels: towards secure and resource efficient IoV networks. Computing. 2022;104(6):1337–58. doi:10.1007/s00607-021-01040-7.
14. Djahel S, Doolan R, Muntean GM, Murphy J. A communications-oriented perspective on traffic management systems for smart cities: challenges and innovative approaches. IEEE Commun Surv Tutor. 2015;17(1):125–51. doi:10.1109/COMST.2014.2339817.
15. Tang F, Kawamoto Y, Kato N, Liu J. Future intelligent and secure vehicular network toward 6G: machine-learning approaches. Proc IEEE. 2020;108(2):292–307. doi:10.1109/jproc.2019.2954595.

16. Shafique K, Khawaja BA, Sabir F, Qazi S, Mustaqim M. Internet of Things (IoT) for next-generation smart systems: a review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. IEEE Access. 2020;8:23022–40. doi:10.1109/ACCESS.2020.2970118.
17. Madububambachu U, Fatima R, Sherif A, Khalil K. Security and privacy solutions in intelligent transportation systems: a survey. Internet Things. 2025;34(3):101812. doi:10.1016/j.iot.2025.101812.
18. Ahmed SF, Bin Alam MS, Afrin S, Rafa SJ, Taher SB, Kabir M, et al. Toward a secure 5G-enabled Internet of Things: a survey on requirements, privacy, security, challenges, and opportunities. IEEE Access. 2024;12(8):13125–45. doi:10.1109/ACCESS.2024.3352508.
19. Mahmood MR, Matin MA, Sarigiannidis P, Goudos SK. A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era. IEEE Access. 2022;10:87535–62. doi:10.1109/ACCESS.2022.3199689.
20. Saad W, Bennis M, Chen M. A vision of 6G wireless systems: applications, trends, technologies, and open research problems. IEEE Netw. 2020;34(3):134–42. doi:10.1109/MNET.001.1900287.
21. Sumalee A, Ho HW. Smarter and more connected: future intelligent transportation system. IATSS Res. 2018;42(2):67–71. doi:10.1016/j.iatssr.2018.05.005.
22. Hisyam Ng HA, Mahmoodi T. Intelligent traffic engineering for 6G heterogeneous transport networks. Computers. 2024;13(3):74. doi:10.3390/computers13030074.
23. Xu H, Berres A, Yoginath SB, Sorensen H, Nugent PJ, Severino J, et al. Smart mobility in the cloud: enabling real-time situational awareness and cyber-physical control through a digital twin for traffic. IEEE Trans Intell Transp Syst. 2023;24(3):3145–56. doi:10.1109/TITS.2022.3226746.
24. Din IU, Ahmad Awan K, Almogren A. Secure and privacy-preserving trust management system for trustworthy communications in intelligent transportation systems. IEEE Access. 2023;11:65407–17. doi:10.1109/access.2023.3290911.
25. Du J, Jiang C, Wang J, Ren Y, Debbah M. Machine learning for 6G wireless networks: carrying forward enhanced bandwidth, massive access, and ultrareliable/low-latency service. IEEE Veh Technol Mag. 2020;15(4):122–34. doi:10.1109/mvt.2020.3019650.
26. Kim Anh VT. The rise of AI in 6G networks: a comprehensive review of opportunities, challenges, and applications. In: Proceedings of the 2024 International Conference on Advanced Technologies for Communications (ATC); 2024 Oct 17–19; Ho Chi Minh City, Vietnam. p. 333–8. doi:10.1109/atc63255.2024.10908115.
27. Telagam N, Kandasamy N, Manoharan AK, Anandhi P, Atchudan R. Beyond 5G: exploring key enabling technologies, use cases, and future prospects of 6 G communication. Nano Commun Netw. 2025;43(6):100560. doi:10.1016/j.nancom.2024.100560.
28. Adam M, Hammoudeh M, Alrawashdeh R, Alsulaimy B. A survey on security, privacy, trust, and architectural challenges in IoT systems. IEEE Access. 2024;12(4):57128–49. doi:10.1109/access.2024.3382709.
29. Singh A, Satapathy SC, Roy A, Gutub A. AI-based mobile edge computing for IoT: applications, challenges, and future scope. Arab J Sci Eng. 2022;47(8):9801–31. doi:10.1007/s13369-021-06348-2.
30. Alwahedi F, Aldhaheri A, Ferrag MA, Battah A, Tihanyi N. Machine learning techniques for IoT security: current research and future vision with generative AI and large language models. Internet Things Cyber Phys Syst. 2024;4(4):167–85. doi:10.1016/j.iotcps.2023.12.003.
31. Porambage P, Gur G, Osorio DPM, Liyanage M, Gurtov A, Ylianttila M. The roadmap to 6G security and privacy. IEEE Open J Commun Soc. 2021;2:1094–122. doi:10.1109/ojcoms.2021.3078081.
32. Shafik W. Emerging advanced technology-based services scenario for secure 6G smart cities. In: Security paradigms in 6G smart cities and IoT ecosystems navigating the future. Boca Raton, FL, USA: CRC Press; 2025.
33. Sanjalawe Y, Fraihat S, Al-E'Mari S, Abualhaj M, Makhadmeh S, Alzubi E. A review of 6G and AI convergence: enhancing communication networks with artificial intelligence. IEEE Open J Commun Soc. 2025;6(2):2308–55. doi:10.1109/ojcoms.2025.3553302.
34. Idhalama OU, Oredo JO. Exploring the next generation Internet of Things (IoT) requirements and applications: a comprehensive overview. Inf Dev. 2024;32(2):75. doi:10.1177/02666669241267852.

35. Rahman A, Debnath T, Kundu D, Cerasuolo F, Islam MJ, Rahman M, et al. Unlocking the potential of IoT, AI, and blockchain in transforming public and private industries. Cambridge, UK: Cambridge Scholars Publishing; 2024.
36. Kim M, Oh I, Yim K, Sahlabadi M, Shukur Z. Security of 6G-enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies. IEEE Access. 2024;12(3):33972–4001. doi:10.1109/access.2023.3348409.
37. Sun H, Liu Y, Al-Tahmeesschi A, Nag A, Soleimanpour M, Canberk B, et al. Advancing 6G: survey for explainable AI on communications and network slicing. IEEE Open J Commun Soc. 2025;6(177):1372–412. doi:10.1109/ojcoms.2025.3534626.
38. Zhang Z, Xiao Y, Ma Z, Xiao M, Ding Z, Lei X, et al. 6G wireless networks: vision, requirements, architecture, and key technologies. IEEE Veh Technol Mag. 2019;14(3):28–41. doi:10.1109/mvt.2019.2921208.
39. Ijala AD, Thomas S, Oshiga O, Hussein SU, Karataev T, Osanaiye O. A review of vision and challenges of the 6G wireless networks. In: Proceedings of the 2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS); 2021 Jul 15–16; Abuja, Nigeria. p. 1–6. doi:10.1109/icmeas52683.2021.9692366.
40. Jiao L, Shao Y, Sun L, Liu F, Yang S, Ma W, et al. Advanced deep learning models for 6G: overview, opportunities, and challenges. IEEE Access. 2024;12(8):133245–314. doi:10.1109/access.2024.3418900.
41. Ibn-Khedher H, Laroui M, Alfaqawi M, Magnouche A, Moungla H, Afifi H. 6G-edge support of Internet of autonomous vehicles: a survey. Trans Emerg Telecommun Technol. 2024;35(1):e4918. doi:10.1002/ett.4918.
42. Painuly S, Kohli P, Matta P, Sharma S. Advance applications and future challenges of 5G IoT. In: Proceedings of the 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS); 2020 Dec 3–5; Thoothukudi, India. p. 1381–4. doi:10.1109/iciss49785.2020.9316004.
43. Jagatheesaperumal SK, Bibri SE, Huang J, Rajapandian J, Parthiban B. Artificial intelligence of things for smart cities: advanced solutions for enhancing transportation safety. Comput Urban Sci. 2024;4(1):10. doi:10.1007/s43762-024-00120-6.
44. Ma Y, Wang C, Fu T, Meng Z. The analysis of acquisition system for electronic traffic signal in smart cities based on the Internet of Things. Sci Rep. 2025;15(1):20628. doi:10.1038/s41598-025-07423-6.
45. Gad AR, Nashat AA, Barkat TM. Intrusion detection system using machine learning for vehicular *ad hoc* networks based on ToN-IoT dataset. IEEE Access. 2021;9:142206–17. doi:10.1109/access.2021.3120626.
46. Ferrag MA, Debbah M, Al-Hawawreh M. Generative AI for cyber threat-hunting in 6G-enabled IoT networks. In: Proceedings of the 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW); 2023 May 1–4; Bangalore, India. p. 16–25. doi:10.1109/ccgridw59191.2023.00018.
47. Yang X, Shu L, Liu Y, Hancke GP, Ferrag MA, Huang K. Physical security and safety of IoT equipment: a survey of recent advances and opportunities. IEEE Trans Ind Inf. 2022;18(7):4319–30. doi:10.1109/tii.2022.3141408.
48. Stergiou CL, Psannis KE, Gupta BB. IoT-based big data secure management in the fog over a 6G wireless network. IEEE Internet Things J. 2021;8(7):5164–71. doi:10.1109/jiot.2020.3033131.
49. Bergies S, Aljohani TM, Su SF, Elsisi M. An IoT-based deep-learning architecture to secure automated electric vehicles against cyberattacks and data loss. IEEE Trans Syst Man Cybern Syst. 2024;54(9):5717–32. doi:10.1109/tsmc.2024.3409314.
50. Moya Osorio DP, Ahmad I, Sánchez JDV, Gurtov A, Scholliers J, Kutila M, et al. Towards 6G-enabled Internet of vehicles: security and privacy. IEEE Open J Commun Soc. 2022;3(4):82–105. doi:10.1109/ojcoms.2022.3143098.
51. Munir A, Blasch E, Kwon J, Kong J, Aved A. Artificial intelligence and data fusion at the edge. IEEE Aerosp Electron Syst Mag. 2021;36(7):62–78. doi:10.1109/maes.2020.3043072.
52. Yang L, Li Y, Yang SX, Lu Y, Guo T, Yu K. Generative adversarial learning for intelligent trust management in 6G wireless networks. IEEE Netw. 2022;36(4):134–40. doi:10.1109/mnet.003.2100672.
53. Khalid W, Rehman MAU, Van Chien T, Kaleem Z, Lee H, Yu H. Reconfigurable intelligent surface for physical layer security in 6G-IoT: designs, issues, and advances. IEEE Internet Things J. 2024;11(2):3599–613. doi:10.1109/JIOT.2023.3297241.
54. Kavaiya S, Patel DK. Restricting passive attacks in 6G vehicular networks: a physical layer security perspective. Wireless Netw. 2023;29(3):1355–65. doi:10.1007/s11276-022-03189-1.

55. Son S, Kim M, Park Y. A lightweight seamless authentication scheme for edge-assisted IoV networks. In: Proceedings of the 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN); 2023 Jul 4–7; Paris, France. p. 305–10. doi:10.1109/ICUFN57995.2023.10200823.
56. Ramezanpour K, Jagannath J. Intelligent zero trust architecture for 5G/6G networks: principles, challenges, and the role of machine learning in the context of O-RAN. Comput Netw. 2022;217(2):109358. doi:10.1016/j.comnet.2022.109358.
57. Wang S, Qureshi MA, Miralles-Pechuán L, Huynh-The T, Gadekallu TR, Liyanage M. Explainable AI for 6G use cases: technical aspects and research challenges. IEEE Open J Commun Soc. 2024;5(2):2490–540. doi:10.1109/ojcoms.2024.3386872.
58. Yuan X, Chen J, Yang J, Zhang N, Yang T, Han T, et al. FedSTN: graph representation driven federated learning for edge computing enabled urban traffic flow prediction. IEEE Trans Intell Transp Syst. 2023;24(8):8738–48. doi:10.1109/TITS.2022.3157056.
59. Imoize AL, Adedeji O, Tandiya N, Shetty S. 6G enabled smart infrastructure for sustainable society: opportunities, challenges, and research roadmap. Sensors. 2021;21(5):1709. doi:10.3390/s21051709.
60. Garai M, Sliti M, Mrabet M, Ben Ammar L. AI-enabled vehicular data offloading for sustainable smart cities: taxonomy, KPI models, and open challenges. IEEE Access. 2026;14(16):1468–92. doi:10.1109/ACCESS.2025.3648539.
61. Chu T, Wang J, Codeca L, Li Z. Multi-agent deep reinforcement learning for large-scale traffic signal control. IEEE Trans Intell Transport Syst. 2020;21(3):1086–95. doi:10.1109/tits.2019.2901791.
62. Roy C, Saha R, Misra S, Dev K. Micro-safe: microservices- and deep learning-based safety-as-a-service architecture for 6G-enabled intelligent transportation system. IEEE Trans Intell Transp Syst. 2022;23(7):9765–74. doi:10.1109/TITS.2021.3110725.
63. Liang L, Ye H, Yu G, Li GY. Deep-learning-based wireless resource allocation with application to vehicular networks. Proc IEEE. 2020;108(2):341–56. doi:10.1109/jproc.2019.2957798.
64. Hijji M, Iqbal R, Kumar Pandey A, Doctor F, Karyotis C, Rajeh W, et al. 6G connected vehicle framework to support intelligent road maintenance using deep learning data fusion. IEEE Trans Intell Transp Syst. 2023;24(7):7726–35. doi:10.1109/TITS.2023.3235151.
65. Li P, Zhong Y, Zhang C, Wu Y, Yu R. FedRelay: federated relay learning for 6G mobile edge intelligence. IEEE Trans Veh Technol. 2023;72(4):5125–38. doi:10.1109/tvt.2022.3225087.
66. Wu W, Zhou C, Li M, Wu H, Zhou H, Zhang N, et al. AI-native network slicing for 6G networks. IEEE Wirel Commun. 2022;29(1):96–103. doi:10.1109/mwc.001.2100338.
67. Kumar N, Mittal S, Garg V, Kumar N. Deep reinforcement learning-based traffic light scheduling framework for SDN-enabled smart transportation system. IEEE Trans Intell Transp Syst. 2022;23(3):2411–21. doi:10.1109/TITS.2021.3095161.
68. Salh A, Audah L, Shah NSM, Alhammadi A, Abdullah Q, Kim YH, et al. A survey on deep learning for ultra-reliable and low-latency communications challenges on 6G wireless systems. IEEE Access. 2021;9:55098–131. doi:10.1109/ACCESS.2021.3069707.
69. Arana-Catania M, Sonee A, Khan AM, Fatehi K, Tang Y, Jin B, et al. Explainable reinforcement and causal learning for improving trust to 6G stakeholders. IEEE Open J Commun Soc. 2025;6(6):4101–25. doi:10.1109/OJCOMS.2025.3563415.
70. Yan K, Ma W, Yang Q, Sun S, Wang W. Info-chain: reputation-based blockchain for secure information sharing in 6G intelligent transportation systems. IEEE Internet Things J. 2024;11(5):9198–212. doi:10.1109/JIOT.2023.3323011.
71. Kumar R, Gupta SK, Wang HC, Kumari CS, Korlam SSVP. From efficiency to sustainability: exploring the potential of 6G for a greener future. Sustainability. 2023;15(23):16387. doi:10.3390/su152316387.
72. Adhikari M, Hazra A, Menon VG, Chaurasia BK, Mumtaz S. A roadmap of next-generation wireless technology for 6G-enabled vehicular networks. IEEE Internet Things Mag. 2021;4(4):79–85. doi:10.1109/iotm.001.2100075.
73. Vijayakumar P, Azees M, Kozlov SA, Rodrigues JJPC. An anonymous batch authentication and key exchange protocols for 6G enabled VANETs. IEEE Trans Intell Transport Syst. 2022;23(2):1630–8. doi:10.1109/tits.2021.3099488.

74. Ahmed M, Moustafa N, Akhter AFMS, Razzak I, Surid E, Anwar A, et al. A blockchain-based emergency message transmission protocol for cooperative VANET. IEEE Trans Intell Transport Syst. 2022;23(10):19624–33. doi:10.1109/tits.2021.3115245.
75. Wei L, Cui J, Xu Y, Cheng J, Zhong H. Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs. IEEE Trans Inf Forensics Secur. 2021;16:1681–95. doi:10.1109/TIFS.2020.3040876.
76. Jiang W, Han B, Habibi MA, Schotten HD. The road towards 6G: a comprehensive survey. IEEE Open J Commun Soc. 2021;2:334–66. doi:10.1109/ojcoms.2021.3057679.
77. Liu R, Lin H, Lee H, Chaves F, Lim H, Sköld J. Beginning of the journey toward 6G: vision and framework. IEEE Commun Mag. 2023;61(10):8–9. doi:10.1109/mcom.2023.10298069.
78. Serôdio C, Cunha J, Candela G, Rodriguez S, Sousa XR, Branco F. The 6G ecosystem as support for IoE and private networks: vision, requirements, and challenges. Future Internet. 2023;15(11):348. doi:10.3390/fi15110348.
79. Deng X, Wang L, Gui J, Jiang P, Chen X, Zeng F, et al. A review of 6G autonomous intelligent transportation systems: mechanisms, applications and challenges. J Syst Archit. 2023;142(3):102929. doi:10.1016/j.sysarc.2023.102929.
80. Aktas F, Shayea I, Ergen M, Aldasheva L, Saoud B, Tussupov A, et al. Routing challenges and enabling technologies for 6G-satellite network integration: toward seamless global connectivity. Technologies. 2025;13(6):245. doi:10.3390/technologies13060245.
81. Gong T, Zhu L, Yu FR, Tang T. Edge intelligence in intelligent transportation systems: a survey. IEEE Trans Intell Transport Syst. 2023;24(9):8919–44. doi:10.1109/tits.2023.3275741.
82. Othman WM, Ateya AA, Nasr ME, Muthanna A, ElAffendi M, Koucheryavy A, et al. Key enabling technologies for 6G: the role of UAVs, terahertz communication, and intelligent reconfigurable surfaces in shaping the future of wireless networks. J Sens Actuator Netw. 2025;14(2):30. doi:10.3390/jsan14020030.
83. Zhang S, Li J, Shi L, Ding M, Nguyen DC, Tan W, et al. Federated learning in intelligent transportation systems: recent applications and open problems. IEEE Trans Intell Transp Syst. 2024;25(5):3259–85. doi:10.1109/TITS.2023.3324962.
84. Akhter AFMS, Arnob TZ, Noor EB, Hizal S, Pathan AK. An edge-supported blockchain-based secure authentication method and a cryptocurrency-based billing system for P2P charging of electric vehicles. Entropy. 2022;24(11):1644. doi:10.3390/e24111644.
85. AlHousrya O, Bennagi A, Cotfas PA, Cotfas DT. The role of the industrial IoT in advancing electric vehicle technology: a review. Appl Sci. 2025;15(17):9290. doi:10.3390/app15179290.
86. Kumar R, Dutta J, Vamsi N, Sankararao Varri U, Puthal D. Next-generation security in the 6G era: the role of AI in safeguarding future networks. IEEE Access. 2026;14(7):17347–80. doi:10.1109/ACCESS.2025.3650208.
87. Kadam S, Kim DI. IoT-enabled traffic management system using vehicle count prediction in a semantic communication framework. IEEE Internet Things J. 2025;12(17):36258–73. doi:10.1109/JIOT.2025.3581778.
88. Telikani A, Sarkar A, Du B, Santoso F, Shen J, Yan J, et al. Autonomous aerial vehicles-aided intelligent transportation systems: vision, challenges, and opportunities. IEEE Commun Surv Tutor. 2025;27(6):3772–819. doi:10.1109/COMST.2025.3530913.
89. Abdullahi AD, Bahrami E, Dargahi T, Al-Khalidi M, Hammoudeh M. Interplay between security, privacy and trust in 6G-enabled intelligent transportation systems. IEEE Open J Intell Transp Syst. 2025;6(1):1625–54. doi:10.1109/OJITS.2025.3637333.
90. Tahir HA, Alayed W, Hassan WU. Privacy-preserving federated learning with adaptive model aggregation for efficient vehicle-to-vehicle (V2V) communication in intelligent transportation systems. IEEE Access. 2025;13:182393–409. doi:10.1109/ACCESS.2025.3618999.
91. Soni M, Singh DK. Blockchain-based group authentication scheme for 6G communication network. Phys Commun. 2023;57(3):102005. doi:10.1016/j.phycom.2023.102005.
92. Tataria H, Shafi M, Molisch AF, Dohler M, Sjöland H, Tufvesson F. 6G wireless systems: vision, requirements, challenges, insights, and opportunities. Proc IEEE. 2021;109(7):1166–99. doi:10.1109/jproc.2021.3061701.
93. Pan G, Gao Y, Gao Y, Yu W, Zhong Z, Yang X, et al. AI-driven wireless positioning: fundamentals, standards, state-of-the-art, and challenges. IEEE Commun Surv Tutor. 2026;28:4394–428. doi:10.1109/COMST.2025.3648577.

94. Chataut R, Nankya M, Akl R. 6G networks and the AI revolution-exploring technologies, applications, and emerging challenges. Sensors. 2024;24(6):1888. doi:10.3390/s24061888.
95. Sharma S, Popli R, Singh S, Chhabra G, Saini GS, Singh M, et al. The role of 6G technologies in advancing smart city applications: opportunities and challenges. Sustainability. 2024;16(16):7039. doi:10.3390/su16167039.
96. Dang S, Amin O, Shihada B, Alouini MS. What should 6G be? Nat Electron. 2020;3(1):20–9. doi:10.1038/s41928-019-0355-6.
97. Zhang L, Liang YC, Niyato D. 6G Visions: mobile ultra-broadband, super Internet-of-Things, and artificial intelligence. China Commun. 2019;16(8):1–14. doi:10.23919/jcc.2019.08.001.
98. Al Amin A, Hong J, Bui VH, Su W. Emerging 6G/B6G wireless communication for the power infrastructure in smart cities: innovations, challenges, and future perspectives. Algorithms. 2023;16(10):474. doi:10.3390/a16100474.
99. Manogaran G, Baabdullah T, Rawat DB, Shakeel PM. AI-assisted service virtualization and flow management framework for 6G-enabled cloud-software-defined network-based IoT. IEEE Internet Things J. 2022;9(16):14644–54. doi:10.1109/JIOT.2021.3077895.
100. Ma T, Qian B, Qin X, Liu X, Zhou H, Zhao L. Satellite-terrestrial integrated 6G: an ultra-dense LEO networking management architecture. IEEE Wirel Commun. 2022;31(1):62–9.
101. Song W, Rajak S, Dang S, Liu R, Li J, Chinnadurai S. Deep learning enabled IRS for 6G intelligent transportation systems: a comprehensive study. IEEE Trans Intell Transport Syst. 2023;24(11):12973–90. doi:10.1109/tits.2022.3184314.
102. Eze E, Eze J. Artificial intelligence support for 5G/6G-enabled Internet of Vehicles networks: an overview. ITU J Future Evol Technol. 2023;4(1):178–95. doi:10.52953/iezn8770.
103. Shehzad MK, Rose L, Butt MM, Kovacs IZ, Assaad M, Guizani M. Artificial intelligence for 6G networks: technology advancement and standardization. IEEE Veh Technol Mag. 2022;17(3):16–25. doi:10.1109/mvt.2022.3164758.
104. de Alwis C, Pham QV, Liyanage M. 6G frontiers: towards future wireless systems. Hoboken, NJ, USA: John Wiley & Sons, Inc.; 2022. doi:10.1002/9781119862321.
105. Qadir Z, Le KN, Saeed N, Munawar HS. Towards 6G Internet of Things: recent advances, use cases, and open challenges. ICT Express. 2023;9(3):296–312. doi:10.1016/j.icte.2022.06.006.
106. Alsabah M, Naser MA, Mahmmod BM, Abdulhussain SH, Eissa MR, Al-Baidhani A, et al. 6G wireless communications networks: a comprehensive survey. IEEE Access. 2021;9:148191–243. doi:10.1109/ACCESS.2021.3124812.
107. Noor-A-Rahim M, Liu Z, Lee H, Khyam MO, He J, Pesch D, et al. 6G for vehicle-to-everything (V2X) communications: enabling technologies, challenges, and opportunities. Proc IEEE. 2022;110(6):712–34. doi:10.1109/JPROC.2022.3173031.
108. Chakrabarti K. Deep learning based offloading for mobile augmented reality application in 6G. Comput Electr Eng. 2021;95(2):107381. doi:10.1016/j.compeleceng.2021.107381.
109. Rafique S, Iqbal S, Ali D, Khan F. Navigating ethical challenges in 6G-enabled smart cities: privacy, equity, and governance. ICCK Trans Sens Commun Control. 2025;2(1):48–65. doi:10.62762/tscc.2025.291581.
110. Mollajafari S, Bechkoum K. Blockchain technology and related security risks: towards a seven-layer perspective and taxonomy. Sustainability. 2023;15(18):13401. doi:10.3390/su151813401.
111. Laña I, Sanchez-Medina JJ, Vlahogianni EI, Del Ser J. From data to actions in intelligent transportation systems: a prescription of functional requirements for model actionability. Sensors. 2021;21(4):1121. doi:10.3390/s21041121.