GAS Journal of Engineering and Technology (GASJET)

Volume 3 | Issue 1, 2026 Homepage: https://gaspublishers.com/gasjet-home/ ISSN: 3048-5800

Security and Privacy Issues of Intelligent Transportation System

Mohammed Ahmed Abdullah Al-Anzi

Prince Sattam bin Abdulaziz University

Received: *10.01.2026* | ***Accepted:*** *24.01.2026* | ***Published:*** *27.01.2026*

***Corresponding Author:** Mohammed Ahmed Abdullah Al-Anzi

DOI: *10.5281/zenodo.18384622*

Abstract **Original Research Article**

Intelligent Transportation Systems (ITS) represent a critical integration of information, communication, and sensor technologies into transportation infrastructure, aimed at enhancing safety, efficiency, and sustainability. However, the increasing connectivity and data exchange inherent in ITS introduce significant cybersecurity vulnerabilities and privacy concerns. This paper provides a comprehensive review of security and privacy challenges within ITS, examining potential attack vectors such as wireless exploitation, sensor vulnerabilities, and software exploits, alongside risks related to user data collection, location tracking, and profiling. Through case studies and forward-looking scenarios, the paper highlights real-world implications of security breaches and privacy violations. Furthermore, it explores innovative mitigation strategies, including embedded cybersecurity roles, crowdsourced vulnerability detection, and privacy-by-design principles. The analysis concludes with an examination of emerging technologies such as blockchain and autonomous cyber-agents, as well as the essential role of regulatory frameworks and public awareness in safeguarding ITS. Ultimately, this review underscores the necessity of robust, multi-layered security and privacy measures to ensure the resilience, trustworthiness, and societal acceptance of intelligent transportation ecosystems.

Keywords: Intelligent Transportation Systems (ITS), Cybersecurity, Data Privacy, Vehicular Networks, Secure Infrastructure.

Copyright © 2026 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

1. Introduction

Intelligent transportation systems (ITS) refer to the application of computing, information, and communication technologies to enhance transportation infrastructure and operations. ITS integrates advanced technologies like sensors, data analytics, and wireless communications into vehicles, roads, traffic signals, transit systems, and other transportation components and services. The ultimate goals are to improve safety, mobility, efficiency, and sustainability across all modes of travel.

The origins of ITS can be traced back to the 1960s research into road-vehicle communication systems and efforts to develop technologies like ramp metering, variable traffic signals, and electronic toll collection. However, ITS emerged as a concerted initiative in the late 1980s and early 1990s as advances in computing, telecommunications, and sensor technologies enabled more sophisticated and integrated transportation management capabilities.

In 1991, the Intermodal Surface Transportation Efficiency Act in the United States formally created

the Intelligent Transportation Systems program to coordinate the development and deployment of ITS technologies across the country. Similar national ITS initiatives followed in other countries and regions like Japan, Europe, and Singapore through the 1990s and 2000s. The recent proliferation of connected vehicle technologies, smartphones, cloud computing, and artificial intelligence has ushered in new ITS applications like ride-sharing, smart parking, autonomous trucks, and predictive traffic management.

While providing significant benefits, the increasing connectivity, automation, and data sharing involved in ITS introduces new cybersecurity vulnerabilities related to potential hacking of vehicles or infrastructure as well as threats to user privacy. As ITS becomes more pervasive, proactively addressing these security and privacy challenges is crucial for maintaining safety, operational resilience, and public acceptance of intelligent transportation technologies and services.

2. Background and Related Work

Intelligent transportation systems (ITS) integrate advanced information, communication, sensor and control technologies into transportation infrastructure and services. Key ITS applications include traffic management, transit operations, emergency response, traveler information systems and automated/autonomous vehicles (Ami et al., 2011).

As ITS becomes more ubiquitous and interconnected, cybersecurity vulnerabilities arise that could be exploited to disrupt transportation networks or access sensitive data (Lyu et al., 2019). Potential attack vectors include hacking into digital components like traffic signal controllers (Ghena et al., 2014), compromising vehicle communications like DSRC safety messages (Petit &Shladover, 2015), intercepting wireless transmissions from onboard sensors/ECUs (Hoppe et al., 2008), and exploiting software vulnerabilities.

User privacy is also a major concern as ITS technologies collect and share increasing amounts of location data, travel patterns, and other personal information (Cottrill, 2020). Vehicle probing data from smartphones/navigation apps and automated data recording from connected cars create risk of unauthorized surveillance or monetization of user data (Gerlach et al., 2017).

Key research areas include developing secure vehicle-to-everything (V2X) communication protocols (Maniatis et al., 2021), implementing robust cryptography and access controls in ITS devices/infrastructure (Deljoo et al., 2018), designing privacy-preserving data sharing frameworks (Asuquo et al., 2018), and implementing security lifecycle processes for ITS technologies (Lorgat et al., 2021).

3. ITS Architecture and Components

Intelligent transportation systems consist of an integrated framework of complementary components and subsystems working together to enable advanced transportation capabilities. The National ITS Architecture in the United States provides a common framework for planning, defining, and integrating ITS (Mullin et al., 2022).

The main components and subsystems include (Dimitrakopoulos&Demestichas, 2010):

- Vehicles - Equipped with onboard sensors, computers, wireless communications, and potentially automation capabilities for functions like collision avoidance, navigation, platooning.
- Travelers - Personal devices like smartphones providing travel information, navigation, reservation and payment services.
- Centers - Management centers for functions like traffic management, transit operations, emergency response, data collection/fusion.
- Field Equipment - Roadside equipment like cameras, traffic signals, sensors, dynamic message signs providing monitoring and control.

These components interconnect via wired and wireless networks utilizing dedicated short-range communications (DSRC), cellular, WiFi, and other standardized protocols to share real-time data.

Key enabling technologies include (Bagheri et al., 2020):

- Global Navigation Satellite Systems (GNSS) for positioning
- Sensors like radar, lidar, cameras for perception
- Vehicular ad-hoc networks (VANETs) for V2X communications
- Computing hardware/platforms for data processing
- Artificial intelligence/machine learning for optimization

Major ITS applications span areas like advanced traffic management, advanced traveler information, commercial vehicle operations, public transportation management, electronic payment services, and emerging vehicle-to-everything (V2X) capabilities (Bagheri et al., 2020).

4. Security Challenges in ITS

While offering many benefits, the increasing connectivity, automation, and data sharing involved in ITS also introduces a range of potential cybersecurity threats and vulnerabilities that must be addressed:

- Wireless Attacks - ITS rely heavily on various wireless communication technologies (DSRC, cellular, WiFi) that are susceptible to jamming, eavesdropping, spoofing, and other wireless attacks (Asuquo et al., 2018). Adversaries could potentially intercept safety-critical messages.
- Sensor Vulnerability - Connected vehicles utilize various onboard sensors (cameras, lidar, radar) that may have security flaws allowing sensor data to be spoofed or corrupted, impacting perception capabilities (Parkinson et al., 2017).
- Software/Firmware Exploits - ITS components like vehicles, traffic controllers, roadside units run complex software/firmware that may contain vulnerabilities enabling malicious code injection or control (Leng&Nitz, 2019).
- Physical Attacks - ITS infrastructure like sensors, controllers, networking gear situated along roads present physical attack surfaces that could be tampered with if not properly secured (Qudrat et al., 2021).
- Insider Threats - Insiders with access to ITS backend systems, databases, and maintenance operations pose risks for theft/abuse of data or systems (Dorri et al., 2017).
- Unintended Behavior - Even without malicious intent, design flaws or functional glitches in ITS systems create potential for hazardous unintended behaviors that impact safety (Zheng et al., 2019).
- Scalability/Heterogeneity - ITS involves diverse components that must securely integrate across modes/jurisdictions. Security mechanisms must scale and adapt to this heterogeneity (Leng&Nitz, 2019).

5. Privacy Concerns in ITS

In addition to cybersecurity risks, the increasing collection and sharing of data by ITS technologies also raises significant privacy concerns for individual users:

- Location Tracking - ITS applications like navigation apps, traffic monitoring, electronic tolling, etc. can enable detailed tracking of a person's location and movements over time (Balocco et al., 2016). This poses risks related to unauthorized surveillance.
- User Profiling - Combining location data with other information like payment details, contact lists, online activity, etc. allows building detailed profiles about individuals' habits, interests, associates and more (Krauss et al., 2020).
- Data Monetization - There are business incentives for commercialization and unauthorized secondary uses of ITS user data by data brokers, advertisers, and other third parties (Rao et al., 2019).
- Lack of Anonymity - Technologies like automated license plate recognition, vehicular networks identifying specific vehicles, facial recognition systems etc. can

associate data to known individuals (Lefrancois&Lefèvre, 2017).Consent/Control - Users may have limited ability to know what data is collected about them, how it is used/shared, and exercise control over their personal data in ITS contexts (Milutinovic et al., 2016).While data sharing is required for many ITS capabilities, preserving privacy through anonymization, consent frameworks, access controls and other technical/policy measures is essential for public acceptance.

6. Case Studies of Security and Privacy Breaches

6.1.The Phantom Traffic Pileup

It was just another sunny Friday morning in the city when suddenly all hell broke loose on the highways. Traffic ground to a halt as cars slammed on brakes and backed up for miles in every direction. Except there was no accident - no disabled vehicles, no debris in the road. It was all caused by hackers who infiltrated the city's traffic management system and falsified the data flows.

By feeding fake traffic and incident data into the system, they created the illusion of a massive pileup on every major artery. This triggered hundreds of traffic signals to turn red, highway signs to warn of obstructions, and navigation apps to re-route vehicles. Chaos reigned for hours before authorities could regain control. The perpetrators were never caught, but the attack demonstrated how fundamental ITS is to keeping a city moving.

6.2.The Automotive Spy Syndicate

For years, a sophisticated international criminal organization ran an audacious privacy-exploting racket made possible by connected vehicle technologies. They hacked into multiple automakers' vehicle communications systems and databases to covertly access tons of driver data.

Using machine learning, they created detailed behavior profiles analyzing people's driving habits, common destinations, travel routines, in-vehicle conversations, and more. They sold this invaluable intel to anyone willing to pay - private investigators, corporate espionage firms, even hostile nation-states. Celebrities, politicians, business executives - no one's privacy was safe from these vehicular voyeurs until an insider finally leaked the scheme.

6.3.The Highway Hostage Crisis

An act of cyberterrorism brought a metropolitan area's transportation network to its knees one historic day. Hackers breached security vulnerabilities in roadway sensors and traffic signal controllers to seize complete control of traffic flows.

They caused signals to go haywire, remotely raising gates and closing tunnels to trap vehicles on highways. Private data from navigation systems and automated car systems allowed them to target and immobilize specific vehicles as well. Holding the entire city's mobility hostage, the hackers issued demands for untold sums of cryptocurrency before finally being paid off to release their control hours later. The event underscored how desperately ITS cybersecurity needs to be shored up.

Those are just a few fictional examples, but I tried to illustrate through imaginative storytelling how various security and privacy risks could potentially play out in real-world ITS breach scenarios. The continuously evolving cyber-physical nature of intelligent transportation means proactively guarding against such incidents is crucial.

7. Innovative Strategies and Solutions

7.1.The Cyber Transportation Marshals

With cybersecurity threats intensifying, transportation agencies began embedding cyber first responders directly into ITS operations centers. These "cyber marshals" acted as round-the-clock roadies, vigilantly monitoring networks for any anomalies and ready to swing into incident response mode at the first sign of trouble.

Leveraging AI analytics tuned to detect even the faintest hints of malicious activity, the marshals could swiftly isolate and neutralize threats before they could propagate through interconnected systems. Their advanced training and cloud-based threat intelligence gave them the knowledge to stay ahead of devious hackers.

Deploying these cyber guardians onto the digital highways brought much-needed resilience, ensuring ITS could recover rapidly when attacks inevitably occurred. The marshals' physical presence also reinforced a culture of cybersecurity awareness and vigilance across the entire workforce.

7.2.The Vehicle Vulnerability Bug Hunters

To get ahead of potential cyber exploits targeting the multitude of software and components in modern vehicles, automakers turned to an innovative crowdsourced security model. Dubbed the "bug hunters," this elite global community of white hat hackers got behind-the-scenes access to companies' codebases, development processes, even prototype vehicles.

Their mission? Relentlessly probe for vulnerabilities, software flaws or design lapses that could open vehicles up to remote cyber hijackings before the bad guys found them first. Bug hunters who discovered and responsibly reported valid issues earned bounties sometimes totaling millions for the most critical finds.

This proactive vulnerability disclosure program helped automakers drastically shrink their exposure windows by getting a head start patching weaknesses. The initiative cultivated constructive relationships between manufacturers and the hacker community while fostering greater transparency. For the hunters, it provided a legal, lucrative avenue to use their skills ethically.

7.3.The Privacy By-Design Architects

As ITS user privacy threats escalated from theoretical to concrete, a new discipline emerged focused on data privacy protections. Chief Privacy Engineers were hired to ensure every system, product, and service baked in privacy from the initial architecture and design phases using cutting-edge techniques.

Deidentification, pseudonymization, differential privacy algorithms - the CPEs wielded a potent toolkit to anonymize and obfuscate personal data flows. They implemented leading encryption, access controls, and authentication mechanisms to lock down information. Analytics and data sharing pipelines were constructed with privacy filters and firewalls.

Rather than unwieldy compliance exercises, CPEs took a holistic approach making privacy a core part of an organization's processes, training, and mindset. Their overarching "privacy by-design" principles future-proofed systems for emerging regulations while fostering trustworthiness and user confidence. Most importantly, their work allowed ITS to deliver transformative mobility solutions while steadfastly upholding individual privacy rights.

I tried to illustrate some innovative strategies to address ITS security and privacy challenges in a more imaginative, storytelling style versus a dry technical breakdown. The goal was to spark thinking around new roles, methods and priorities that could be adopted to stay ahead of evolving risks. Let me know if you would like me to elaborate on any of these concepts further.

8. Future Directions and Emerging Technologies

8.1.The Blockchain Mobility Ledger

In the cities of the future, every vehicle's movement, communication, and transaction is recorded as an immutable entry in a decentralized blockchain repository known as the Mobility Ledger. This unified ledger provides an auditable, cryptographically secured master record of all transportation activity across modes.

Each block represents a specific vehicle or infrastructure component, containing data detailing its identity, status, location, actions and interactions at any given point in time. Cutting-edge blockchain protocols and consensus mechanisms ensure this comprehensive mobility database remains inviolable and tamper-proof.

For users, the Ledger facilitates secure mobility credential and payment management while privacy-preserving cryptography techniques obfuscate personal details. Transportation providers tap into its data troves to optimize operational efficiency while upholding data integrity and system resilience. Regulatory oversight is simplified through transparent monitoring.

Rather than today's labyrinth of fragmented, vulnerable information silos, the Mobility Ledger establishes an authoritative distributed record strengthened by mass decentralization. Its unparalleled security, transparency and availability ushers in a new era of trusted, unified transportation intelligence.

8.2.The Cybercities Traffic Guardians

To protect modern cities' highly interdependent, hyperconnected transportation cyberinfrastructures, a new class of intelligent autonomous cybersecurity agents was developed - the Cyberbiotics. Part AI software robot, part physical drone, these guardian sentries continuously patrol ITS networks and infrastructure looking for anomalies.Swarming as coordinated decentralized nodes, Cyberbiotics agents leverage advanced machine learning to detect and neutralize cyber threats in real-time. Their software virtualized essences can rapidly disperse to quarantine infected systems and repair code vulnerabilities. When required, their drone embodiments can physically airlift into equipment terminals, using specialized tools to override controls or repair damage.Cybercities agents operate under Asimov-inspired prime cyberdirectives - to proactively defend ITS assets from compromise at all costs while never causing harm. Their tireless, ethically-constrained vigilance provides a last impenetrable line of active automated defense for mobility networks of the future.

8.3.Trans light privacy filtering relays

Even as smart transportation technologies become more indispensable in our hyper-connected world, preserving individual privacy remains paramount. This challenge is addressed through the development of Translight - an intelligent anonymous routing and privacy filtering protocol enabling personal mobility while preventing data leakage.

When users travel through the integrated Translight relay network, their identity and attributes are cloaked via cutting-edge cryptographic privacy techniques. Personal signals are disassociated across multiple dynamic routing nodes, preventing any single point from piecing together individual trip trajectories. Differential privacy algorithms sanitize data flows to remove identifying details.

Yet certified transportation providers and services can still securely interface with the network to validate credentials, collect payments, and deliver authorized mobility assistance when required. The zero-knowledge proofs and selective disclosure capabilities of Translight balance privacy with functionality.

From autonomous car sharing to efficient traffic management, Translight empowers a new generation of applications by unlocking access to previously anonymized personal mobility data streams. Its widespread adoption allows society to ethically harness the power of intelligent transportation while preserving treasured individual privacy rights.

I tried to envision some potential future technologies and paradigms that could emerge to bolster ITS security and privacy through imaginative, creative narratives rather than dry technical descriptions. Themes I aimed for included decentralization, autonomous intelligent agents, privacy-preserving encryption/filtering, and finding innovative ways to balance data utility with privacy rights as ITS becomes more ubiquitous.

9. Challenges facing smart security systems

9.1.The Mimic Men

As artificial intelligence capabilities advanced, a new breed of threat emerged - the Mimic Men. These were hackers who could digitally imprint and impersonate anyone's identity, allowing them to sublimely bypass even the most advanced biometric authentication systems.

Using deepfake audiovisual reconstruction combined with digital fingerprint and retinal forgery, the Mimic Men could perfectly replicate how you looked, sounded, and passed all biological verification checks. Their mal-AI could even analyze time-series data to forecast precise behaviors and speech patterns, never breaking character.

This made the Mimic Men utterly undetectable by smart security systems that relied solely on identifying authentic human traits. Once they infiltrated networks in digital masquerade, their

polymorphic malware could shape-shift to avoid traditional threat signatures as well. Only advanced behavioral analysis heuristics applying multi-modal bayesian reasoning had a chance at unmasking their eerie human camouflage.

9.2.The Metadata Psychographers

Even with encrypted data being the norm, skilled analysts known as metadata psychographers proved they could potentially undermine systems by reverse-engineering amazingly accurate psychological profiles based just on anonymized metadata patterns.

By applying exotic mathematical techniques like geometric deep learning and temporal network mapping to seemingly innocuous signals like location pings, traffic patterns, and time/duration stamps, the psychographers unveiled startling insights into people's behaviors, routines, personalities and relationships.It allowed them to reconstruct remarkably specific psychological composites - from predicting where individuals would be at any given time based on habits, to anticipating their subjective mindsets and likely responses in scenarios. In the wrong hands, these psychographic targeting vectors represented a massive risk to smart systems relying solely on traditional privacy protection measures like data anonymization.

9.3.The Seamless Deepforgers

As virtual and physical realities blurred through the advent of photorealistic augmented environments, a new cyberthreat emerged from deepforgers - hackers able to convincingly inject malicious synthetic data directly into the augmented data streams overlaying smart security systems.By learning and modeling the real-time sensor and rendering pipelines used to manifest virtual details over physical spaces, the deepforgers found insidious ways to manipulate what you visually perceived. They could seamlessly underlay hidden signals and forgeries undetected, making you see illusions of their choosing mixed within the actual surroundings.

This allowed them to subtly spoof targets with hyper-realistic deepfakes customized for each individual or environs. Deepforgers could bypass system authentication checks by forging perceived "legitimate" credentials. Or trigger social engineering attacks by manifesting phantoms designed to mislead and manipulate. Defending against cloaked attacks woven into digitally augmenting our sensory reality stream proved enormously complex.I tried to depict some imaginative, creative scenarios around future challenges smart security systems may face as technologies like deepfakes, AI, augmented reality and more continue advancing.

10. The importance of providing security and privacy in the intelligent transportation system:

10.1. The Unseeing Eye

Imagine a world where your daily travels were scrutinized by an ever-present Unseeing Eye - a formidable surveillance intelligence that cataloged every movement, errand, rendezvous and detour you made across the city's sprawling mobility network. This unblinking watcher used persistent tracking and data profiting to compile shockingly intimate digitized dossiers on your life.

From the morning rideshare it detected you calling, to the self-driving electric car renting patterns suggesting you were having an affair, to the freight drone dropping off packages at atherapis clinic - nothing escaped the Unseeing Eye's remorseless algorithmic gaze. It cross-referenced endless mobility datasets to make cooly analytical yet terrifyingly accurate predictions about your habits, beliefs, relationships, indiscretions.

In this disquieting surveillance state, the smart transportation grid meant to revolutionize urban mobility with hyper-efficiency became a prison of ceaseless monitoring from which there was no escape. What restaurant you visited, what parking lots you idled in, what neighborhoods you avoided or frequented - all were pixels feeding the hungry Unseeing Eye's insatiable appetites.

Without robust privacy safeguards and uncompromising security measures enforcing true data anonymity across intelligent transportation networks, such an omniscient electronic panopticon

remained a perpetual risk. The sanctity and freedom of personal mobility would be forever compromised, impacts reverberating across all aspects of society. This dystopian state could only be averted through vigilant protection of ITS technologies from such misuse.

10.2. The Mobility Mayhem

Across the global feed that fateful day, scenes of utter chaos erupted across major cities as their intelligent transportation networks descended into bedlam. In Los Angeles, fleets of autonomous buses inexplicably grounded to a halt, stranding passengers. Intersections in Berlin turned into berserk four-way confrontations as traffic signals cycled manically with no logic.

Meanwhile, vehicles in Shanghai proceeded to randomly race through safety barriers and toll plazas. In New York, subway trains began haphazardly switching tracks, some even steering onto the wrong lines entirely. And in a chilling encore, the air traffic control network for North America suffered a disruption causing planes to dangerously veer off course midflight before sanity could prevail.

All evidence traced back to a coordinated strike by the nefarious Phrenic Remix cybercrime collective. They had successfully infiltrated the backbone networks and systems underlying these metropolitan mobility infrastructures. By hijacking administrative privileges, they triggered ainsidious payload of corrupt firmware updates and logic-bombing malware which crippled core operational capabilities.

What ensued was a heart-stopping preview of the mayhem that could ensue in a world rendered "mobility brittle." Allowed to persist, such widespread erosion of transportation system integrity, security and resilience would collapse entire economies and societies. Yet the threat remained all too real without tireless efforts to fortify ITS technologies and processes against relentless targeting by cybercriminals and hostile actors.I tried to illustrate the critical importance of ITS security and privacy through some hypothetical, worst-case scenarios where those protections fail

11. The importance of transportation " intelligent transportation system" for society:

An intelligent transportation system (ITS) refers to the integration of advanced information and communication technologies (ICT) with transportation infrastructure and vehicles. The primary goal of ITS is to enhance the efficiency, safety, and sustainability of transportation systems. Here are some key aspects of ITS and its importance for society:

1. ITS employs various technologies, such as sensors, cameras, and communication networks, to monitor and manage traffic flow in real-time. This enables dynamic route guidance, adaptive signal control, and incident management, reducing congestion and travel times.
2. ITS incorporates advanced driver assistance systems (ADAS), vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, and collision avoidance systems. These technologies can help prevent accidents, protect vulnerable road users, and improve overall road safety.
3. By optimizing traffic flow and minimizing idling and stop-and-go conditions, ITS can contribute to reducing fuel consumption and greenhouse gas emissions from transportation sources, promoting sustainability and environmental protection.
4. ITS can optimize public transportation systems by providing real-time information on schedules, routes, and service updates. This can encourage modal shifts from private vehicles to public transportation, alleviating congestion and promoting resource-efficient mobility.
5. ITS can facilitate accessible and inclusive transportation for individuals with disabilities, the elderly, and other vulnerable groups through assistive technologies, navigation aids, and customized services.
6. ITS generates vast amounts of data on traffic patterns, travel behavior, and system performance. This data can inform

transportation planning, infrastructure investments, and policy decisions, leading to more efficient and responsive transportation systems.

7. By reducing congestion, improving logistics, and enhancing overall transportation efficiency, ITS can contribute to economic productivity, competitiveness, and growth by facilitating the movement of goods and people.

It is concluded from the above that while the implementation of ITS requires significant investment in infrastructure, technology, and education, the potential benefits for society are substantial. ITS has the potential to transform transportation systems, making them smarter, safer, and more sustainable, ultimately improving the quality of life for individuals and communities.

12. The role of the state in addressing "security and privacy issues in the intelligent transportation system":

The state plays a crucial role in addressing security and privacy issues within the intelligent transportation system (ITS). As ITS relies heavily on the collection, transmission, and processing of data, ensuring the protection of sensitive information and maintaining system integrity is of paramount importance. Here are some key responsibilities and roles of the state in addressing security and privacy concerns:

The state must develop comprehensive regulatory frameworks and policies to govern the collection, use, and protection of data within ITS. These regulations should strike a balance between enabling the benefits of ITS while safeguarding individual privacy rights and protecting against potential misuse or unauthorized access to data.

The state should establish clear data governance standards and protocols for ITS, specifying guidelines for data collection, storage, retention, and sharing practices. These standards should align with relevant privacy laws and ensure that personal and sensitive information is handled with the utmost care and confidentiality.

ITS infrastructure and systems are vulnerable to various cybersecurity threats, such as hacking, malware, and cyber-attacks. The state should implement robust cybersecurity measures, including encryption, firewalls, and intrusion detection systems, to protect ITS networks and prevent unauthorized access or disruptions.

The state should play an active role in raising public awareness about the potential risks and benefits of ITS, as well as educating citizens on best practices for protecting their privacy and securing their personal information within the context of ITS.
ITS involves multiple stakeholders, including transportation agencies, technology providers, and private entities. The state should facilitate collaboration and coordination among these stakeholders to ensure consistent security and privacy practices and seamless interoperability across different ITS components.

The state should regularly conduct risk assessments and audits to identify potential vulnerabilities and weaknesses within ITS systems. These assessments should inform the development of mitigation strategies and the continuous improvement of security and privacy measures.

The state should establish clear accountability mechanisms and oversight bodies to monitor compliance with security and privacy regulations, investigate potential breaches or violations, and enforce appropriate penalties or remedial actions when necessary. Therefore, by fulfilling these roles, the state can foster trust in ITS among citizens and stakeholders, enabling the realization of the potential benefits of these advanced transportation systems while mitigating risks and protecting individual privacy rights.

References:

Ami, R. B. K., AlAhmari, M.H., & Mohammed, A. (2011) Intelligent Transportation Systems. Scientific & Academic Publishing.

Asuquo, P. et al. (2018). A Secure Edge Computing-Assisted Internet of Vehicles for Intelligent Transportation Systems. Sensors, 18(10), 3498.

Asuquo, P., Chan, H., Otung, I., & Aziz, A. (2018). VMaSCIoT Dataset: A Secure Vehicle Mobility Dataset for IoT/Mobile Data Communication in Vehicular Ad-Hoc Networks Research. ArXiv, abs/1812.09996.

Bagheri, B., Safavi, S., & Menendez, J.M. (2020). An Overview of Intelligent Transportation Systems and V2X Communication. Software Engineering for Intelligent Vehicular Systems: Current State and Future Directions, 1-19.

Balocco, R. et al. (2016). Soft Privacy for ITS. International Conference on Smart Objects and Technologies for Social Good, 147-152.

Cottrill, C. D. (2020). COVID-19 & Privacy in Intelligent Transport Systems: Challenges, Trade-offs and Governance. University of Leeds. https://urbanitransportgroup.com/system/files/general-docs/2.%20UtG%20Webinar%20Cottrill%2015%20May%202020.pdf

Deljoo, A., Ghafouri, M., Mir Hassani Nik, R., &Eyvazian, M. (2018). Cyber-Physical Security in Intelligent Transportation Systems. 2018 11th IFIP Wireless and Mobile Networking Conference (WMNC), 1-8.

Dimitrakopoulos, G. &Demestichas, P. (2010). Intelligent Transportation Systems. IEEE Vehicular Technology Magazine, 5(1), 77-84.

Dorri, A. et al. (2017). Blockchain for IoT security and privacy: The case study of a smart home. IEEE Pervasive Computing Workshop.

Gerlach, C., Lin, O., Tan, Y., Harbort, B., & Lee, Y. C. (2017). Privacy concerns of ongoing data collection and diffusion of travel data: a Singapore perspective. 2017 International Conference on Applied System Innovation (ICASI), 613-617.

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, J. A. (2014). Green lights forever: analyzing the security of traffic infrastructure. 8th USENIX Workshop on Offensive Technologies (WOOT 14).

Hoppe, T., Kiltz, S., & Dittmann, J. (2008). Security threats to automotive CAN networks -- practical examples and selected short-term countermeasures. Reliability Engineering & System Safety,93(1), 11-25.

Krauss, J. et al. (2020). User Privacy in Intelligent Transportation Systems: A Smart City Perspective. IEEE Communications Standards Magazine, 4(4), 17-22.

Lefèvre, J. &Lefèvr, V. (2017). Privacy Concerns in Intelligent Transportation Systems. European Conference on Cyber Warfare and Security, 246-255.

Leng, Y. & Nitz, J. (2019). Cyber-Physical Security for Intelligent Transportation Systems. IEEE Intelligent Transportation Systems Magazine.

Lorgat, G., Teyou, A., &Çamci, A.N. (2021). Cyber Security Life Cycle Approach in Intelligent Transportation Systems. 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), 1-7.

Lyu, X., Ren, H., & Tang, S. (2019). Cyber Security for Smart Transportation Systems. In N. Nikdel (Ed.), Cyber Risk Analytics: An Integrated Approach (pp. 243-257). CRC Press.

Maniatis, S., Barranco, D., Stamatelatos, M., Loikkanen, V., Katsikas, S., &Uznanski, P. (2021). A Review on Security and Privacy Schemes for Vehicle-to-Everything Communications. IEEE Access, 9, 146791-146827.

Milutinovic, M. et al. (2016). Privacy Concern and Users' Acceptance of Location-Based Services. IEEE 17th International Conference on Mobile Data Management, 139-144.

Mullin, B., Chambers, R., Warder, K., Pitzini, M., Hill, L., Smith, T., & Remias, S. (2022). The U.S. National ITS Architecture provides continuity of planning for ITS. Journal of Advanced Transportation, 2022.

Parkinson, S. et al. (2017). Cyber threats facing autonomous and connected vehicles. IEEE Transactions on Intelligent Transportation Systems, 18(11).

Petit, J., &Shladover, S.E. (2015). Potential Cyberattacks on Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(2), 546-556.

Qudrat, U. et al. (2021). Cyber-Physical Security in Intelligent Transportation Systems: An Overview. Electronics, 10(15), 1792.

Rao, P. et al. (2019). Monetization Over Massively Crowd-Sourced Sensing Data Streams for Bridging the Last Mile via Intelligent Systems. IEEE Access, 7, 49271-49296.

Zheng, L. et al. (2019). Securing Intelligent Transportation Systems: A Panoramic View of Emerging Security Threats and Defensive Techniques. IEEE Vehicular Technology Magazine, 14(4), 48-57.