



REVIEW

Applications of IoT in Intelligent Transportation Systems: Research Landscape, Technological Innovations, Challenges, and Future Opportunities

Mahbub Hassan¹ , Md Kamrul Islam^{2,*} , Md Shafiul Alam³ , Mohammad Bin Amin^{4,5,*} ,
M. M. Hafizur Rahman⁶ , Md Ehtesamul Haque⁷ and Zoltán Nagy⁸

¹Department of Civil Engineering, Faculty of Engineering, Chulalongkorn University, Bangkok, Thailand

²Department of Civil and Environmental Engineering, College of Engineering, King Faisal University, Al Ahsa, Saudi Arabia

³Department of Electrical Engineering, College of Engineering, King Faisal University, Al Ahsa, Saudi Arabia

⁴Doctoral School of Management and Business, Faculty of Economics and Business, University of Debrecen, Bösörményi Street 138, Debrecen, Hungary

⁵Department of Business Administration, Faculty of Business Studies, Bangladesh Army University of Science and Technology, Saidpur, Nilphamari, Bangladesh

⁶Department of Computer Networks & Communications, College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al Ahsa, Saudi Arabia

⁷Department of Computer Science, College of Computer Science and Information Technology (CCSIT), King Faisal University, Al Ahsa, Saudi Arabia

⁸John von Neumann University, Kecskemét, Hungary

*Corresponding Authors: Md Kamrul Islam. Email: maislam@kfu.edu.sa; Mohammad Bin Amin. Email: binamindu@gmail.com

Received: 11 May 2026; Accepted: 22 June 2026; Published: 15 September 2026

ABSTRACT: The integration of the Internet of Things (IoT) into Intelligent Transportation Systems (ITS) is transforming urban mobility through widespread sensing, real-time data exchange, and Artificial Intelligence (AI)-driven adaptive control. Although research in this domain has expanded rapidly, bibliometric analyses combined with critical thematic synthesis remain limited. This study addresses this gap through a two-stage analysis of 574 peer-reviewed articles indexed in Scopus from 2011 to 2024. Using performance analysis, keyword co-occurrence mapping, and co-authorship network visualization, the study maps global publication trends, institutional productivity, and collaboration patterns. The results show an annual growth rate of 27.06%, with China, India, and the United States emerging as the leading contributors. Thematic evolution analysis identifies three research phases: foundational IoT connectivity from 2011 to 2019, distributed AI and fog computing from 2020 to 2022, and blockchain-enabled secure automation from 2023 to 2024. The synthesis covers eight application domains, including cybersecurity, blockchain, edge computing, traffic prediction, V2X communication, and signal optimization. It also proposes a functional taxonomy of IoT integration across sensing, communication, processing, control, security, and human-system interaction layers. Key deployment challenges include interoperability constraints, legacy system integration, data governance, and sociotechnical barriers to equitable adoption. Emerging research priorities include digital twins, federated learning, vehicular edge AI, post-quantum cryptography, trustworthy and explainable AI for safety-critical decision-making, and large language models as semantic reasoning layers within IoT-ITS workflows. This review provides a critically synthesized reference for researchers and policymakers and identifies practical directions for developing scalable, secure, and socially inclusive intelligent transportation systems.

KEYWORDS: Artificial intelligence; large language models; cybersecurity; digital twins; vehicular communication; Internet of Things; intelligent transportation systems

1 Introduction

The integration of the Internet of Things (IoT) into Intelligent Transportation Systems (ITS) is reshaping the design, management, and optimization of urban mobility infrastructure. Continuous data exchange among vehicles, roadside units, sensors, and control centers enables adaptive traffic management, real-time incident response, connected mobility services, and the deployment of connected and autonomous vehicles [1,2]. As transportation networks increasingly operate as cyber-physical systems, the convergence of IoT and ITS has become a core component of smart city development and sustainable mobility planning.

Research on IoT-enabled ITS has expanded rapidly over the past decade, advancing several interrelated frontiers. In infrastructure and service integration, Ke et al. [3] developed a hybrid edge-cloud smart parking framework that reduces vehicle search time through real-time occupancy sensing, while Kumari et al. [4] proposed a tri-layer blockchain-IoT-6G architecture for Unmanned Aerial Vehicle (UAV)-assisted traffic control. In cybersecurity, Stellios et al. [5] developed a structured taxonomy of IoT-specific attack surfaces in transportation systems, and Lei et al. [6] introduced a distributed cryptographic protocol based on IEEE 802.11p and elliptic-curve encryption to reduce dependence on centralized certificate authorities. Artificial intelligence has become a further enabler of this expansion. Chu et al. [7] proposed MultiConvLSTM for spatiotemporal demand forecasting, Iqbal et al. [8] applied fuzzy logic to real-time congestion prediction, Nie et al. [9] developed a Convolutional Neural Network (CNN)-based intrusion detection system for vehicular networks, and Abdel-Basset et al. [10] proposed FED-IDS, a federated framework combining Transformer-based traffic representation learning with blockchain-secured model validation. Akbar et al. [11] further integrated Complex Event Processing with predictive models to support adaptive, low-latency forecasting at the network edge.

Architectural innovation has progressed alongside these algorithmic developments. Kang et al. [12] proposed a fog-based, privacy-preserving scheme using cryptographic signatures and context-aware parameters for secure data offloading. Lin et al. [13] integrated Software-Defined Networking with spatiotemporal modeling to support congestion-aware adaptive routing, and Sodhro et al. [14] designed a self-adaptive framework that coordinates 5G-enabled fog-cloud layers to improve quality-of-service for real-time vehicular multimedia. Together, these studies reflect a broader transition from centralized cloud dependence toward distributed, latency-sensitive ITS architectures.

Despite this momentum, several gaps remain. Existing reviews are often domain-specific or narrative in scope, and few studies apply quantitative bibliometric methods to systematically map the intellectual structure of IoT-ITS research. Limited attention has been given to approaches that combine bibliometric performance analysis with critical thematic synthesis, capable of jointly capturing macro-level publication trends and the conceptual depth of technological development. The growing convergence of IoT-ITS with Transformer-based architectures and large language models (LLMs) also remains underexplored as a structured research direction, and a comparative understanding of how these methods relate to established machine learning approaches in transportation is still limited [15].

This study addresses these gaps through a dual-method framework that integrates bibliometric analysis with structured thematic synthesis. Drawing on 574 peer-reviewed articles indexed in Scopus between 2011 and 2024, it maps global publication trends, institutional collaboration networks, keyword co-occurrence patterns, and thematic clusters, and critically reviews high-impact studies to trace methodological trajectories and identify persistent research deficiencies. The contribution of this study is threefold. First, it applies an integrated bibliometric-thematic methodology to IoT-ITS as a unified research domain. Second, it develops a structured taxonomy of IoT integration across ITS functional layers, including sensing, communication, processing, control, security, and human-system interaction. Third, it critically synthesizes

emerging paradigms, including federated learning, vehicular edge AI, blockchain-based security, and the prospective role of LLMs in intelligent mobility systems.

To guide the investigation, three research questions are formulated:

- RQ1: How has IoT-ITS research evolved over time in terms of publication volume, thematic clusters, and dominant technological paradigms?
- RQ2: How do existing studies address core ITS functionalities, including security, real-time data processing, scalability, and edge intelligence, and what methodological patterns characterize the literature?
- RQ3: What principal research gaps and underexplored opportunities exist in the IoT-ITS domain, as revealed through integrated bibliometric and thematic analysis?

The remainder of this paper is organized as follows. [Section 2](#) describes the bibliometric methodology, including data collection, PRISMA-based screening, and analytical procedures. [Section 3](#) presents the performance analysis and science mapping results. [Section 4](#) synthesizes IoT applications across eight thematic domains. [Section 5](#) examines technical, governance, and societal challenges and identifies future research directions. [Section 6](#) summarizes the principal findings, contributions, and limitations of the study.

2 Methodology

This study adopts a systematic, data-driven bibliometric methodology to examine the intellectual evolution, structural dynamics, and thematic progression of research on IoT applications in ITS. The methodological framework follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines [16], supporting transparency, replicability, and methodological rigor. The analysis covers the period from 2011 to 2024, capturing both the early development of IoT-ITS research and its subsequent expansion into advanced paradigms such as edge computing, federated learning, and AI-driven traffic management.

As illustrated in [Fig. 1](#), the research process consists of five sequential stages. The first stage involved data collection, where Scopus was selected as the source database and a structured search query was applied to retrieve publications from 2011 to 2024. The second stage involved data processing through a PRISMA-aligned screening procedure, including subject area, document type, and language filters, followed by manual eligibility assessment. The third stage focused on software selection, using Bibliometrix in R, Python, and VOSviewer to support bibliometric processing, visualization, and network analysis. The fourth stage comprised the analytical framework, including performance analysis, data visualization, and science mapping. The final stage synthesized the results in relation to IoT applications in transportation, deployment challenges, and future research directions. This multi-stage design enables a systematic assessment of publication trends, collaboration networks, and thematic evolution across the global IoT-ITS research landscape.

2.1 Data Source Selection and Justification

Selecting a reliable bibliographic database is a foundational step in bibliometric research because it shapes the scope, completeness, and analytical validity of the resulting corpus. This study uses Scopus as the primary data source because of its broad interdisciplinary coverage, high metadata completeness, and established compatibility with scientometric tools [17–20]. The decision to rely exclusively on Scopus was based on a structured comparison with the Web of Science (WoS), considering retrieval volume, metadata structure, and domain representativeness.

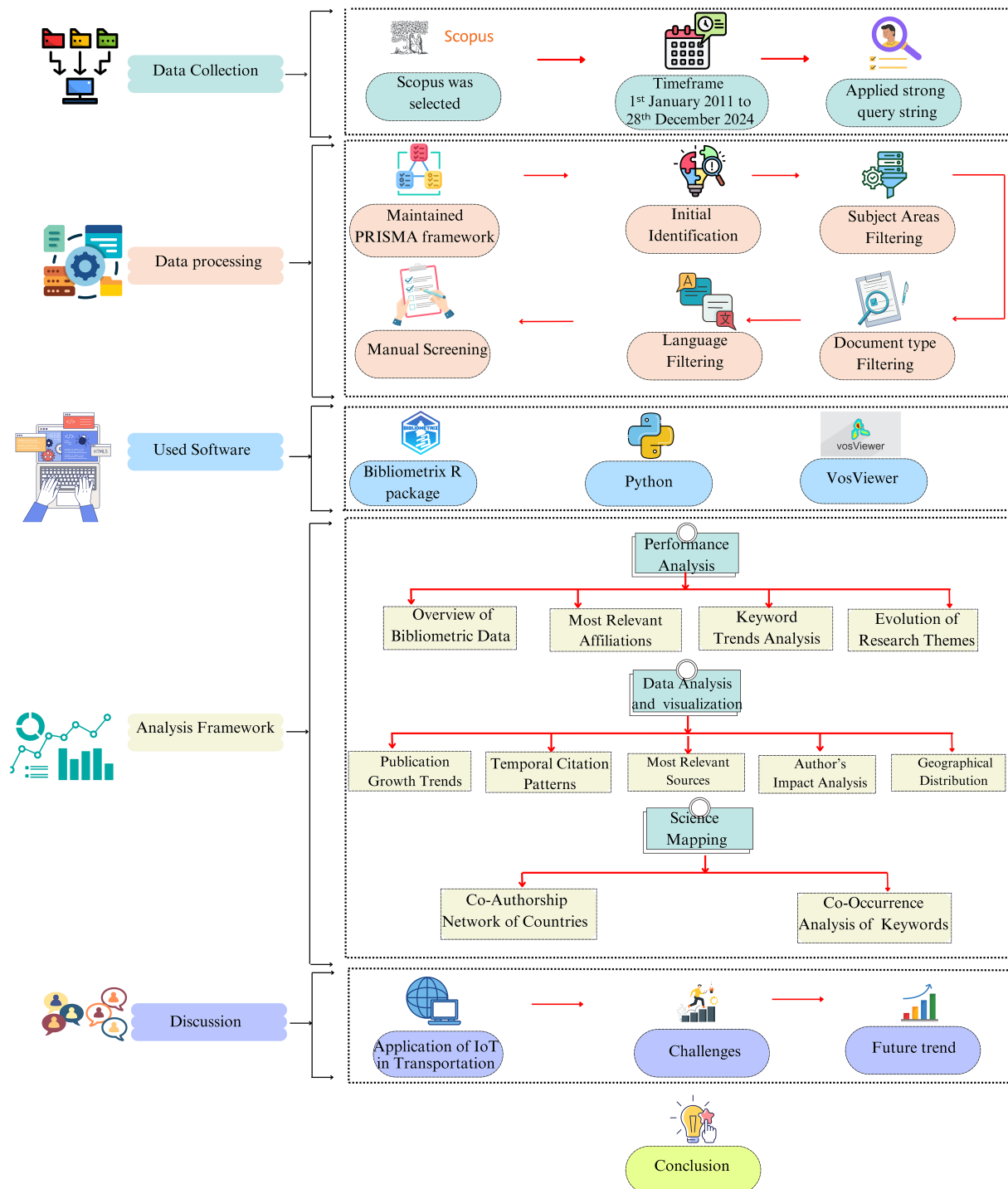


Figure 1: Methodological framework of the bibliometric study on IoT-enabled ITS, integrating PRISMA-based filtering and analysis via Bibliometrix, VOSviewer, and Python.

A parallel query conducted on both platforms retrieved 1511 records from Scopus and a substantially smaller number from WoS, indicating broader indexing coverage in Scopus. This difference is particularly relevant for a technology-intensive and rapidly evolving field such as IoT-ITS, where early innovations often appear in conference proceedings before being developed into journal publications [21–23]. Scopus

indexes major publication venues relevant to this domain, including IEEE Transactions on Intelligent Transportation Systems, Transportation Research Part C: Emerging Technologies, Sensors, and Expert Systems with Applications, thereby supporting both disciplinary breadth and scholarly relevance.

In addition to coverage, Scopus provides metadata fields required for the bibliometric analyses conducted in this study, including co-citation mapping, keyword co-occurrence analysis, and co-authorship network visualization. Its exported metadata can also be processed directly in VOSviewer [24], Bibliometrix in R [25], and CiteSpace [26]. By contrast, merging records from multiple databases can introduce duplicate entries, citation inconsistencies, and field-level mismatches, which may reduce reproducibility. Manual cross-verification further indicated that most WoS-indexed IoT-ITS publications retrieved during the comparison were also captured in Scopus, supporting its use as a standalone source for this review.

Nevertheless, exclusive reliance on Scopus introduces a coverage limitation. Studies indexed only in Web of Science, IEEE Xplore, ACM Digital Library, or transportation-specific outlets and databases may not be represented in the final corpus. This limitation is common in bibliometric studies, but it should be considered when interpreting the geographic, institutional, and disciplinary patterns reported in this review. Future syntheses may benefit from multi-database integration protocols that address deduplication, metadata harmonization, and citation consistency in a systematic manner.

2.2 Data Collection and Refinement

The dataset was constructed using a structured Boolean search query applied to Scopus on 28 December 2024. The query targeted publications at the intersection of IoT technologies and ITS and retrieved 1,511 records, including journal articles, conference papers, book chapters, and review articles. The full search string and retrieval parameters are presented in Table 1.

Table 1: Search strategy and data retrieval parameters for the bibliometric analysis.

Date	Database	Time Frame	Search Query
28 December 2024	Scopus	2011–2024	TITLE-ABS-KEY ((“Internet of Things” OR “IoT-enabled” OR “smart sensor*” OR “connected vehicle*” OR “vehicle-to-infrastructure” OR “vehicular network*” OR “V2X communication” OR “IoT platform*”) AND (“intelligent transportation system*” OR “ITS” OR “smart mobility” OR “traffic management” OR “traffic flow” OR “transportation infrastructure” OR “adaptive traffic signal*” OR “urban mobility” OR “smart city transportation”))

The period from 2011 to 2024 was selected to capture the broad trajectory of IoT-ITS research, from its early technological foundations to its more recent expansion into advanced paradigms such as edge computing, federated learning, and AI-driven traffic management. The starting year was chosen because it corresponds to a period in which scalable cloud computing platforms, low-power wireless sensor standards, and connected vehicle research began to gain stronger visibility in transportation-related scholarship. This period also aligns with major public initiatives directed toward intelligent mobility, including the United States Connected Vehicle Program and European Union Horizon research initiatives [27], which contributed to increased research activity in IoT-enabled transportation. The upper boundary of 2024 ensures coverage of recent advances in artificial intelligence, blockchain-based security, and edge computing within ITS contexts.

Following retrieval, a five-stage refinement protocol aligned with PRISMA standards [16] was applied to improve dataset quality and thematic coherence. Table 2 summarizes each filtering stage and the corresponding inclusion and exclusion criteria.

Table 2: Data refinement and PRISMA-aligned filtering process for the bibliometric corpus.

Stage	Description	Retained Records	Inclusion/Exclusion Criteria
Initial Search	Comprehensive retrieval using the defined Boolean query	1511	All document types included
Subject Filtering	Removal of records from non-relevant disciplines, including social sciences, physics, and decision sciences	897	Retained engineering, computer science, and ITS-related subject areas
Document Filtering	Exclusion of non-scholarly document types, including editorials, short notes, and trade publications	849	Retained peer-reviewed journal articles, conference papers, book chapters, and review articles
Language Filtering	Restriction to English-language publications	844	Ensured interpretability and compatibility with analytical tools
Manual Screening	Title, abstract, and keyword review by two independent screeners; disagreements resolved by consensus	574	Inclusion: peer-reviewed journal articles, conference papers, book chapters, and review articles on IoT-enabled ITS applications; Exclusion: policy-only documents, opinion pieces, and studies without substantive technical content

The manual screening stage was conducted by two independent reviewers using a predefined eligibility protocol. Each record was assessed independently based on its title, abstract, and author keywords. Studies were included when they met all of the following criteria: (i) the document was a peer-reviewed journal article, conference paper, book chapter, or review article; (ii) the study explicitly addressed IoT, IoV, connected sensors, edge or cloud platforms, vehicular communication, cyber-physical data exchange, or IoT-enabled infrastructure within an ITS or transportation context; and (iii) the paper reported an empirical, methodological, architectural, algorithmic, or applied contribution relevant to IoT-enabled ITS. Records were excluded when they: (i) focused only on general smart-city policy without substantive IoT-ITS content; (ii) discussed transportation policy, planning, or sustainability without a clear technical IoT component; (iii) were editorials, short notes, opinion papers, commentaries, trade publications, or other non-scholarly documents; (iv) lacked clear engagement with either IoT or ITS as operationalized in the search query; or (v) were not written in English. Inter-rater agreement was assessed before consensus resolution using Cohen's kappa, yielding $\kappa = 0.84$, which indicates substantial agreement between the two reviewers. Disagreements were resolved through discussion and consensus by rechecking disputed records against the eligibility protocol. The final corpus of 574 peer-reviewed documents therefore provides a thematically coherent and methodologically defensible dataset for bibliometric mapping and qualitative thematic synthesis.

2.3 Data Analysis and Software Selection

Methodological triangulation was achieved using three complementary tools, each serving a distinct function within the analytical workflow.

- **Bibliometrix (R):** Bibliometrix was used for quantitative performance analysis, including publication growth trends, citation metrics, author productivity, journal output, and institutional contributions [25]. The package provided the statistical basis for characterizing the developmental trajectory of the field.
- **VOSviewer:** VOSviewer was applied for science mapping and network visualization, including co-authorship, co-citation, and keyword co-occurrence analyses [24]. The resulting maps were used to identify collaborative clusters, intellectual linkages, and shifts in thematic priorities across the study period.
- **Python:** Python was used for data preprocessing, deduplication validation, and the generation of customized analytical visualizations. The pandas, matplotlib, and seaborn libraries supported temporal trend modeling and the production of publication-quality figures.

To ensure reproducibility, the analytical parameters are reported explicitly below.

(i) **Counting method.** Citation counts were based on total citation frequency extracted directly from Scopus metadata at the time of retrieval on 28 December 2024. The initial Scopus query retrieved 1511 records, which were reduced through PRISMA-aligned filtering to a final analytical corpus of 574 peer-reviewed documents published between 2011 and 2024. No fractional or weighted citation counting was applied; each citation received by a document contributed one unit to its total citation count. The corpus accumulated 13,760 citations, corresponding to an average of 23.97 citations per document. Publication output, source productivity, country contribution, institutional affiliation, and author productivity were also interpreted using full counting, whereby each document was counted once for every relevant bibliographic unit represented in the exported Scopus metadata.

(ii) **Normalization method.** No field normalization or age normalization was applied to citation counts. This decision reflects the domain-specific scope of the review, where absolute citation influence within the IoT-enabled ITS corpus is more relevant than cross-field comparability. Citation indicators were therefore interpreted as descriptive measures of influence within the selected IoT-ITS dataset rather than as normalized measures of impact across disciplines or publication years. For network visualization, VOSviewer association-strength normalization was applied to reduce the dominance of highly frequent terms and improve the interpretability of relational structures.

(iii) **Keyword co-occurrence threshold.** The corpus contained 1521 author keywords and 3176 Keywords Plus terms. Before network construction, author keywords were cleaned using a manual thesaurus file, reducing 1521 raw keyword variants to 1318 normalized keyword forms. For the author-keyword co-occurrence analysis, a minimum co-occurrence threshold of five was applied in VOSviewer. This threshold retained 87 keywords in the final network, representing 6.6% of the normalized keyword set. The resulting keyword co-occurrence map contained 1038 links and a total link strength of 3276. The average number of links per retained keyword was 23.86, indicating a moderately dense and thematically interpretable network. Terms below the threshold were excluded from the visualization network to reduce noise, but they were retained in the underlying bibliometric dataset used for descriptive keyword-frequency analysis.

(iv) **Clustering resolution.** Network clustering in VOSviewer used the default resolution parameter of 1.0 with association-strength normalization. This configuration produced four conceptual clusters, consistent with the thematic structure shown in the keyword co-occurrence network. Cluster 1 contained 31 terms and was anchored by “Internet of Things,” “Intelligent Transportation Systems,” and “Smart City,” representing the integrative foundation of IoT-enabled ITS research. Cluster 2 contained 26 terms and grouped “Internet

of Vehicles,” “Security,” “Deep Learning,” and “Machine Learning,” reflecting the convergence of networked architectures, cybersecurity, and AI-driven analytics. Cluster 3 contained 17 terms centered on vehicular communication protocols, including “VANET,” “V2V,” “V2X,” and related communication technologies. Cluster 4 contained 13 terms associated with low-latency routing, decentralized processing, autonomous systems, edge computing, and smart mobility services. The four-cluster solution was retained because it provided clear thematic separation without fragmenting closely related topics.

(v) Time-slicing strategy. Thematic evolution was analyzed across three discrete phases derived from publication growth patterns and temporal keyword prominence. The first phase, 2011–2019, represents the foundational connectivity phase and includes 222 documents, accounting for 38.7% of the corpus. Research in this phase focused primarily on IoT connectivity, vehicular networks, wireless sensing, traffic monitoring, quality of service, and early privacy-preserving frameworks. The second phase, 2020–2022, represents the distributed AI and fog computing phase and includes 181 documents, accounting for 31.5% of the corpus. During this period, the field shifted toward edge computing, fog computing, machine learning, deep learning, task offloading, and real-time traffic analytics. The third phase, 2023–2024, represents the blockchain-enabled secure automation phase and includes 171 documents, accounting for 29.8% of the corpus. This recent phase shows stronger emphasis on blockchain, cybersecurity, federated learning, digital twins, V2X communication, and secure decentralized automation. These phase boundaries were determined empirically from annual publication trends and temporal keyword frequency distributions rather than imposed a priori.

(vi) Thesaurus and term normalization. The IoT-ITS literature exhibits substantial terminological fragmentation due to the widespread use of abbreviations, spelling variations, singular and plural forms, and alternative expressions for the same concept. Before constructing the keyword co-occurrence network, a manual thesaurus file was applied in VOSviewer to merge semantically equivalent terms and improve the accuracy of thematic mapping. For example, “Internet of Things,” “IoT,” “IoT-enabled,” “IoT based,” and “IoT-based” were unified under the normalized term “Internet of Things.” Similarly, “Internet of Vehicles,” “IoV,” “Vehicle Internet,” and “Internet-of-Vehicles” were consolidated as “Internet of Vehicles.” Standardization was also performed for other frequently occurring terms, including “intelligent transportation system” and “intelligent transportation systems,” “vehicular ad hoc network” and “VANET,” “vehicle-to-everything” and “V2X,” “vehicle-to-vehicle communication” and “V2V,” as well as “edge computing” and “edge-computing.” Overall, the thesaurus cleaning process reduced 1521 raw author-keyword variants to 1318 normalized keyword forms, representing a 13.3% reduction in terminological redundancy. The cleaning procedure was applied consistently across all author-keyword records before network generation, preventing artificial fragmentation of conceptually identical topics. This process improved the interpretability of the four-cluster keyword structure reported in the co-occurrence analysis and ensured that thematic relationships reflected substantive research patterns rather than differences in terminology.

Together, these tools formed a reproducible and methodologically transparent analytical pipeline. Bibliometrix provided quantitative precision in performance measurement, VOSviewer represented the spatial structure of scholarly collaboration and intellectual influence, and Python enabled flexible preprocessing and visualization beyond the capabilities of dedicated bibliometric software. This integrated approach strengthens both the depth and interpretive scope of the investigation into global IoT-ITS research trends, thematic convergence, and the field’s intellectual structure.

3 Results

This section presents the bibliometric findings from two complementary perspectives. The first is performance analysis, which quantifies publication trends, citation patterns, authorship characteristics, source

productivity, and institutional contributions. The second is science mapping, which examines collaboration structures, intellectual linkages, and thematic relationships within IoT-enabled ITS research.

3.1 Performance Analysis

Performance analysis uses citation metrics, authorship patterns, and source-level indicators to characterize the developmental trajectory of a research domain [28]. The following subsections synthesize the main findings related to publication growth, source prominence, institutional productivity, and global collaboration.

3.1.1 Bibliometric Overview and Publication Growth Trends

Table 3 summarizes the core bibliometric indicators for the 574-document corpus covering the period from 2011 to 2024. The dataset spans 277 sources and shows an annual growth rate of 27.06%, indicating substantial expansion of IoT-ITS research during the study period. The average citation rate of 23.97 citations per document, together with 19,730 total references, suggests an active and well-connected intellectual base. The average of four co-authors per document and the international co-authorship rate of 33.1% indicate a collaborative research culture with notable cross-border engagement. Review articles represent only 3% of the corpus, suggesting that integrative synthesis remains relatively limited in this rapidly developing field, a gap that this study addresses.

Table 3: Descriptive bibliometric statistics for IoT-ITS research from 2011 to 2024, summarizing document output, citation patterns, authorship characteristics, and publication types.

Metric	Value
Timespan	2011–2024
Number of Sources	277
Total Documents	574
Annual Growth Rate (%)	27.06
Average Document Age (years)	4.77
Average Citations per Document	23.97
Total References	19,730
Keywords Plus	3176
Author Keywords	1521
Total Authors	1862
Single-Authored Documents	28
Co-Authors per Document	4
International Co-Authorship Rate (%)	33.1
Journal Articles	315
Conference Papers	200
Book Chapters	42
Review Articles	17

As shown in Fig. 2, annual output increased from a relatively low publication base during 2011–2016 to 90 publications in 2024, following an exponential trajectory modeled by $y = 12.84e^{0.15x}$. A clear increase in publication momentum emerged around 2017–2018, indicating a shift from exploratory studies toward broader research engagement across connected transportation and intelligent mobility domains.

This increase is interpreted cautiously as coinciding with 5G NR standardization under 3GPP Release 15, active industry trials, early deployment activity, and growing research investment in 5G-enabled mobility, rather than as evidence of widespread operational 5G adoption during that period [29]. Empirical studies of commercial 5G performance became more visible from 2019 onward, as operational networks and smartphone-based field measurements began to emerge [30]. Concurrent advances in edge computing, vehicular communication, and deep learning further intensified scholarly attention to IoT-enabled ITS. The sustained growth observed through 2023–2024 reflects continued diversification toward federated learning, vehicular AI, blockchain-based ITS security, and edge-enabled intelligent mobility [1].

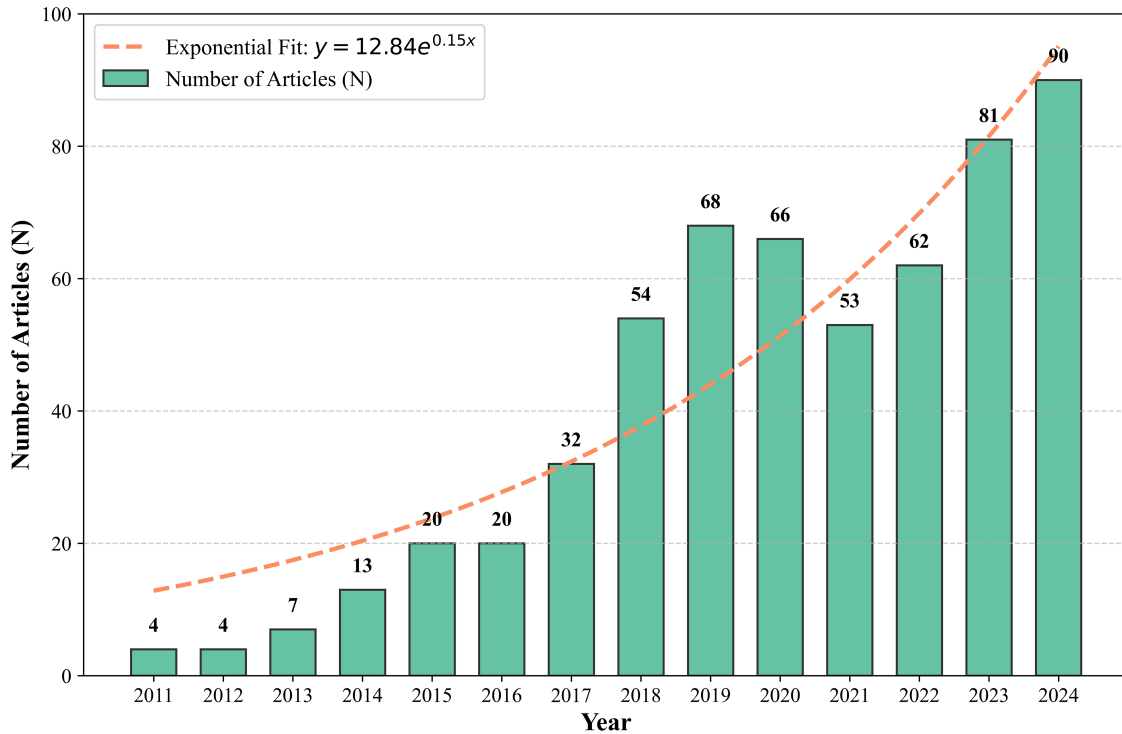


Figure 2: Annual publication trends in IoT-enabled ITS research from 2011 to 2024. Green bars represent yearly publication volume, and the orange dashed line denotes the exponential growth trend ($y = 12.84e^{0.15x}$).

3.1.2 Most Relevant Sources

Fig. 3 presents the leading publication venues in the corpus. IEEE Transactions on Intelligent Transportation Systems contributed the largest number of documents (43), followed by the IEEE Internet of Things Journal (38). This pattern reflects the dual grounding of IoT-ITS research in transportation engineering and networked computing systems. The prominence of IEEE venues also indicates the strong role of empirical, system-oriented, and application-driven research in the field. In addition to journals, conference series such as Lecture Notes in Computer Science and the ACM International Conference Proceedings Series, with 12 documents each, function as early dissemination channels for emerging methods, prototype systems, and rapidly developing technical contributions. This combined publication structure, with journals supporting mature scholarly contributions and conference proceedings enabling timely methodological dissemination, has supported the field's rapid development across both theoretical and applied research directions.

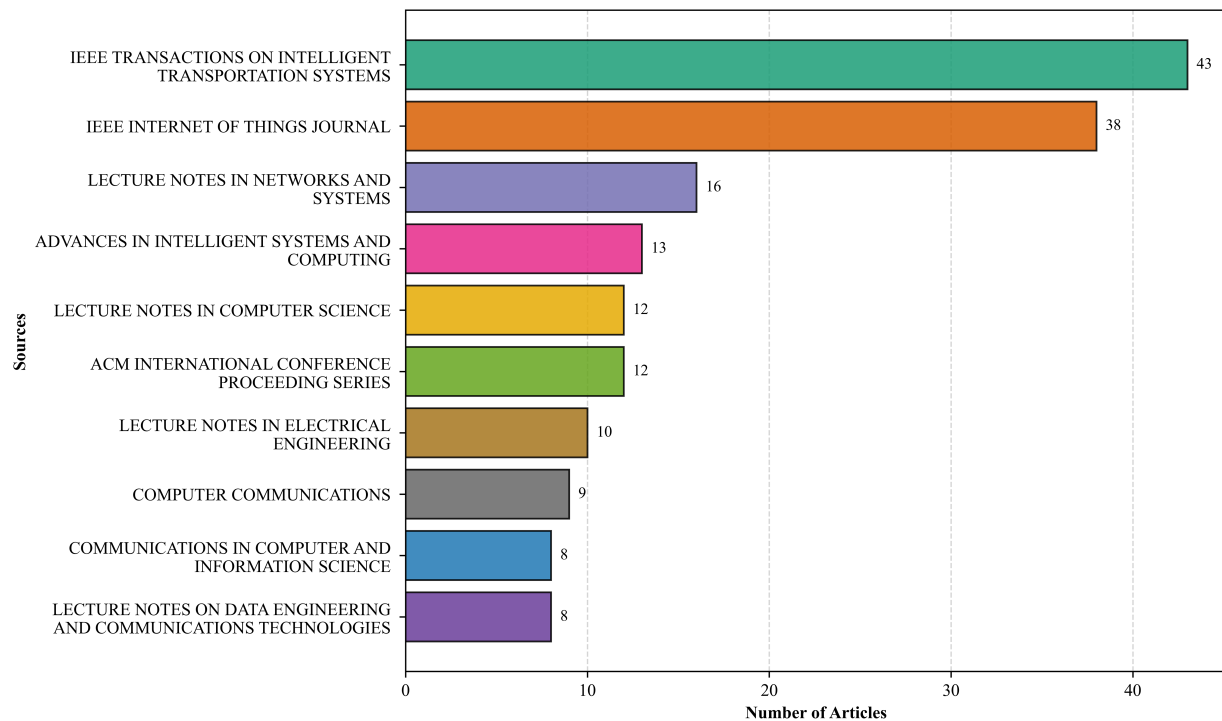


Figure 3: Leading publication sources in IoT-ITS research from 2011 to 2024, ranked by document volume. The distribution indicates the field's dissemination structure across specialized journals and active conference proceedings.

3.1.3 Most Relevant Affiliations

Fig. 4 shows the most productive institutions during the study period. The University of Electronic Science and Technology of China leads with 16 publications, followed by COMSATS University Islamabad and Xidian University, with 13 publications each, and Johannes Kepler University, with 12 publications. Chinese institutions account for a large share of the top-ranked affiliations, reflecting sustained research activity in AI-driven mobility, vehicular security, and IoT infrastructure. Two observations can be drawn from this distribution. First, the concentration of output among a relatively small group of Asian institutions raises questions about geographic balance in knowledge production and the extent to which deployment contexts in other regions, particularly Africa, Latin America, and Southeast Asia, are represented in the literature. Second, the presence of Pakistani, Australian, Chinese, and European institutions indicates a gradually diversifying research base, although participation remains uneven across regions. As the field matures, broader institutional participation will be important for developing ITS solutions that are responsive to varied infrastructure conditions, governance systems, and regulatory environments.

3.1.4 Global Research Landscape and Collaboration Trends

Figs. 5 and 6 present the geographic distribution of research output and the ratio of Single-Country Publications (SCP) to Multi-Country Publications (MCP) across leading countries. China, India, and the United States account for the largest share of publications, reflecting strong research activity in smart infrastructure, urban digitalization, connected mobility, and autonomous transportation systems. The United Kingdom, Saudi Arabia, and Canada show comparatively high MCP ratios, indicating active cross-border engagement rather than predominantly domestic research activity. This pattern suggests that international collaboration is unevenly distributed. High-output countries tend to sustain relatively self-contained research

ecosystems, whereas several mid-output countries rely more heavily on international partnerships to extend their scholarly reach.

A key limitation of this geographic distribution, consistent with the use of Scopus as the data source, is the underrepresentation of research from Africa, Latin America, and parts of Southeast Asia. These regions face substantial transportation infrastructure and urban mobility challenges, yet they contribute relatively little to the indexed literature. This underrepresentation may reflect structural barriers, including limited access to indexed publication venues and lower institutional research capacity, rather than the absence of IoT-ITS activity in practice. Future reviews should consider regional databases and gray literature to develop a more globally representative evidence base.

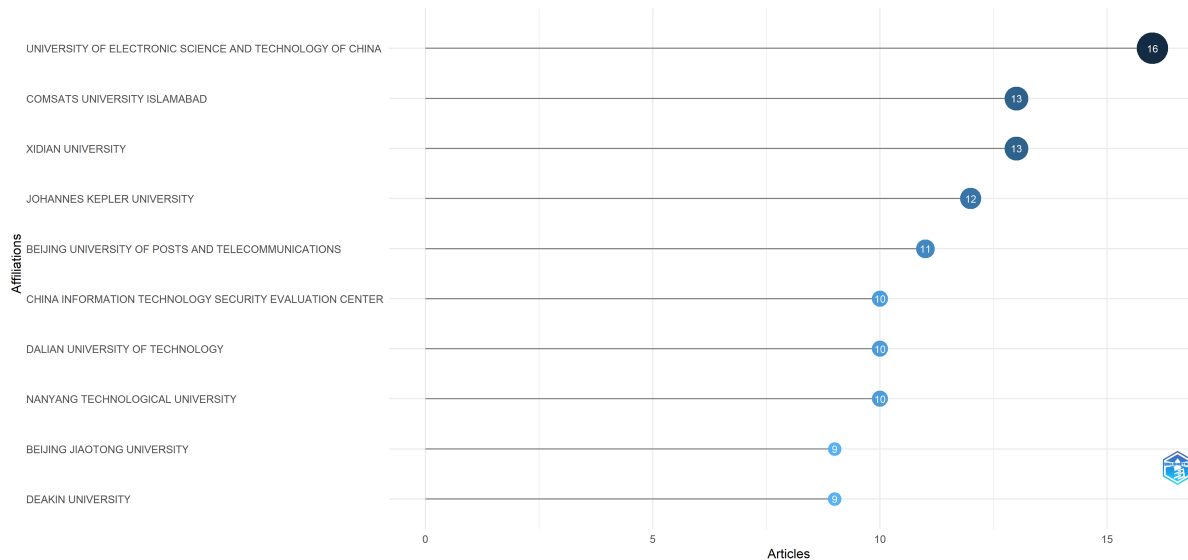


Figure 4: Leading institutional contributors to IoT-enabled ITS research from 2011 to 2024, ranked by publication volume.

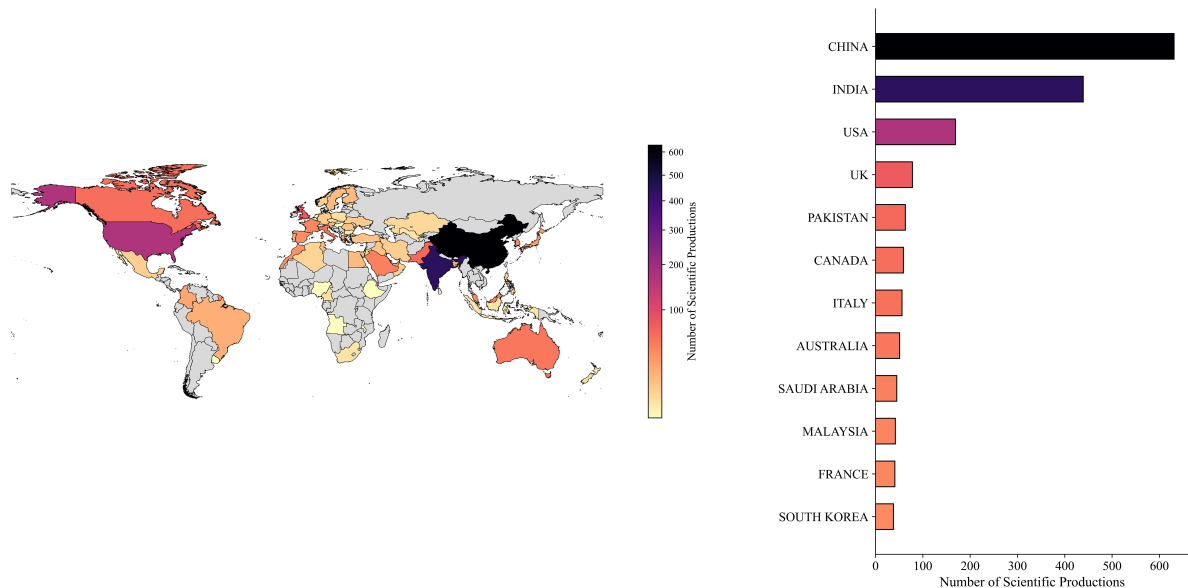


Figure 5: Global distribution of IoT-ITS research output from 2011 to 2024, showing country-level publication intensity.

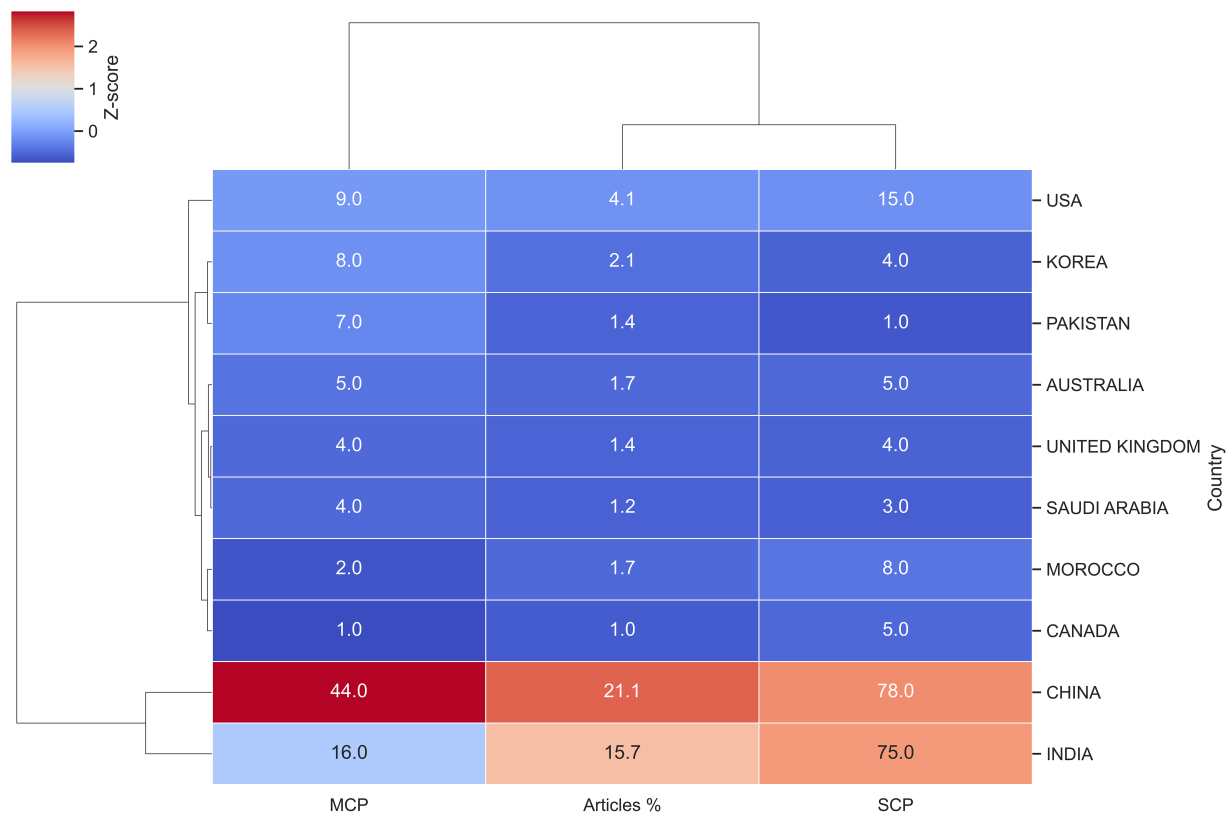


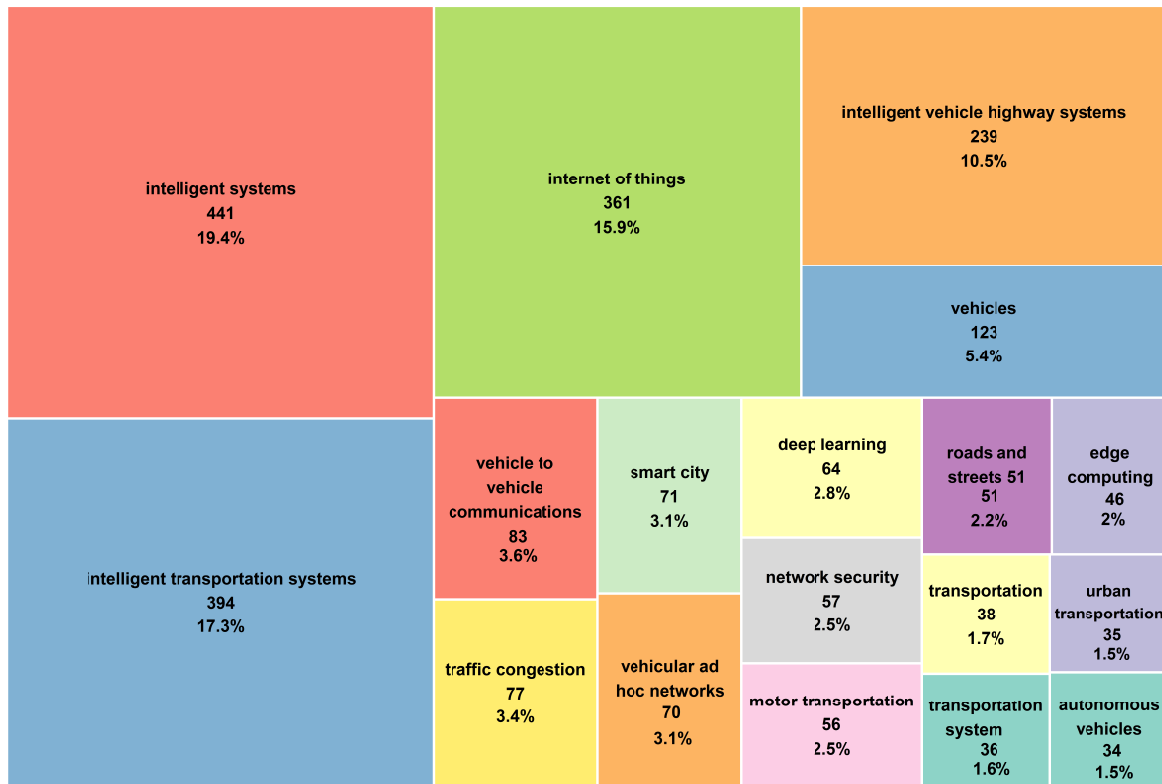
Figure 6: Single-Country Publications (SCP) and Multi-Country Publications (MCP) in IoT-enabled ITS research from 2011 to 2024, showing the balance between domestic research output and international collaboration by country.

3.1.5 Thematic Structure and Evolution of IoT-ITS Research

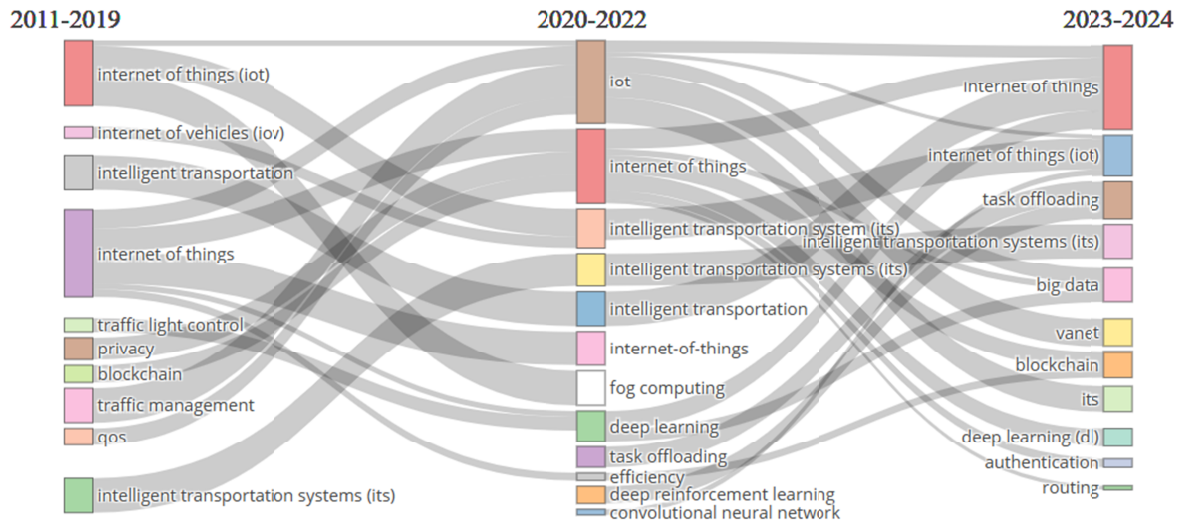
Keyword frequency and temporal co-occurrence analyses, shown in Fig. 7, reveal the conceptual composition of the field and its evolution across three phases.

The most frequent terms, Intelligent Systems with 441 occurrences (18.5%), Intelligent Transportation Systems with 394 occurrences (16.5%), and Internet of Things with 361 occurrences (15.1%), confirm the centrality of connectivity and intelligence as organizing concepts in IoT-ITS research. Terms such as Vehicle-to-Vehicle Communications with 83 occurrences (3.5%), Vehicular Ad Hoc Networks with 70 occurrences (2.9%), and Deep Learning with 64 occurrences (2.7%) indicate the field's gradual convergence toward decentralized and AI-augmented vehicular ecosystems. The presence of Network Security with 57 occurrences (2.4%) and Edge Computing with 46 occurrences (1.9%) further reflects growing attention to distributed processing and cybersecurity resilience.

Three temporal phases are evident. From 2011 to 2019, research concentrated on foundational IoT connectivity, quality-of-service architectures, and early privacy-preserving frameworks. From 2020 to 2022, the field diversified toward AI integration, fog computing, and task offloading, reflecting the maturation of edge intelligence as a design paradigm. In 2023 and 2024, Big Data, Blockchain, and VANETs emerged as dominant themes, indicating a shift toward secure, large-scale, and decentralized automation. Transformer-based models and large language models remain largely absent from the keyword clusters of earlier phases but show early signs of emergence in the most recent period. This pattern suggests an emerging research frontier that has not yet been systematically addressed in the IoT-ITS literature [15]. This gap motivates the future research directions discussed in Section 5.



(a) Keyword frequency distribution (2011–2024).



(b) Temporal evolution of research themes (2011–2024).

Figure 7: Thematic structure and evolution of IoT-enabled ITS research from 2011 to 2024: (a) keyword frequency distribution and (b) temporal progression of dominant research themes across three phases.

3.2 Science Mapping

Science mapping complements performance analysis by visualizing relational structures among authors, institutions, countries, and concepts [28]. The co-authorship and keyword co-occurrence networks presented in Fig. 8 reveal the collaborative geography and conceptual architecture of IoT-ITS scholarship.

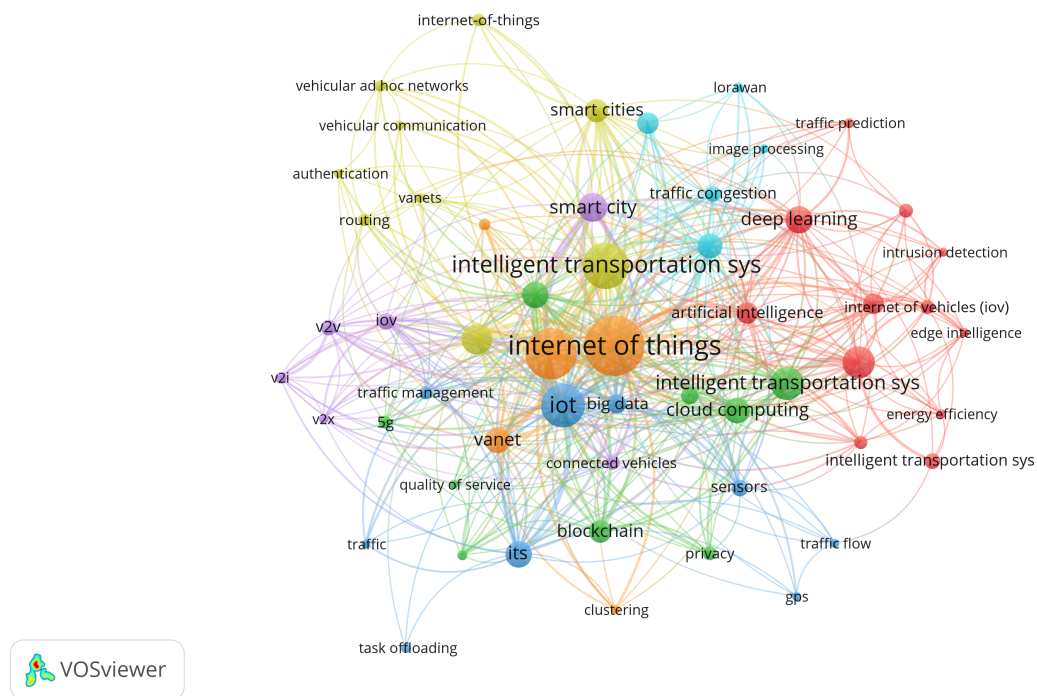
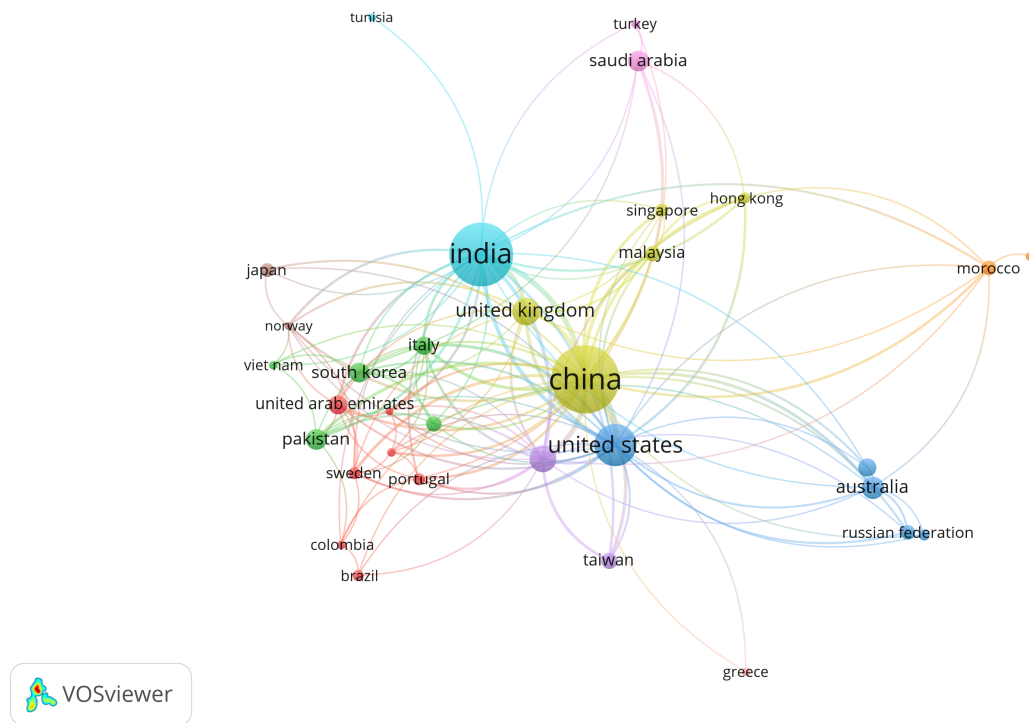


Figure 8: Science mapping of IoT-enabled ITS research from 2011 to 2024: (a) international co-authorship network and (b) keyword co-occurrence network showing major thematic clusters.

The co-authorship network identifies four geographically coherent clusters. The first cluster, led by China and connected with Russia, Norway, Finland, and Sweden, reflects research linkages between China

and Europe in vehicular communication and AI-enabled mobility. The second cluster, centered on India and connected with the United Kingdom, Bangladesh, and the United Arab Emirates, forms a collaboration corridor linking South Asia, the Middle East, and the United Kingdom, with emphasis on urban mobility and IoT security. The third cluster, comprising the United States, Canada, Australia, Hong Kong, and Japan, is associated with autonomous vehicular systems and advanced cybersecurity research. The fourth cluster, including Spain, Greece, and Colombia, reflects work on IoT-driven logistics and sustainable mobility in European and Latin American contexts. The near absence of African countries across these clusters reinforces the geographic coverage concern identified earlier and suggests a structural gap in the field's collaborative architecture.

The keyword co-occurrence network reveals four conceptual clusters. The central cluster, anchored by Internet of Things, Intelligent Transportation Systems, and Smart City, represents the integrative foundation of the field. The cluster containing Internet of Vehicles, Security, Deep Learning, and Machine Learning reflects the convergence of networked architectures, cybersecurity, and AI-driven analytics. Another cluster centers on vehicular communication protocols, including VANET and V2V, whereas a further cluster is associated with low-latency decentralized routing and autonomous mobility systems. The separation between AI-oriented terms and protocol-oriented terms suggests that communication-layer research and AI-based decision-making remain only partially integrated. This fragmentation has implications for the development of end-to-end intelligent vehicular systems that require coordination across sensing, communication, computation, and control layers.

Taken together, the bibliometric and science mapping analyses indicate that IoT-ITS has developed into a globally distributed and thematically layered research field. The field's center of gravity has shifted from foundational connectivity toward distributed intelligence, cybersecurity, and AI-driven automation. However, geographic imbalances in research production, the limited visibility of LLM and Transformer-based approaches in the keyword landscape, and the partial separation between AI-oriented and protocol-level research clusters highlight clear directions for future investigation.

4 Applications of IoT in ITS

IoT integration in ITS is commonly organized through four interdependent layers: Perception, Network, Processing, and Application, as shown in Fig. 9. Together, these layers transform raw transportation data into operational intelligence for real-time mobility management.

The *Perception Layer* collects vehicular, environmental, and infrastructure data through sensors, LiDAR, Global Positioning System (GPS), and embedded IoT devices, supporting accident detection, vehicle localization, and road condition monitoring. The *Network Layer* enables data exchange among vehicles, infrastructure, and control centers through 5G, Wi-Fi, and dedicated short-range communications (DSRC), supporting V2V, V2I, and V2X connectivity. The *Processing Layer* uses cloud platforms, edge and fog computing, and AI or Machine Learning (ML) algorithms to filter, analyze, and fuse high-frequency traffic data for congestion management, route optimization, and predictive maintenance. The *Application Layer* translates these analytical outputs into user-oriented services, including smart parking, adaptive signal control, public transport coordination, and emergency response. Collectively, these layers provide the operational foundation for scalable, data-intensive, and adaptive ITS.

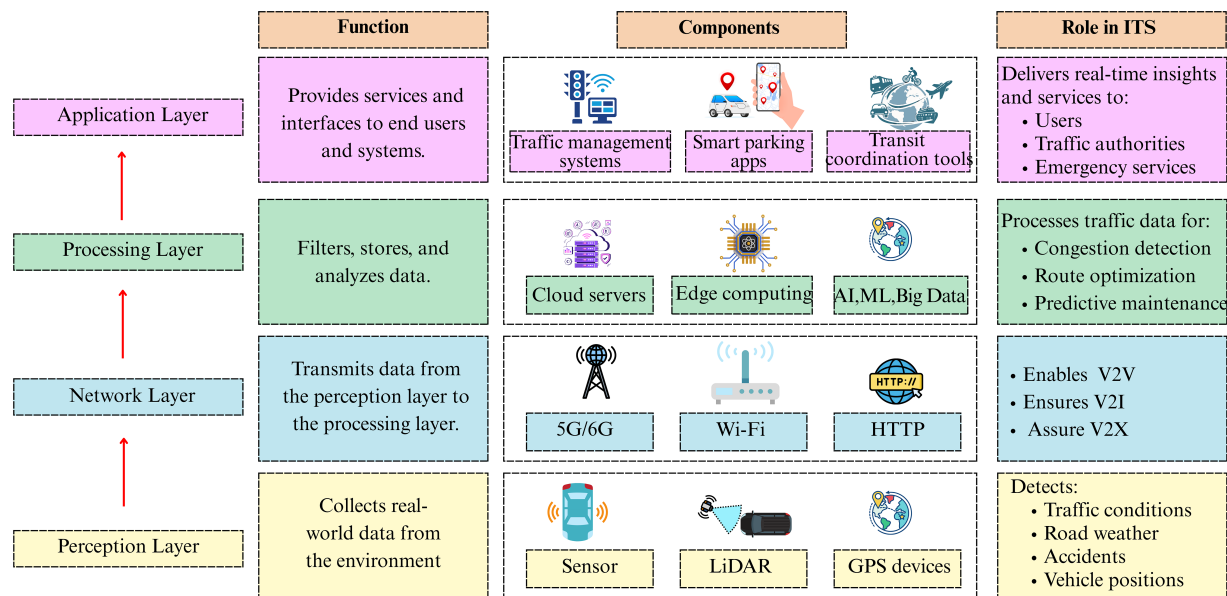


Figure 9: Layered architecture of IoT applications in ITS, illustrating data flow across the Perception, Network, Processing, and Application layers.

This review synthesizes IoT applications in ITS by focusing on emerging paradigms and enabling technologies that shape contemporary transportation innovation. The reviewed literature is organized into eight thematic domains:

- Cybersecurity and privacy
- Blockchain and decentralization
- Edge and fog computing for real-time data processing
- Traffic prediction and mobility optimization
- IoT-enabled architectures and frameworks
- Wireless communication protocols and V2X connectivity
- Federated, hybrid, and smart governance models
- Smart mobility and signal optimization

These domains capture the breadth of IoT-enabled innovation and the technical, operational, and governance challenges associated with large-scale ITS deployment. The discussion distinguishes between technically mature contributions supported by empirical validation and conceptual or simulation-based proposals that require further testing. This distinction provides a grounded assessment of deployment readiness for researchers, practitioners, and policymakers. A detailed synthesis of representative IoT-enabled ITS studies, including the problem addressed, IoT role, methodology, limitations, and future research directions, is provided in [Appendix A](#).

4.1 Cybersecurity and Privacy

Cybersecurity represents one of the most developed domains in IoT-ITS research, with a substantial body of work examining both attack vectors and defensive mechanisms. Stellios et al. [5] developed an early taxonomy of cyberattacks in IoT-based ITS, distinguishing direct, indirect, and subliminal threats and identifying infotainment systems as a key vulnerability. Sun et al. [31] applied the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (STRIDE) model to the

Internet of Vehicles (IoV), highlighting GPS spoofing and Sybil attacks and recommending multilayered defenses that combine intrusion detection with privacy-aware communication protocols.

Subsequent studies have advanced machine learning and cryptographic approaches to ITS security. Nie et al. [9] proposed a CNN-based intrusion detection system (IDS) that shifts computation from On-Board Units (OBUs) to Roadside Units (RSUs), achieving high detection accuracy under simulated DDoS conditions. However, the system was not validated against dynamic or adversarial attack patterns, which limits its applicability to evolving threat environments. Srinivas et al. [32] introduced UAP-BCIoT, a lightweight Elliptic Curve Cryptography (ECC)-based authentication scheme that uses fuzzy extractors to support biometric stability. Although the scheme achieves high throughput and low latency, its reliance on centralized control gateways constrains scalability in large vehicular networks.

Federated and blockchain-based models represent a further shift in ITS security design. Abdel-Basset et al. [10] developed FED-IDS, a federated deep learning intrusion detection framework that transfers the learning process from central servers to distributed vehicular edge nodes. The framework uses context-aware Transformer networks with redesigned encoder and decoder modules to learn spatiotemporal representations of vehicular traffic flows for multiclass attack classification. It also employs a consortium blockchain to coordinate federated training through delegated Byzantine Fault Tolerance (dBFT) consensus. In this design, roadside units act as miners that verify the quality of submitted local gradients against a common test set before aggregation, thereby excluding poisoned or low-quality updates. Evaluations on the TON_IOT and Car-Hacking datasets achieved 94.85% and 97.82% accuracy, respectively, and the framework maintained stable detection performance with up to 50% malicious participants. However, the authors acknowledge that supervised training requires large volumes of labeled vehicular data, while encryption, key generation, and consensus operations remain time-consuming. These constraints motivate further work on computationally efficient consensus mechanisms for real-time deployment.

Related studies have addressed secure access control and fog-enabled protection. Jin et al. [33] combined digital twins with multi-agent reinforcement learning for cyber-physical traffic control, reducing queue lengths by 40%. Gupta et al. [34] proposed ITS-ABACG, an attribute-based access control model that uses Message Queuing Telemetry Transport (MQTT) and contextual attributes, including location and velocity, to support efficient policy enforcement under simulation.

Lightweight encryption and privacy protection remain active research areas. Wu et al. [35] designed a fog-based authentication and key exchange protocol that provides forward secrecy and pseudonym privacy with low computational overhead. Ghane et al. [36] used differential privacy and pseudonym rotation to improve V2X anonymity while retaining 90% data utility. Kang et al. [37] addressed location privacy through entropy-based trajectory obfuscation in cloud and edge IoV systems, although reliance on synthetic data limits external validity.

The security architectures developed in this domain may also inform adjacent intelligent transportation applications. For example, CNN-based and federated intrusion detection frameworks designed for vehicular networks can support the security requirements of autonomous driving perception pipelines and traffic camera-based anomaly detection [9]. This broader applicability underscores the relevance of IoT-ITS security research for computer vision-dependent transportation systems.

Persistent gaps include post-quantum resilience, real-world adversarial validation, and privacy-preserving federated architectures for heterogeneous vehicular networks. Future work should prioritize scalable and adaptive security designs that can protect real-time vehicular ecosystems under high-mobility conditions.

4.2 Blockchain and Decentralization

Blockchain has emerged as an important enabler of decentralized and secure ITS by supporting immutability, distributed trust, and transparent coordination. These properties are particularly relevant for addressing vulnerabilities in centralized vehicular networks as ITS increasingly integrates IoT sensors, edge computing, and vehicular communication. However, many blockchain-based ITS contributions remain at the architectural or simulation stage, and the gap between conceptual designs and field-validated systems remains a defining limitation of this domain.

Kumari et al. [4] proposed a tri-layer architecture that integrates blockchain, IoT, and 6G for UAV-assisted traffic monitoring and emergency routing. Although the framework is conceptually well developed, it does not provide empirical validation of latency, interoperability, or energy efficiency. Mollah et al. [38] introduced a multilayer blockchain-based ITS model combining Delegated Proof of Stake (DPoS), Directed Acyclic Graphs (DAGs), Software-Defined Networking (SDN), and edge computing for electric vehicle charging and ride-sharing. However, its real-time performance and field deployment remain unexplored.

For secure vehicular communication, Lei et al. [6] replaced centralized certificate authorities with distributed Security Managers using IEEE 802.11p, ECIES, and ECDSA. Simulations over a nine-domain Beijing topology showed low-latency authentication and efficient rekeying, although privacy-preserving authentication was not addressed. Humayun et al. [39] developed BCTLF, a blockchain-IoT logistics framework that uses smart contracts for decentralized routing and asset tracking within SmaTaxi and TradeLens. However, privacy safeguards and large-scale testing were not examined.

In cybersecurity, Abdel-Basset et al. [10] proposed FED-IDS, a federated deep learning intrusion detection framework in which a context-aware Transformer network learns spatiotemporal representations of vehicular traffic flows. The framework uses consortium blockchain-managed federated training with delegated Byzantine Fault Tolerance (dBFT) consensus to secure distributed model updates across vehicular edge nodes. Evaluations on the TON_IoT and Car-Hacking datasets demonstrated strong attack detection and privacy preservation. Nevertheless, consensus and encryption overhead remain time-consuming, which constrains real-time deployment.

Key engineering challenges across this domain include computational overhead from consensus mechanisms, the absence of unified cross-domain communication standards, and insufficient attention to energy costs in high-throughput vehicular settings. Future research should prioritize lightweight consensus protocols, post-quantum cryptographic schemes, and integration with edge and federated computing frameworks. These directions are necessary to bridge the gap between the theoretical promise of blockchain and its operational feasibility in large-scale ITS.

4.3 Edge and Fog Computing for Real-Time ITS

Edge and fog computing are central to real-time and scalable ITS because they process data closer to the source, reduce latency, improve energy efficiency, and decrease reliance on centralized cloud infrastructure. This domain includes several empirically grounded contributions in IoT-ITS, particularly studies that report validated system-level performance metrics.

Ke et al. [3] developed a hybrid edge-cloud smart parking system using Raspberry Pi 3B and TensorFlow Lite for on-device object detection. The system achieved 95.6% accuracy and reduced daily data transmission from 86 GB to 70 MB. However, its 1 frame per second (FPS) throughput limited real-time responsiveness in high-density environments. Wan et al. [40] proposed a bandwidth-efficient video analytics pipeline that combines redundancy elimination with a lightweight YOLOv3 model, achieving 52 FPS at 95%

precision. Nevertheless, Mobile Edge Computing (MEC) integration and robustness to environmental noise remained limited.

Architectural optimization has also received considerable attention. Yu et al. [41] proposed a fog-cloud-IoV (FC-IoV) framework using an ILP-based placement heuristic that improved cost efficiency under realistic topologies, although static mobility assumptions constrained its generalizability. Yuvaraj et al. [42] integrated DNNs and blockchain into a Smart City Management System for optimizing electric waste-collection vehicles, reducing latency and energy use. However, adaptive learning and field testing were not included.

Security-oriented studies further demonstrate the role of edge intelligence in ITS. Alladi et al. [43] introduced a CNN-LSTM intrusion detection model for edge devices, achieving a 96.75% F1-score on the VeReMi dataset. Its fixed sliding-window architecture, however, limits adaptability to novel or gradually evolving attack patterns. Sodhro et al. [14] proposed QGSRA, a QoS-aware edge-IoT framework for V2V multimedia communication using convex optimization and IEEE 802.11p. The framework achieved sustainable performance but lacked ML integration and real-world validation.

At the system level, Yu et al. [44] proposed a hierarchical vehicular cloud using game-theoretic resource allocation and virtual machine migration to reduce latency, although privacy and energy dimensions were not addressed. Ouallane et al. [45] reviewed AI-IoT-integrated ITS through a three-tier Vehicular Fog Computing (VFC) model, highlighting its potential while noting limited benchmarking. Ali et al. [46] demonstrated a Geographically Distributed Fog (GDF) architecture that reduced latency by 40% through mobility-aware orchestration. Al-Dweik et al. [47] introduced SERSU, a real-time roadside advisory system using Long Term Evolution (LTE) and Radio Frequency (RF) links, although validation was limited to laboratory conditions.

The lightweight inference pipelines and distributed misbehavior detection frameworks developed in this domain are also relevant to autonomous driving perception stacks and traffic camera-based anomaly detection systems. These applications face similar constraints related to latency, bandwidth, and hardware capacity [40,43]. Future research should advance adaptive fog orchestration, hybrid AI architectures, security-aware edge intelligence, and large-scale field validation.

4.4 Traffic Prediction and Mobility Optimization

Traffic prediction has shifted from rule-based and conventional statistical methods toward deep learning architectures capable of capturing spatiotemporal dependencies across large sensor networks. Several contributions in this domain have been validated using real-world datasets, making it one of the more empirically active areas of IoT-ITS research.

Akbar et al. [11] developed a scalable real-time framework that combines Complex Event Processing (CEP) with Adaptive Moving Window Regression (AMWR), implemented using Node-RED, Apache Kafka, scikit-learn, and Esper. The system achieved a Mean Absolute Percentage Error (MAPE) of 3% in Madrid IoT traffic trials. However, limited multimodal support and reliance on static rule bases reduce its adaptability under volatile traffic conditions. Chu et al. [7] proposed MultiConvLSTM, a deep learning architecture for Origin-Destination (OD) flow prediction in Mobility-on-Demand (MoD) systems. Using OD tensors and residual learning, the model outperformed Autoregressive Integrated Moving Average (ARIMA), CNN, and Long Short-Term Memory (LSTM) benchmarks on the NYC taxi dataset, although interpretability and computational efficiency under operational constraints remained unresolved concerns.

Liu et al. [48] introduced TSDNet, a three-stage dehazing model with Multi-Scale Spatial Attention for vehicle detection under adverse visual conditions. The model improved mean Average Precision by

3.2% and maintained 30 FPS, although accuracy declined under severe occlusion, illustrating the sensitivity of vision-based ITS to environmental variability. Qiu et al. [49] proposed Nei-TTE, a GRU-based travel-time estimation model that uses fine-grained temporal features and neighborhood-level road-segment representations from taxi GPS trajectories. This study is relevant to IoT-enabled ITS because taxi GPS streams function as connected mobility data for smart-city traffic prediction and travel-time forecasting. Evaluated on the Porto taxi dataset, the model achieved a reported MAPE of 0.070%. However, its reliance on historical trajectory patterns limits responsiveness to non-recurrent disruptions such as crashes, road closures, and sudden incidents. Zhou et al. [50] introduced R-STAGNN, which integrates Graph Attention Networks (GAT), Gated Recurrent Units (GRUs), and reinforcement learning for adaptive spatiotemporal forecasting. Validated on METR-LA and PEMS-BAY, the model achieved high predictive accuracy, but sensitivity to sensor faults and centralized computation remain barriers to edge deployment.

A critical gap across these contributions is the absence of systematic comparison between Transformer-based models and LLM-augmented traffic prediction systems against the CNN, GRU, and Graph Neural Network (GNN) architectures reviewed here [15]. Given the potential of attention mechanisms to capture long-range spatiotemporal dependencies, such comparative evaluation represents an important research priority for IoT-enabled ITS.

4.5 IoT-Enabled Architectures and Frameworks

IoT-ITS architectures vary considerably in maturity, ranging from empirically evaluated modular deployments to conceptual integration frameworks. Distinguishing between these levels of maturity is important for assessing which contributions are closer to operational adoption and which require further empirical validation.

Iyer [51] developed a taxonomy that links AI techniques to ITS subsystems across global and Indian application contexts. The framework supports modular system design, although it lacks empirical benchmarking and stakeholder participation. Ullah et al. [52] proposed an AI-IoT convergence architecture that integrates UAV relaying, LSTM-based traffic prediction, and edge-based distributed decision-making. However, the evaluation remains conceptual and does not include prototype implementation. These contributions are therefore best understood as design references rather than validated operational systems.

Muthuramalingam et al. [53] proposed s-ITS, a modular architecture that combines Vehicular Ad Hoc Networks (VANETs) based on IEEE 802.11p, Radio Frequency Identification (RFID)-based vehicle identification, and big data analytics. The system was evaluated in Chennai and reported favorable Root Mean Square Error (RMSE), MAPE, and packet delivery metrics, although real-time streaming and city-scale scalability were not demonstrated. Guerrero-Ibanez et al. [54] developed a layered ITS model that integrates connected vehicles, IoT sensors, and vehicular cloud computing through DSRC and LTE. However, the absence of edge AI and federated trust mechanisms limits its adaptability in dynamic urban networks.

Belhajem et al. [55] proposed a hybrid localization framework that combines low-cost IoT sensors, Support Vector Machine (SVM)-based drift correction, and an Extended Kalman Filter. The framework reduced RMSE by 94% on a 4.2 km real-world route, although reliance on synthetic GPS outage profiles constrains real-world generalizability. Liang [56] introduced an Ant Colony Optimization-enhanced SVM model for real-time accident detection using heterogeneous sensor data. The model achieved high accuracy but did not incorporate V2X communication support.

The most consistent limitation across this domain is the gap between modular design and operational scalability. Future research should prioritize standardized communication interfaces, adaptive AI coordination, and the transition from campus-scale or corridor-level pilots to city-wide deployments.

4.6 Wireless Communication Protocols and V2X

V2X communication is a foundational component of modern ITS, enabling real-time connectivity among vehicles, infrastructure, users, and control systems [57]. Research in this domain covers protocol benchmarking, routing optimization, edge-integrated communication, and intrusion-resilient network design.

Datta et al. [58] evaluated low-power wireless protocols, including Bluetooth LE, Bluetooth Classic, ZigBee, LoRa, and nRF24, across varying terrains for V2I and V2IoT communication. LoRa demonstrated stronger range stability, while Bluetooth LE performed well in dense urban settings. However, the study did not examine mesh networking, SDN integration, or 5G and 6G compatibility, which are important requirements for next-generation ITS. Zhang and Lu [59] compared Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) in an IoT-integrated urban framework and found that AODV performed better in packet delivery and delay under high-mobility conditions. Lin et al. [13] developed SCAPP, an SDN-IoT congestion-aware routing protocol, reporting improvements in delay and reliability under simulation. However, its adaptability under real mobility conditions was not evaluated.

Alladi et al. [43] proposed an edge-deployable CNN-LSTM intrusion detection model that achieved high classification accuracy on the VeReMi benchmark. However, its fixed-window architecture limits adaptability under sustained or evolving attack patterns. Kaur et al. [60] optimized SDN controller placement in the Internet of Autonomous Vehicles (IoAV) using a multi-objective heuristic to minimize latency and energy use, but the approach was not validated under dynamic mobility conditions. Yan et al. [61] introduced ST-ChebGNN, a spatiotemporal Chebyshev Graph Neural Network for edge-based traffic forecasting, reporting strong accuracy on PeMSD4 and PeMSD8. Nevertheless, its reliance on static graph structures limits adaptability under changing road topology.

The most pressing gaps in this domain include multi-protocol interoperability across DSRC, C-V2X, and 5G NR-V2X standards; adaptive AI-driven management of communication stacks; and privacy-preserving mechanisms for real-time vehicular data exchange.

4.7 Federated, Hybrid, and Smart Governance Models

Federated and hybrid governance models represent an emerging but strategically important domain within IoT-ITS. Contributions in this area emphasize system-level integration among simulation environments, real-world sensing, and adaptive traffic control.

Zhu et al. [62] developed the Parallel Transportation Systems (PTS) framework based on Artificial Societies, Computational Experiments, and Parallel Execution (ACP theory). By coupling IoT sensor networks and social data with artificial transport simulations, PTS establishes a continuous feedback loop between simulated and physical traffic systems. Field deployments in Binzhou and Qingdao demonstrated measurable performance improvements at urban intersections using Gaussian Mixture Models, Parallel Driving Policies, and Adaptive Dynamic Programming for traffic optimization. However, scalability under network heterogeneity and sensitivity to noise in social data streams remain documented limitations. PTS is one of the few governance-oriented IoT-ITS contributions supported by real-world field validation, making it a useful benchmark for hybrid simulation-control frameworks.

Future governance research should address federated decision-making protocols, cross-agency data-sharing frameworks, and the integration of explainable AI into transportation management systems. These directions can support more transparent, accountable, and adaptive mobility governance.

4.8 Smart Mobility and Signal Optimization

Smart mobility and signal optimization encompass task offloading, adaptive routing, low-cost sensing, and pedestrian-aware signal control [63]. This domain includes both empirically validated prototypes and simulation-based proposals at different stages of deployment readiness.

Boukerche and Soto [64] developed a mobility-aware task offloading framework for Vehicular Edge Computing (VEC), combining Recurrent Neural Networks for trajectory prediction with an Artificial Bee Colony algorithm for latency and energy optimization. Implemented through a three-stage Mobility-Oriented Retrieval Protocol using 5G-V2X and LTE-V, the framework achieved measurable latency and energy gains in Simulation of Urban Mobility (SUMO), NS-3, and EdgeCloudSim simulations. However, the absence of real-world 5G slicing tests and formal security validation remains a primary barrier to deployment. Goswami et al. [65] proposed a routing protocol based on Q-learning and fuzzy logic, reporting improvements of up to 30% in packet delivery and energy efficiency under simulation. The approach, however, lacks empirical validation and does not incorporate trust mechanisms.

Feng et al. [66] introduced MagMonitor, a low-cost vehicle detection system using tri-axial magnetic sensors, ARM Cortex-M microcontrollers, and BLE communication. With a unit cost of \$30–\$50, the system achieved sub-5% speed estimation error at speeds up to 70 km/h and supported offline operation. Performance degraded under multilane vehicle occlusion, indicating the need for multimodal sensor fusion. Its low-cost design makes it particularly relevant for resource-constrained deployment contexts where vision-based sensing infrastructure is unavailable. Pau et al. [67] developed a fuzzy logic-based pedestrian signal system that uses IoT sensors to dynamically adjust green phase durations, demonstrating reduced pedestrian waiting time in simulation. However, static rule structures and idealized sensing assumptions limit its applicability to real mixed-traffic environments.

Collectively, IoT integration in ITS, from federated governance to smart mobility and signal optimization, supports real-time sensing, adaptive control, and efficient urban management, as shown in Fig. 10. These advances indicate a broader movement toward data-driven, resilient, and sustainable mobility ecosystems. Across the eight domains reviewed in this section, a consistent pattern emerges: cybersecurity, edge computing, and traffic prediction contain the highest concentration of empirically validated contributions, whereas blockchain, federated governance, and signal optimization remain largely simulation-based. Bridging this validation gap through real-world pilots, standardized benchmarks, and cross-domain integration remains a central challenge for large-scale IoT-ITS deployment.

5 Challenges and Future Research Directions

The integration of IoT into ITS creates substantial opportunities for intelligent, data-driven mobility, but large-scale deployment remains constrained by persistent and interrelated challenges. This section examines these challenges across five dimensions and outlines emerging research directions that define the next phase of IoT-enabled ITS development.

5.1 Technological Challenges in IoT-Enabled ITS

Interoperability and standards. Transportation systems rely on heterogeneous communication protocols, including Wi-Fi, Bluetooth, Zigbee, and Cellular V2X, which can produce fragmented architectures, impede data exchange, and increase integration costs. Although emerging frameworks such as International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 30161 aim to establish common interfaces, practical plug-and-play compatibility across multi-vendor platforms remains limited. The absence of unified data formats also continues to constrain cross-system scalability.

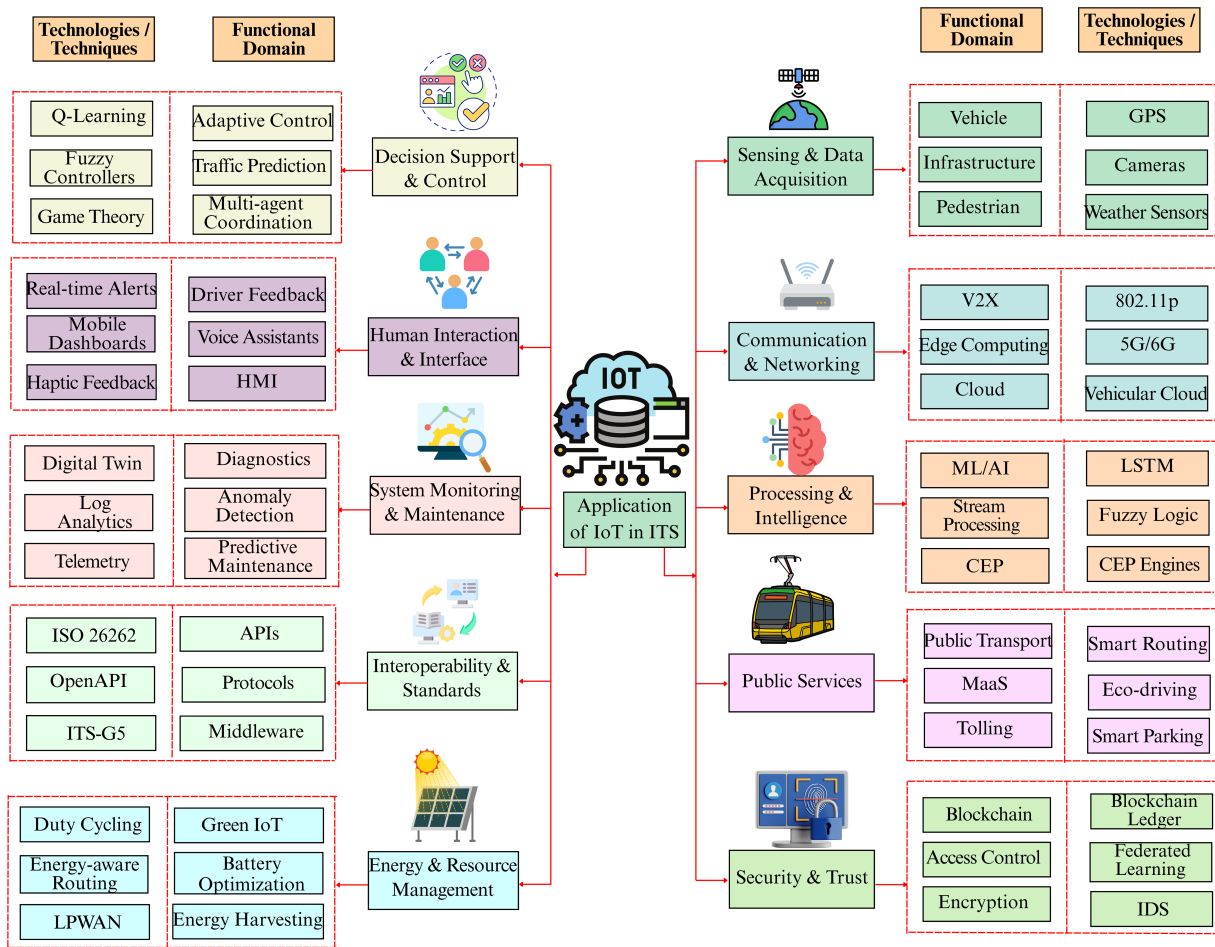


Figure 10: Functional architecture of IoT applications in ITS showing integrated sensing, communication, processing, control, and security layers for real-time, resilient mobility. Note: 5G/6G, Fifth Generation and Sixth Generation cellular networks; 802.11p, IEEE wireless access standard for vehicular environments; AI, Artificial Intelligence; API, Application Programming Interface; CEP, Complex Event Processing; GPS, Global Positioning System; HMI, Human Machine Interface; IDS, Intrusion Detection System; ISO 26262, International Organization for Standardization road vehicles functional safety standard; ITS-G5, Intelligent Transport Systems operating in the 5.9 GHz band; LPWAN, Low Power Wide Area Network; LSTM, Long Short-Term Memory; MaaS, Mobility as a Service; ML, Machine Learning; V2X, Vehicle-to-Everything.

Scalability. Deployments involving large numbers of connected vehicles, roadside units, and sensors place substantial demands on network capacity and computing infrastructure. Hierarchical and distributed architectures based on fog and edge computing can improve scalability, but they require effective load balancing, data synchronization, and device management to maintain system performance as network size increases.

Latency and real-time responsiveness. Safety-critical applications, such as collision avoidance, require near-instantaneous system response. Centralized cloud architectures can introduce unacceptable latency for these use cases. Edge computing reduces response time by processing data at or near the source, while 5G and 6G networks with multi-access edge computing are expected to further support low-latency operation. However, coordinating distributed intelligence across edge and cloud layers remains technically complex.

Energy efficiency. IoT nodes deployed in vehicles and roadside environments operate under strict power constraints. Continuous sensing and high-frequency communication can drain limited battery capacity and increase maintenance requirements. Energy-aware routing, duty cycling, and low-power wide-area networks (LPWAN) are therefore essential for extending device lifetime. Research on energy harvesting and self-sustaining sensor nodes also offers longer-term pathways for sustainable large-scale IoT operation.

Cybersecurity and privacy. Pervasive IoT connectivity expands the attack surface of transportation infrastructure. Common threats include denial-of-service attacks, GPS spoofing, Sybil attacks, and unauthorized access to vehicular networks. Lightweight encryption, blockchain-based authentication, and secure firmware management are important mitigation strategies, although achieving strong security without compromising latency or energy efficiency remains an open engineering challenge. Privacy risks arising from continuous location and behavioral data collection also require anonymization and governance mechanisms aligned with the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) standards.

5.2 Infrastructure and Deployment

Legacy system integration. Many cities operate aging traffic control, transit, and tolling systems with proprietary interfaces that are difficult to integrate with modern IoT components. Bridging these legacy platforms requires cross-agency coordination and substantial investment, while also creating the risk of isolated smart infrastructure islands that remain disconnected from broader mobility networks [68].

Connectivity disparities. IoT infrastructure is concentrated in well-funded urban areas, whereas rural and low-income regions often remain underserved [69]. Limited 4G and 5G coverage constrains real-time communication in parts of Latin America, Africa, and the Middle East. Satellite IoT, mesh networking, and roadside edge processing offer partial remedies, but equitable connectivity remains a structural challenge that requires coordinated investment.

Sensor reliability and maintenance. Transport sensors operate under demanding conditions, including weather exposure, vibration, and mechanical wear. Sensor failures reduce data accuracy and degrade service reliability [70,71]. Predictive maintenance, hardware redundancy, and self-healing network protocols can improve resilience, although operational costs remain high for many public agencies.

Deployment cost and pilot-to-scale transition. IoT-based ITS requires substantial upfront investment, and funding constraints continue to limit adoption even when long-term benefits are evident [72]. Many initiatives remain confined to small-scale pilots that do not expand citywide because of technical heterogeneity, institutional barriers, and the absence of stable funding mechanisms [70,73,74]. Scalable deployment requires coordinated governance, standardized procurement, workforce capacity building, low-cost sensing strategies, and shared infrastructure models [75].

5.3 Data Management and Analytics

Volume, velocity, and integration. Urban IoT networks generate large volumes of data from cameras, vehicles, and environmental sensors. Centralized processing faces bandwidth and storage constraints, which motivates edge-cloud collaboration for local filtering and aggregated transmission [28,76]. Data integration is further complicated by inconsistent formats and the absence of shared taxonomies across agencies and vendors [77,78]. Standards such as Data Exchange (DATEX) II and General Transit Feed Specification (GTFS) improve data structure, but semantic interoperability across domains remains unresolved [79,80].

Real-time analytics and data quality. The operational value of IoT in ITS depends on timely inference for applications such as adaptive signal control, hazard detection, and incident response [81,82]. Reliable

real-time analytics at the edge requires streaming architectures and AI models capable of rapid inference under resource constraints. Data quality is a parallel concern because sensor noise, drift, and data loss can degrade model inputs. Fusing heterogeneous data streams from speed sensors, video feeds, and social media also requires robust uncertainty handling [83]. Bias in connected vehicle data may further distort system outputs, highlighting the need for governance frameworks and balanced sampling strategies to ensure representativeness.

Privacy, ownership, and standardization. Transport data can encode sensitive personal traces. Balancing analytical utility with privacy protection requires anonymization, differential privacy, and encryption aligned with GDPR and CCPA [84]. Ownership of IoT-generated data remains contested among drivers, automakers, and public agencies [85]. Although the EU Data Act clarifies certain rights, it does not fully resolve tensions between commercial interests and public benefit. The lack of consistent performance metrics also limits comparability across deployments. Unified Key Performance Indicator (KPI) standards, including congestion indices and emission benchmarks, are being developed by ISO, IEEE, and ITS America [86].

5.4 Policy and Governance

Regulatory frameworks. Technological innovation often outpaces regulatory development in IoT-enabled ITS. The debate between DSRC and C-V2X for the 5.9 GHz band illustrates the difficulty of aligning spectrum policy with competing industry approaches [87]. Divergent autonomous vehicle legislation and data-logging requirements across jurisdictions further contribute to regulatory fragmentation [88]. International bodies, including ISO, IEEE, the European Telecommunications Standards Institute (ETSI), and SAE International (SAE), are defining communication and cybersecurity standards [89], while the EU Data Act and AI Act provide proactive governance models that other regions are beginning to consider [70]. However, regulatory capacity and cross-border enforcement remain uneven.

Liability, privacy, and public-private governance. Liability in IoT-assisted or autonomous transport incidents remains legally unresolved because accountability may span drivers, manufacturers, software providers, and infrastructure operators [90,91]. Continuous sensing also raises surveillance risks that require privacy-by-design principles and legally defined limits on data collection, retention, and use [92,93]. Smart mobility projects increasingly depend on private technology partners, requiring governance frameworks that protect the public interest, prevent vendor lock-in, and ensure inclusive access for elderly and disabled users [94–96]. Cross-jurisdictional coordination through national ITS architectures and United Nations Economic Commission for Europe (UNECE) WP.29 cybersecurity regulations provides a partial harmonization framework, although implementation remains inconsistent [97,98].

5.5 Societal and Economic Impacts

Public trust and equity. Approximately half of surveyed users are willing to share IoT mobility data for public benefit, but trust in government data stewardship remains lower than trust in non-profit institutions [99,100]. Transparency, visible performance improvements, and proactive breach communication are central to maintaining public confidence. Equity is a parallel concern because the benefits of IoT-enabled ITS often concentrate in high-income urban areas and among users with access to advanced vehicles or smartphones. Rural and low-income populations therefore risk systematic exclusion [101,102]. Inclusive policy design, subsidized access, and accessible interface standards are necessary to support a more equitable distribution of mobility benefits.

Economic and environmental sustainability. IoT-enabled ITS requires substantial capital investment but can generate long-term returns through congestion reduction, fuel savings, and avoided healthcare costs [103,104]. Environmental benefits arise from optimized routing, smoother traffic flow, and smart grid

integration for Electric Vehicle (EV) charging [105]. However, device manufacturing, data center energy consumption, and electronic waste can partially offset these gains [106]. Lifecycle analyses indicate that long-term operational efficiency can outweigh production-phase impacts, but green IoT practices, including low-power hardware design and lifecycle assessment frameworks, remain essential for sustainability at scale.

Workforce and safety. IoT adoption is reshaping transport labor markets by increasing demand for data analytics, cybersecurity, and systems engineering skills while reducing reliance on some traditional driving and operations roles [107]. Phased deployment, reskilling programs, and coordinated labor policy are needed to manage these transitions. Safety improvement remains a primary societal justification for ITS investment. Collision avoidance, adaptive signaling, and automated emergency response can reduce crash risk and improve emergency management [108]. However, high-profile incidents involving autonomous systems underscore the need for rigorous validation, fail-safe design, and transparent incident reporting.

5.6 Future Research Directions

Research on IoT-enabled ITS is converging toward more adaptive, secure, and decentralized paradigms. The following directions represent major research frontiers for the next phase of the field, as summarized in Table 4.

Table 4: Emerging technologies and approaches in ITS: key applications and addressed challenges.

Emerging Technology/Approach	Key Applications in ITS	Challenges Addressed
Digital Twins (DT)	Real-time virtual models of transportation networks for simulation, predictive analysis, and scenario testing. For instance, a city DT can simulate traffic flow and incidents with live data to optimize signal plans or emergency responses [33].	- Integrates diverse IoT data for a holistic view (interoperability) - Enables real-time decision-making support and what-if analyses (uncertainty mitigation) - Aids in predictive maintenance via simulation of asset degradation and failure (asset reliability).
Federated Learning & Distributed AI	Collaborative machine learning across vehicles/infrastructure without centralizing data. For example, connected cars jointly train AI models for hazard detection by sharing updates, not raw data [4].	- Preserves data privacy (privacy-aware AI) - Reduces network load (scalability) - Enhances model robustness while avoiding bias (ethical AI).
Vehicular Edge Computing & On-board AI	Utilizing vehicles and roadside units as computational nodes. Examples include on-board vision systems for autonomous driving and edge servers analyzing local traffic feeds for incident detection [14].	- Ensures low-latency decision-making (safety-critical) - Operates independently of the cloud (resilience) - Offloads computation to distributed nodes (scalability).
Blockchain and Distributed Ledger	Secure and decentralized data sharing, e.g., blockchain-based traffic event logging, smart contracts for tolls or parking, and identity management in V2X systems [38].	- Enhances data integrity and tamper resistance (security) - Builds stakeholder trust (transparency) - Supports trusted autonomous transactions (interoperable services).
Quantum Computing & Quantum Security	Quantum algorithms for optimizing traffic networks, logistics, and signal control. Quantum encryption, including Quantum Key Distribution (QKD), can support secure communications [109].	- Addresses large-scale computational challenges (optimization) - Introduces future-proof encryption methods (cybersecurity) - Improves precision in synchronization and sensing (accuracy).

(Continued)

Table 4 (continued)

Emerging Technology/Approach	Key Applications in ITS	Challenges Addressed
Large Language Models (LLMs) for ITS	Leveraging advanced language-based AI for multimodal traffic data interpretation, incident detection, natural-language interfaces for operators, and integration with IoT-driven digital twins. For example, LLM copilots can summarize real-time traffic events and recommend adaptive control measures [15,110].	• Harmonizes heterogeneous IoT and V2X data into unified semantic representations (interoperability) • Provides interpretable and human-centered decision support (explainability) • Facilitates adaptive control and scenario reasoning through natural-language interaction (resilience and inclusivity).

Digital twins for transportation. Digital twin (DT) technology connects virtual and physical transport systems through real-time IoT data, enabling continuous simulation, predictive analysis, and what-if scenario evaluation before real-world implementation. DTs can support anomaly detection by comparing live sensor data with predictive baselines and can facilitate asset lifecycle management through simulated degradation modeling. Effective DT deployment requires reliable 5G connectivity, edge computing, and standardized data interfaces. The next generation of AI-driven DTs is expected to move toward semi-autonomous decision-making, in which models can recommend and execute adaptive control actions with limited operator intervention.

Federated learning and collaborative AI. Federated learning (FL) enables model training across distributed vehicles and infrastructure nodes without centralizing raw data, thereby addressing privacy concerns associated with large-scale IoT data collection. Relevant applications include cooperative perception, localized traffic prediction, and privacy-preserving anomaly detection. However, FL faces challenges related to model convergence under heterogeneous data distributions and robustness against adversarial participants. Federated averaging, differential privacy, and secure multi-party computation remain active areas of methodological development. Future ITS architectures are likely to integrate FL with edge AI at scale, enabling decentralized collective learning while preserving data security and communication efficiency.

Vehicular edge computing and on-board AI. Vehicular Edge Computing (VEC) envisions vehicles and roadside units as distributed computational nodes capable of local decision-making without dependence on cloud latency. On-board AI supports safety-critical functions such as sensor fusion, object detection, and path planning. Cooperative perception systems further extend situational awareness by sharing local model outputs across vehicles. Key research challenges include consensus mechanisms for decentralized agents, consistency under intermittent connectivity, and safe fallback operations during communication disruptions.

Blockchain and decentralized trust. Blockchain provides tamper-evident infrastructure for vehicular data exchange, identity management, and automated transactions. Its potential applications include authenticated event logging, smart contract-based tolling, and transparent logistics tracking. The central engineering challenges are scalability, consensus overhead, and the fact that blockchain can ensure data integrity but cannot verify the correctness of the underlying sensor inputs. Permissioned, high-throughput ledgers and lightweight consensus algorithms represent the most promising near-term directions for ITS deployment.

Quantum computing and communications. Quantum technologies intersect with ITS through three distinct paradigms that differ in mechanism, maturity, and security function and should not be treated as interchangeable. The first paradigm, quantum annealing, is a computational approach directed toward combinatorial optimization problems, including large-scale traffic signal coordination, logistics routing,

vehicle scheduling, and charging allocation. For example, Inoue et al. [109] demonstrated the application of a D-Wave quantum annealer to traffic signal coordination on a large-scale city grid, achieving better performance than conventional local control and classical simulated annealing. However, current quantum optimization applications in ITS remain exploratory because available hardware and algorithms still face scalability, noise, embedding, and benchmarking limitations.

The second paradigm, Quantum Key Distribution (QKD), is a communication-security technology that uses quantum physical properties to establish secret keys between communicating parties. Its relevance to ITS lies in securing critical V2I and infrastructure communication links, rather than solving traffic optimization problems. Fowler et al. [111] implemented a free-space optical QKD system within a live V2I testbed, where quantum-derived keys supported secure V2I communication and a zero-trust protocol rejected spoofed messages from a compromised roadside device. Stavdas et al. [112] further proposed a software-defined networking architecture that integrates QKD into the end-to-end V2I communication path. These studies indicate that QKD is promising for fixed or semi-fixed ITS infrastructure links, although free-space deployment remains constrained by line-of-sight requirements, environmental sensitivity, key management complexity, cost, and mobility-related handover issues.

The third paradigm, post-quantum cryptography (PQC), is an algorithmic defense based on classical cryptographic schemes designed to resist quantum attacks while remaining deployable on conventional hardware. PQC is directly relevant to ITS because many existing V2X and V2I security schemes rely on elliptic-curve cryptography, as reflected in the ECC-based V2I authentication schemes of Ali et al. [113] and Wu et al. [35]. These primitives would become vulnerable in the presence of a sufficiently powerful quantum computer running Shor's algorithm. Addressing this transition, Dharminder et al. [114] developed a post-quantum conditional privacy-preserving authentication scheme for edge-based vehicular communication. The scheme uses the hardness of the short integer solution problem in random lattices while supporting batch verification and revocation. In summary, quantum annealing addresses computation and optimization, QKD addresses key establishment through quantum communication, and PQC strengthens vehicular security protocols against quantum-era adversaries.

Future research should evaluate these three pathways under realistic ITS conditions rather than treating them as interchangeable solutions. For quantum annealing, studies should benchmark performance against classical optimization, reinforcement learning, and metaheuristic methods for traffic signal coordination, routing, logistics, and charging management, with attention to scalability, computation time, and real-time feasibility. For QKD, future work should examine deployment in fixed transport infrastructure such as RSU corridors, toll plazas, tunnels, rail backbones, and traffic control centers, while quantifying key generation rate, weather sensitivity, line-of-sight limitations, handover performance, and cost. For PQC, research should prioritize migration strategies for V2X and IoV security frameworks by testing lattice-based and hash-based schemes on resource-constrained OBUs, RSUs, and edge nodes. Particular attention should be given to verification latency, signature size, bandwidth overhead, certificate revocation, and interoperability with current V2X standards. Overall, quantum-resilient ITS research should pursue hybrid architectures that combine QKD-secured infrastructure links, PQC-based vehicle authentication, and scalable edge-cloud security frameworks for future intelligent mobility systems.

Integration of IoT, LLMs, and ITS. The convergence of IoT sensing with large language models (LLMs) represents an emerging frontier for intelligent mobility [15,115]. LLMs can function as an integrative reasoning layer that transforms continuous multimodal IoT data streams into actionable decisions and human-interpretable explanations. Potential applications include IoT-driven digital twins in which LLMs interpret system states and generate natural-language recommendations for operators, multimodal traffic data harmonization across V2X feeds and sensor outputs, and human-in-the-loop governance interfaces that

allow operators to query and refine system logic through natural language. However, LLM-based approaches must be systematically benchmarked against established ML methods, including CNNs, GRUs, and GNNs, under real-time latency constraints before deployment suitability can be established. Key research challenges include low-latency inference for safety-critical control, adherence of model outputs to transportation physics and regulatory constraints, and privacy-preserving integration through federated learning and edge deployment.

Holistic smart city integration. A converging trend involves embedding transportation IoT within broader urban infrastructures, including energy, environmental monitoring, and public safety systems. Practical priorities include IoT-informed transit-oriented development planning, smart grid coordination for off-peak EV charging and vehicle-to-grid power stabilization, and Mobility as a Service (MaaS) platforms that integrate public transit, ride-hailing, and micromobility. Future ITS architectures will increasingly manage multimodal urban spaces, including delivery robot operations and aerial mobility integration. Achieving this vision requires interoperable AI, edge computing, blockchain-supported multi-party transactions, digital twins for cross-domain simulation, and coordinated governance to ensure equitable access and institutional accountability.

6 Conclusion

This study examined the evolving intersection of IoT and ITS through an integrated bibliometric and critical thematic review. Drawing on 574 Scopus-indexed, peer-reviewed publications from 2011 to 2024, the analysis mapped the intellectual structure, technological progression, and global collaboration patterns that define the IoT-ITS research domain. The findings show that the field has expanded rapidly and become increasingly interdisciplinary, with sustained publication growth, diverse institutional participation, and broad geographic engagement. Research activity has increasingly converged around AI-driven traffic optimization, cybersecurity, edge computing, digital twins, and decentralized ITS architectures. China, the United States, and India emerged as the leading contributors, reflecting both national research priorities and expanding international collaboration. Keyword co-occurrence and thematic evolution analyses further indicate a transition from early sensor-based systems toward secure, data-intensive, and intelligent transportation ecosystems.

Despite this progress, several barriers continue to limit large-scale deployment. Interoperability constraints, real-time data processing demands, cybersecurity risks, and the absence of unified implementation standards remain persistent challenges. Addressing these issues requires interoperable frameworks, integrative methodologies, and stronger cross-border collaboration to support resilient, ethical, and scalable IoT-enabled transport systems.

By combining science mapping with qualitative synthesis, this study provides a structured reference for researchers, practitioners, and policymakers working on IoT-based ITS innovation. Future research should prioritize federated learning, explainable and trustworthy AI, post-quantum cybersecurity, and sustainable IoT infrastructure. These directions are central to ensuring that ITS evolve as secure, inclusive, and technologically advanced components of smart and sustainable urban mobility.

Acknowledgement: The authors sincerely acknowledge the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, for its support and encouragement in conducting this research under Grant No. KF262770. During the preparation of this work, the authors used GPT-5.1 to assist with grammar correction, language refinement, and overall clarity. After using this tool, the authors carefully reviewed and edited the content to ensure accuracy, integrity, and adherence to scholarly standards. The authors take full responsibility for the final version of the manuscript.

Funding Statement: This research was funded by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under Grant number KFU262770.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Mahbub Hassan; methodology, Mahbub Hassan and Md Kamrul Islam; software, Mahbub Hassan and Md Ehtesamul Haque; validation, Md Shafiul Alam, M. M. Hafizur Rahman, Md Ehtesamul Haque, Mohammad Bin Amin, and Zoltán Nagy; formal analysis, Mahbub Hassan; investigation, Mohammad Bin Amin, Mahbub Hassan, and Zoltán Nagy; resources, Md Kamrul Islam, Md Shafiul Alam, M. M. Hafizur Rahman, Mohammad Bin Amin, and Zoltán Nagy; data curation, Mahbub Hassan; writing—original draft preparation, Mahbub Hassan; writing—review and editing, Md Kamrul Islam, Zoltán Nagy, Md Shafiul Alam, M. M. Hafizur Rahman, Md Ehtesamul Haque, and Mohammad Bin Amin; visualization, Mahbub Hassan; supervision, Md Kamrul Islam; project administration, Md Kamrul Islam and Mohammad Bin Amin; funding acquisition, Md Kamrul Islam, Zoltán Nagy, and Mohammad Bin Amin. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the corresponding authors upon reasonable request.

Ethics Approval: Not applicable.

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

Appendix A Review Matrix of IoT-Enabled ITS Studies

Table A1: Overview of key studies in IoT-enabled ITS research, including the problem addressed, IoT role and methodology, and limitations and future directions.

Ref.	ITS Domain	Problem Addressed	IoT Role & Methodology	Limitations & Future Directions
[3]	Smart Parking Surveillance	Data overload in vision systems; limited real deployments.	Hybrid edge-server: detection at edge, occupancy on server. Dual-thread SSD + background subtraction; fusion logic.	Low FPS on Pi 3B; sensitive conditions; needs labeled maps. Improve edge speed, generalize layout, add V2X integration.
[5]	Cybersecurity in ITS	No structured IoT attack model in critical systems.	Layered risk model with direct/indirect/subliminal paths. Systematic review, criticality scoring, threat modeling.	No real deployment; lacks defense validation. Secure firmware, lightweight crypto, blockchain IDs, ITS simulations.
[51]	Broad ITS Applications	Fragmented AI adoption; lacks systematized benefits.	AI processing edge/cloud using IoT vehicle and sensor data. Functional ITS classification; global and Indian use cases.	No empirical validation; lacks benchmarks. Stakeholder studies; ethical AI; city benchmarking; capacity building.
[4]	ITS in Smart Cities	Centralization, security flaws, latency in LTE/5G systems.	Three-layer IoT app, 6G comm, blockchain ledger model. Architecture proposals for ITS, grid, healthcare.	No implementation; lacks legacy and energy benchmarks. Quantum-safe blockchain, lightweight consensus, real-time simulation.
[34]	IloV	Lacks scalable, privacy-aware access control in cloud ITS.	ITS-ABACG: dynamic attribute grouping with policy enforcement. Formal model; AWS sim with 50+ vehicles.	AWS-limited; no V2X or 5G/6G; simulation only. Extend to V2X, homomorphic ABAC, edge-assisted control, adaptive policies.

(Continued)

Table A1 (continued)

Ref.	ITS Domain	Problem Addressed	IoT Role & Methodology	Limitations & Future Directions
[52]	ITS (Traffic, AVs, UAV)	Urbanization exposes real-time, modeling, security gaps.	Four-plane smart city model with UAVs, edge analytics, DRL agents. Review of 120+ works; UAV as MEC relay.	No real deployment; lacks blockchain, FL, legacy integration. Real-world DRL training; AI standards; federated UAV learning; ethical AI.
[116]	IoV Security	IoV faces growing cyber threats; no clear taxonomy.	Cloud-enabled V2X system addressing mobility and routing issues. STRIDE-based threat modeling; attack and defense classification.	No simulation; lacks 5G+ edge-cloud transition analysis. Trust-aware routing; delay-sensitive security; cross-layer protocols.
[38]	IoV in ITS	Centralized ITS lacks scalability, privacy.	Multi-chain blockchain with edge/cloud and AI integration. Survey; classified blockchain models, incentives, consensus.	No real tests; scalability unproven. Verifiable offloading; PKI-trust; smart contract edge ops; standards.
[6]	Secure VCS in ITS	Centralized key management causes latency in handovers.	Hierarchical VCS: RSUs → SMs → blockchain. Simulated handovers; analyzed latency/crypto load.	Simulation-only; mining latency; lacks privacy layers. Add privacy layers; real-world pilots; SM–cloud–fog hybrid.
[9]	IoV–IDS	High false alarms; limited resources on OBUs/RSUs.	RSU-centric CNN IDS for traffic monitoring. Simulated LOIC attacks with precision results.	CNN weak on long attacks; sensitivity issues. Multi-attack detection; federated learning; robustness.
[7]	MoD/AMoD	Spatial loss, high-dimensional data challenge OD prediction.	MultiConvLSTM captures spatial-temporal dependencies. NYC taxi dataset; outperforms ARIMA, CNN, LSTM.	Limited to NYC data; accuracy drops on long horizons. Extend OD tensor; real-time routing; IoT stream fusion.
[48]	Visual IoT in ITS	Detection degraded by haze, low contrast.	TSDNet with haze localization, feature extraction. Tested on RESIDE/VOC2007; improved PSNR, SSIM.	No UV/occlusion modeling; static loss weights. Multitask learning; adaptive loss; hardware-software co-design.
[41]	Fog-based IoV for AD	Cloud-only IoV causes delays and backbone overload.	Three-layer fog computing: access, fog, cloud. ILP and heuristic tested on multiple topologies.	No real-world tests; static VTPs; delay underexplored. Add mobility prediction; dynamic deployment.
[32]	Secure IoT ITS auth	Lacks lightweight anonymous authentication.	ECC-based seven-phase protocol for dynamic users. Formal validation; outperforms ECC baselines.	Assumes trusted CG; no blockchain/federated ID. Real deployment; federated ID; fog integration.
[40]	Real-time Traffic Monitoring	Cloud video systems limited by latency and bandwidth.	Edge IoT nodes perform distributed processing. YOLOv3 pipeline; tested on UA-DETRAC, Hollywood2.	No multi-access edge; noise sensitivity; heavy models. Lightweight models; edge-cloud balance; adaptive segmentation.
[39]	Smart Logistics	Centralized IoT lacks trust and real-time sync.	IoT sensors with blockchain-based edge analytics. Use-cases: SmaTaxi, TradeLens; framework mapping.	No simulation, benchmarking, energy analysis. Validate large-scale; enhance privacy; model efficiency.

(Continued)

Table A1 (continued)

Ref.	ITS Domain	Problem Addressed	IoT Role & Methodology	Limitations & Future Directions
[53]	Urban Traffic	Legacy ITS lacks real-time scale and analytics.	IoT-enabled vehicles, VANET, parking nodes. Modular s-ITS with sensor fusion; case study Chennai.	No real-time streams; static assumptions; no energy use. Dynamic city validation; energy-aware routing; real-time tests.
[10]	Cybersecurity for STS	Centralized IDS vulnerable to privacy and attacks.	Federated IDS with Transformer, blockchain security. Evaluated with TON_IoT, Car-Hacking datasets.	Needs labeled data; blockchain latency; no unsupervised. Explainability; latency optimization; semi-supervised models.
[58]	V2IoT Integration	Wireless links suffer loss/range in terrain.	Vehicles as IoT nodes using LPLR technology for V2I communications. Tested three terrains; RSSI, error, protocol comparisons.	Single-vehicle only; lacks 5G/6G/security. Multi-hop/mesh; SDN/fog layers; QoS integration.
[54]	Cross-domain ITS architecture	Fragmented systems; no unified CV-IoT-Cloud framework.	Three-layer: CV, vehicular cloud, IoT subsystems. Conceptual framework; case/project review.	No simulations; lacks security modeling. Federated auth; selective coding; edge/fog AI platforms.
[8]	Smart-city Traffic Monitoring	Lack of adaptive real-time decision systems.	IoT sensors for traffic/environment data. Mamdani FIS, MATLAB; four-layer sensing-communication-processing-UI.	Manual rules; no live deployment; static conditions. ML-adaptive rules; real-time deployment; other domains.
[47]	Roadside Infrastructure	Legacy RSUs lack modularity and sensing fusion.	SERSU rebroadcasts data; MCU with RTOS. CPU load validated; loop closure tests.	No field deployment; static thresholds; unassessed resilience. Field-test; ML thresholds; V2X and edge inference.
[117]	Emergency VANET routing	Latency in routing.	Geometry-based routing. Preemptive routing, queues.	High overhead; no scalability. Event-aware; fog/5G.
[118]	VANET emergency routing	Emergency packet delay.	GIS-based V2V forwarding. Spider-web routing, priority queues.	Simulation only; no field validation. Secure V2X; fog routing.
[44]	V2X video streaming	High latency, poor QoS.	Protocol survey. Vehicle-edge-cloud.	No real tests. Mobility-aware bitrate.
[119]	V2V/V2I communications	Congestion, unstable links.	Simulations with AODV/DSR. Perception-network-application layers.	No real tests; limited protocols. ML routing; fog/5G hybrid.
[120]	Social IoV routing	Ignores vehicle behavior.	Game theory, replicator dynamics. Cluster-based RSU guidance.	No real test; no scaling. Edge AI fusion; city trials.
[121]	Traffic routing Social IoV	Ignores social interactions.	Game-based clustering. Social correlation, route select.	Simulation only; overhead. Real prototype; scalable; incident-aware.
[43]	V2X security	Misbehavior detection.	CNN-LSTM edge DL. Single-stage, hierarchical classifiers.	Confusion; fixed window. Federated learning; adversarial robustness.
[46]	VANET infrastructure	Latency in centralized cloud.	Three-tier fog selection. Vehicle-fog-cloud layers.	Simulation only; no trust model. Edge-AI orchestration; privacy fog.

(Continued)

Table A1 (continued)

Ref.	ITS Domain	Problem Addressed	IoT Role & Methodology	Limitations & Future Directions
[65]	Energy-efficient VANET routing	High energy use.	Q-learning, fuzzy logic. Adaptive routing.	No hardware test; no security. Multi-agent RL; blockchain trust.
[42]	Smart waste ITS	Inefficient routing, security.	DNN, blockchain. Multi-layer sensing, validation.	No real test; latency issues. RL adaptive routing; PQ-crypto.
[64]	Edge computing vehicular IoT	Static offloading.	RNN, ABC optimization. Multi-layer MRP.	No testbed; no security. Blockchain, federated learning, 5G.
[33]	Urban traffic control	Static timing congestion.	MARL, DT, IoT data. Parallel learning.	Simulation only; compute heavy. City-wide DT; privacy RL.
[122]	Connected autonomous vehicles	Low-latency communication.	6G, MEC, blockchain. UAV-assisted V2X.	No prototype; 6G limits. UAV testbeds; quantum-safe security.
[123]	Vehicular networks	Lack of cooperative models.	Game theory, blockchain. Thematic game mapping.	No validation; no integration. Federated games; energy-aware.
[124]	5G VANETs security	Low-latency secure V2X.	Mutual authentication framework. Session keys.	No hardware validation. Blockchain trust; low-power crypto.
[56]	Accident detection	Weak real-time detection.	SVM, ACO, cloud. Multi-layer architecture.	No predictive models. DL-V2X hybrid; context integration.
[125]	Autonomous vehicles and intelligent automation	Safety, perception, cybersecurity, V2X privacy, and AI/IoT integration challenges.	AI, ML, DL, RL, IoT, cloud/edge computing, sensors, LiDAR, SLAM, blockchain. Comprehensive survey of AV applications, safety standards, AI/IoT tools, autonomous EV functions, and real-world AV deployments.	Review only; no new algorithm, dataset, or empirical validation. Robust safety validation; explainable/trustworthy AI; secure V2X; efficient simulation/testing; edge-enabled cooperative AV systems.
[59]	Smart Routing in Cities	Poor traffic-aware routing.	Grid SDN with TGP routing. Time-graph with cost heuristics.	Static intervals; no anomaly handling. LSTM prediction; secure SDN; DT-based tests.
[13]	Green 5G V2X	Energy-hungry ITS.	ITS-Fog-Cloud. Context-aware adaptive scheduling.	No ML; lacks real deployment. FL tuning; secure slicing.
[14]	Marine Micro-Mobility	No low-cost tracking.	Node-Gateway-Cloud. Real deployment on boats; LoRa tests.	No security; single-hop only. Apply to ferries/bikes; mesh LoRa.
[126]	Urban traffic light control	Poor adaptability to emergencies and dynamic flows.	Cournot/Stackelberg game theory; V2I communication. Central controller switches models based on traffic/emergency.	Simulation on single intersection; assumes perfect communications. Extend to multi-intersection; add trust; combine ML · predictions.
[127]	Secure surveillance in ITS	Secure cloud image classification without raw data exposure.	CNN + Paillier homomorphic encryption. CNN with encrypted inference tested on ITS dataset.	High latency; no real-time or hardware acceleration. Hardware acceleration; federated learning; multimodal encrypted analytics.
[113]	Secure V2I messaging	High cost in V2I security protocols.	ECC, HMAC, hybrid signcryption. Lightweight hybrid signcryption with batch verification.	Simulated only; trust assumptions; key lifecycle unexplored. Embedded deployment; blockchain; post-quantum crypto.

(Continued)

Table A1 (continued)

Ref.	ITS Domain	Problem Addressed	IoT Role & Methodology	Limitations & Future Directions
[128]	Socially-aware ITS privacy	Ethical issues in SIoV data collection.	Social IoT nodes with normative ethics frameworks. Ethical sensing and transparent decision-making.	No empirical validation; lacks ethics model. Formal ethical ontologies; privacy laws; decentralized enforcement.
[55]	Vehicle localization GPS-denial	Inaccurate localization during GPS outages.	EKF + SVM with IoT sensor fusion. EKF for signal processing; SVM drift prediction.	Simulated dropouts; short routes; no temporal modeling. LSTM/GRU for drift correction; field validation; fog deployment.
[129]	Public transport fleet monitoring	Lack of scalable modular monitoring.	GPS, OBD-II, MQTT, Docker, Cloud. Microservices for diagnostics and communication.	Real-world campus test; limited analytics. Add secure communications; predictive AI routing; smart city integration.
[37]	Privacy-preserving LBS	Identity leakage in vehicular cloud VM migration.	Pseudonym synchronization with VM migration. Cloud-edge IoV with pseudonym coordination.	Assumes centralized control; synthetic data. Real-world PCSS test; federated privacy; adversary resistance.
[66]	Vehicle speed estimation	Vision/loop sensors impractical for low-resource setups.	Tri-axial magnetometers + BLE. Signal gradient peak detection.	Roadside tests; limited accuracy in platoons. ML integration; hybrid vision-magnetic sensing; occlusion handling.
[45]	Urban signal control	Lack of AI+IoT integrated taxonomy in ITS.	DRL, fuzzy logic, TAPIOCA, AHP. Fog-cloud layered ITS taxonomy.	No experiments; limited trade-off analysis. Multi-agent RL; city-scale testing; semantic IoT.
[36]	Location privacy in connected vehicles	Metadata and cloud identity leakage.	Differential privacy, pseudonym zones, fog nodes. Privacy framework with zone anonymization.	Static DP; coordination infrastructure required. Adaptive DP; adversarial resistance; blockchain trust.
[50]	Urban traffic forecasting	Poor generalization and memory in prediction.	GAT, GRU, RL memory fusion. Spatiotemporal GNN with RL controller.	Static graphs; complex RL; no edge deployment. Online learning; edge deployment; robustness; heterogeneity.
[35]	Secure V2I/V2F communication	High computational overhead, privacy risks.	Lightweight crypto on OBUs; fog offloading. Vehicle-Fog-TA hierarchical model.	Semi-trusted fog risk; central TA reliance. Blockchain decentralization; group authentication; PQ crypto.
[60]	SDN controller placement	High energy, latency, load imbalance.	SDN with heuristic multi-objective optimization. Optimized hierarchical SDN control plane.	No mobility/dynamic placement; heuristic only. AI adaptive control; fog-edge hybrid; resilient architectures.
[31]	IoV Security and Privacy	Multi-layer V2X threats.	ECC, PKI, IDS, trust, STRIDE. Layered perception-communication-trust model.	No simulation; lack AI benchmarking. Federated IDS; blockchain trust; game theory; standards.
[130]	IoV authentication	Lack scalable mutual authentication.	IBE, PKI, symmetric crypto, STRIDE. Multi-layer authentication protocol.	Conceptual only; no benchmarks. Blockchain trust; protocol validation; ML IDS.

(Continued)

Table A1 (continued)

Ref.	ITS Domain	Problem Addressed	IoT Role & Methodology	Limitations & Future Directions
[67]	Pedestrian signal control	Inflexible timing ignoring pedestrian data.	Fuzzy logic controller with pedestrian sensors. FLC rules validated via simulation.	Assumes perfect detection; no vehicle coordination. ANFIS tuning; multimodal control; real pilots.
[131]	Smart urban mobility	Lack integrated AI-IoT frameworks.	Real-time sensing; fog/edge processing. Layered sensing-data-AI-actuation model.	Conceptual; sparse validation; little security. Social behavior modeling; AV-aware AI; privacy ML.
[61]	Traffic flow prediction	Inefficient GNNs on edge; weak fusion.	GCN, GRU, residual learning; 5G/6G data. Spatiotemporal graph-RNN pipeline.	No dynamic graphs; no federated learning. Federated GNN; adaptive graphs; multimodal input; transformers.

Note: AD = Autonomous Driving; ABAC = Attribute Based Access Control; AHP = Analytic Hierarchy Process; AI = Artificial Intelligence; AMoD = Autonomous Mobility on Demand; ANFIS = Adaptive Neuro Fuzzy Inference System; AODV = Ad Hoc On Demand Distance Vector; ARIMA = AutoRegressive Integrated Moving Average; AV = Autonomous Vehicle; AWS = Amazon Web Services; BLE = Bluetooth Low Energy; CG = Control Gateway; CNN = Convolutional Neural Network; CPU = Central Processing Unit; CV = Connected Vehicle; DL = Deep Learning; DNN = Deep Neural Network; DP = Differential Privacy; DRL = Deep Reinforcement Learning; DSR = Dynamic Source Routing; ECC = Elliptic Curve Cryptography; EKF = Extended Kalman Filter; EV = Electric Vehicle; FIS = Fuzzy Inference System; FL = Federated Learning; FLC = Fuzzy Logic Controller; FPS = Frames Per Second; GAT = Graph Attention Network; GCN = Graph Convolutional Network; GIS = Geographic Information System; GNN = Graph Neural Network; GPS = Global Positioning System; GRU = Gated Recurrent Unit; HMAC = Hash based Message Authentication Code; IBE = Identity Based Encryption; IDS = Intrusion Detection System; IIoV = Industrial Internet of Vehicles; ILP = Integer Linear Programming; IoT = Internet of Things; IoV = Internet of Vehicles; ITS = Intelligent Transportation Systems; LBS = Location Based Services; LiDAR = Light Detection and Ranging; LOIC = Low Orbit Ion Cannon; LoRa = Long Range; LPLR = Low Power Long Range; LSTM = Long Short Term Memory; LTE = Long Term Evolution; MARL = Multi Agent Reinforcement Learning; MATLAB = Matrix Laboratory; MCU = Microcontroller Unit; MEC = Mobile Edge Computing; ML = Machine Learning; MoD = Mobility on Demand; MQTT = Message Queuing Telemetry Transport; MRP = Mobility Oriented Retrieval Protocol; NYC = New York City; OBD II = On Board Diagnostics II; OBU = On Board Unit; OD = Origin Destination; PKI = Public Key Infrastructure; PQ = Post Quantum; PSNR = Peak Signal to Noise Ratio; QoS = Quality of Service; RL = Reinforcement Learning; RNN = Recurrent Neural Network; RSSI = Received Signal Strength Indicator; RSU = Roadside Unit; RTOS = Real Time Operating System; SDN = Software Defined Networking; SIIoV = Social Internet of Vehicles; SLAM = Simultaneous Localization and Mapping; SM = Security Manager; SSD = Single Shot Detector; SSIM = Structural Similarity Index Measure; STRIDE = Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege; STS = Smart Transportation Systems; SVM = Support Vector Machine; TA = Trusted Authority; UAV = Unmanned Aerial Vehicle; UI = User Interface; UV = Ultraviolet; V2F = Vehicle to Fog; V2I = Vehicle to Infrastructure; V2IoT = Vehicle to Internet of Things; V2V = Vehicle to Vehicle; V2X = Vehicle to Everything; VANET = Vehicular Ad Hoc Network; VCS = Vehicular Communication System; VM = Virtual Machine; YOLOv3 = You Only Look Once version 3.

References

1. Oladimeji D, Gupta K, Kose NA, Gundogan K, Ge L, Liang F. Smart transportation: an overview of technologies and applications. *Sensors*. 2023;23(8):3880. doi:10.3390/s23083880.
2. Al-Turjman F, Malekloo A. Smart parking in IoT-enabled cities: a survey. *Sustain Cities Soc*. 2019;49:101608. doi:10.1016/j.scs.2019.101608.
3. Ke R, Zhuang Y, Pu Z, Wang Y. A smart, efficient, and reliable parking surveillance system with edge artificial intelligence on IoT devices. *IEEE Trans Intell Transp Syst*. 2021;22(8):4962–74. doi:10.1109/tits.2020.2984197.
4. Kumari A, Gupta R, Tanwar S. Amalgamation of blockchain and IoT for smart cities underlying 6G communication: a comprehensive review. *Comput Commun*. 2021;172(1):102–18. doi:10.1016/j.comcom.2021.03.005.
5. Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J. A survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services. *IEEE Commun Surv Tutor*. 2018;20(4):3453–95. doi:10.1109/COMST.2018.2855563.

6. Lei A, Cruickshank H, Cao Y, Asuquo P, Ogah CPA, Sun Z. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet Things J.* 2017;4(6):1832–43. doi:10.1109/jiot.2017.2740569.
7. Chu KF, Lam AYS, Li VOK. Deep multi-scale convolutional LSTM network for travel demand and origin-destination predictions. *IEEE Trans Intell Transp Syst.* 2020;21(8):3219–32. doi:10.1109/tits.2019.2924971.
8. Iqbal K, Khan MA, Abbas S, Hasan Z, Fatima A. Intelligent transportation system (ITS) for smart-cities using Mamdani fuzzy inference system. *Int J Adv Comput Sci Appl.* 2018;9(2):94–105. doi:10.14569/IJACSA.2018.090215.
9. Nie L, Ning Z, Wang X, Hu X, Cheng J, Li Y. Data-driven intrusion detection for intelligent Internet of vehicles: a deep convolutional neural network-based method. *IEEE Trans Netw Sci Eng.* 2020;7(4):2219–30. doi:10.1109/tNSE.2020.2990984.
10. Abdel-Basset M, Moustafa N, Hawash H, Razzak I, Sallam KM, Elkomy OM. Federated intrusion detection in blockchain-based smart transportation systems. *IEEE Trans Intell Transp Syst.* 2022;23(3):2523–37. doi:10.1109/tits.2021.3119968.
11. Akbar A, Khan A, Carrez F, Moessner K. Predictive analytics for complex IoT data streams. *IEEE Internet Things J.* 2017;4(5):1571–82. doi:10.1109/jiot.2017.2712672.
12. Kang J, Yu R, Huang X, Zhang Y. Privacy-preserved pseudonym scheme for fog computing supported Internet of vehicles. *IEEE Trans Intell Transp Syst.* 2018;19(8):2627–37. doi:10.1109/tits.2017.2764095.
13. Lin C, Han G, Du J, Xu T, Shu L, Lv Z. Spatiotemporal congestion-aware path planning toward intelligent transportation systems in software-defined smart city IoT. *IEEE Internet Things J.* 2020;7(9):8012–24. doi:10.1109/jiot.2020.2994963.
14. Sodhro AH, Pirbhulal S, Sodhro GH, Muzammal M, Zongwei L, Gurtov A, et al. Towards 5G-enabled self adaptive green and reliable communication in intelligent transportation system. *IEEE Trans Intell Transp Syst.* 2021;22(8):5223–31. doi:10.1109/tits.2020.3019227.
15. Hassan M, Kabir ME, Jusoh M, An HK, Negnevitsky M, Li C. Large language models in transportation: a comprehensive bibliometric analysis of emerging trends, challenges and future research. *IEEE Access.* 2025;13(251):132547–98. doi:10.1109/access.2025.3589319.
16. Page MJ, Moher D, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. PRISMA, 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. *BMJ.* 2021;372:n160. doi:10.3122/med.2020.osf.io/gwdhk.
17. Nugroho H, Surendro K. A comprehensive bibliometric analysis of missing value imputation. *IEEE Access.* 2024;12:14819–46. doi:10.1109/access.2024.3357533.
18. Li Z, Wang G, Lu J, Broo DG, Kiritsis D, Yan Y. Bibliometric analysis of model-based systems engineering: past, current, and future. *IEEE Trans Eng Manag.* 2024;71(17):2475–92. doi:10.1109/tem.2022.3186637.
19. Hassan M, Shrabana SS, Islam MA, Basaruddin KS, Ijaz ME, Kamarrudin NSB, et al. Integration of extended reality technologies in transportation systems: a bibliometric analysis and review of emerging trends, challenges, and future research. *Results Eng.* 2025;26:105334. doi:10.1016/j.rineng.2025.105334.
20. Hassan M, Al Nafees A, Shrabana SS, Paul A, Mahin HD. Application of machine learning in intelligent transport systems: a comprehensive review and bibliometric analysis. *Discov Civ Eng.* 2025;2(1):98. doi:10.1007/s44290-025-00256-2.
21. Montoya FG, Alcayde A, Baños R, Manzano-Agugliaro F. A fast method for identifying worldwide scientific collaborations using the scopus database. *Telemat Inform.* 2018;35(1):168–85. doi:10.1016/j.tele.2017.10.010.
22. Zhu J, Liu W. A tale of two databases: the use of web of science and Scopus in academic papers. *Scientometrics.* 2020;123(1):321–35. doi:10.1007/s11192-020-03387-8.
23. Singh VK, Singh P, Karmakar M, Leta J, Mayr P. The journal coverage of web of science, scopus and dimensions: a comparative analysis. *Scientometrics.* 2021;126(6):5113–42. doi:10.1007/s11192-021-03948-5.
24. Wong D. VOSviewer. *Tech Serv Q.* 2018;35(2):219–20.
25. Aria M, Cuccurullo C. bibliometrix: an R-tool for comprehensive science mapping analysis. *J Informetr.* 2017;11(4):959–75. doi:10.1016/j.joi.2017.08.007.

26. Chu WW, Hafiz NRM, Mohamad UA, Ashamuddin H, Chu SWT. A review of STEM education with the support of visualizing its structure through the CiteSpace software. *Int J Technol Des Educ.* 2023;33(1):39–61. doi:10.1007/s10798-022-09728-3.
27. Badassa BB, Sun B, Qiao L. Sustainable transport infrastructure and economic returns: a bibliometric and visualization analysis. *Sustainability.* 2020;12(5):2033. doi:10.3390/su12052033.
28. Hassan M, Mahin HD, Nafees AA, Paul A, Shrabana SS. Big data applications in intelligent transport systems: a bibliometric analysis and review. *Discov Civ Eng.* 2025;2(1):49. doi:10.1007/s44290-025-00205-z.
29. Ghosh A, Maeder A, Baker M, Chandramouli D. 5G evolution: a view on 5G cellular technology beyond 3GPP release 15. *IEEE Access.* 2019;7:127639–51. doi:10.1109/access.2019.2939938.
30. Narayanan A, Ramadan E, Carpenter J, Liu Q, Liu Y, Qian F, et al. A first look at commercial 5G performance on smartphones. In: *Proceedings of the Web Conference 2020, WWW '20; 2020 Apr 20–24; Taipei, Taiwan.* New York, NY, USA: Association for Computing Machinery; 2020. p. 894–905.
31. Sun Y, Wu L, Wu S, Li S, Zhang T, Zhang L, et al. Security and privacy in the Internet of vehicles. In: *Proceedings of the 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI); 2015 Oct 22–23; Beijing, China.* p. 116–21.
32. Srinivas J, Das AK, Wazid M, Vasilakos AV. Designing secure user authentication protocol for big data collection in IoT-based intelligent transportation system. *IEEE Internet Things J.* 2021;8(9):7727–44. doi:10.1109/jiot.2020.3040938.
33. Jin J, Guo H, Xu J, Wang X, Wang FY. An end-to-end recommendation system for urban traffic controls and management under a parallel learning framework. *IEEE Trans Intell Transp Syst.* 2021;22(3):1616–26. doi:10.1109/tits.2020.2973736.
34. Gupta M, Awaysheh FM, Benson J, Alazab M, Patwa F, Sandhu R. An attribute-based access control for cloud enabled industrial smart vehicles. *IEEE Trans Ind Inform.* 2021;17(6):4288–97. doi:10.1109/tii.2020.3022759.
35. Wu TY, Lee Z, Yang L, Luo JN, Tso R. Provably secure authentication key exchange scheme using fog nodes in vehicular ad hoc networks. *J Supercomput.* 2021;77(7):6992–7020. doi:10.1007/s11227-020-03548-9.
36. Ghane S, Jolfaei A, Kulik L, Ramamohanarao K, Puthal D. Preserving privacy in the Internet of connected vehicles. *IEEE Trans Intell Transp Syst.* 2021;22(8):5018–27. doi:10.1109/tits.2020.2964410.
37. Kang J, Yu R, Huang X, Jonsson M, Bogucka H, Gjessing S, et al. Location privacy attacks and defenses in cloud-enabled Internet of vehicles. *IEEE Wirel Commun.* 2016;23(5):52–9. doi:10.1109/mwc.2016.7721742.
38. Mollah MB, Zhao J, Kumar N, Das AK, Puthal D, Zomaya AY, et al. Blockchain for the Internet of vehicles towards intelligent transportation systems: a survey. *IEEE Internet Things J.* 2021;8(6):4157–85. doi:10.1109/jiot.2020.3028368.
39. Humayun M, Jhanjhi NZ, Hamid B, Ahmed G. Emerging smart logistics and transportation using iot and blockchain. *IEEE Internet Things Mag.* 2020;3(2):58–62. doi:10.1109/iotm.0001.1900097.
40. Wan S, Ding S, Chen C. Edge computing enabled video segmentation for real-time traffic monitoring in Internet of vehicles. *Pattern Recognit.* 2022;121(11):108146. doi:10.1016/j.patcog.2021.108146.
41. Yu C, Lin B, Guo P, Zhang W, Li S, He R. Deployment and dimensioning of fog computing-based Internet of vehicle infrastructure for autonomous driving. *IEEE Internet Things J.* 2019;6(1):149–60. doi:10.1109/jiot.2018.2875750.
42. Yuvaraj N, Praghash K, Raja RA, Shankar M, Ramesh TK, Sivakumar S. An investigation of garbage disposal electric vehicles (GDEVs) integrated with deep neural networking (DNN) and intelligent transportation system (ITS) in smart city management system (SCMS). *Wirel Pers Commun.* 2022;123(2):1733–52. doi:10.1007/s11277-021-09210-8.
43. Alladi T, Kohli V, Chamola V, Yu FR. A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems. *Digit Commun Netw.* 2023;9(5):1113–22. doi:10.1016/j.dcan.2022.06.018.
44. Yu R, Zhang Y, Gjessing S, Xia W, Yang K. Toward cloud-based vehicular networks with efficient resource management. *IEEE Netw.* 2013;27(5):48–55. doi:10.1109/MNET.2013.6616115.
45. Ouallane AA, Bahnasse A, Bakali A, Talea M. Overview of road traffic management solutions based on IoT and AI. *Procedia Comput Sci.* 2022;198(2):518–23. doi:10.1016/j.procs.2021.12.279.

46. Ali ZH, Badawy MM, Ali HA. A novel geographically distributed architecture based on fog technology for improving Vehicular Ad hoc Network (VANET) performance. *Peer-Peer Netw Appl.* 2020;13(5):1539–66. doi:10.1007/s12083-020-00910-9.
47. Al-Dweik A, Muresan R, Mayhew M, Lieberman M. IoT-based multifunctional scalable real-time enhanced road side unit for intelligent transportation systems. In: *Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*; 2017 Apr 30–May 3; Windsor, ON, Canada. p. 1–6.
48. Liu RW, Guo Y, Lu Y, Chui KT, Gupta BB. Deep network-enabled haze visibility enhancement for visual IoT-driven intelligent transportation systems. *IEEE Trans Ind Inform.* 2023;19(2):1581–91. doi:10.1109/tii.2022.3170594.
49. Qiu J, Du L, Zhang D, Su S, Tian Z. Nei-TTE: intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city. *IEEE Trans Ind Inform.* 2020;16(4):2659–66. doi:10.1109/tii.2019.2943906.
50. Zhou F, Yang Q, Zhang K, Trajcevski G, Zhong T, Khokhar A. Reinforced spatiotemporal attentive graph neural networks for traffic forecasting. *IEEE Internet Things J.* 2020;7(7):6414–28. doi:10.1109/jiot.2020.2974494.
51. Iyer LS. AI enabled applications towards intelligent transportation. *Transp Eng.* 2021;5(189):100083. doi:10.1016/j.treng.2021.100083.
52. Ullah Z, Al-Turjman F, Mostarda L, Gagliardi R. Applications of artificial intelligence and machine learning in smart cities. *Comput Commun.* 2020;154(2):313–23. doi:10.1016/j.comcom.2020.02.069.
53. Muthuramalingam S, Bharathi A, Kumar SR, Gayathri N, Sathiyaraj R, Balamurugan B. IoT based intelligent transportation system (IoT-ITS) for global perspective: a case study. In: Balas V, Solanki V, Kumar R, Khari M, editors. *Internet of things and big data analytics for smart generation*. Vol. 154 of *Intelligent Systems Reference Library*. Cham, Switzerland: Springer; 2019. p. 255–71.
54. Guerrero-Ibanez JA, Zeadally S, Contreras-Castillo J. Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and Internet of things technologies. *IEEE Wirel Commun.* 2015;22(6):122–8. doi:10.1109/MWC.2015.7368833.
55. Belhajem I, Maissa YB, Tamtaoui A. Improving vehicle localization in a smart city with low cost sensor networks and support vector machines. *Mob Netw Appl.* 2018;23(4):854–63. doi:10.1007/s11036-017-0879-9.
56. Liang G. Automatic traffic accident detection based on the Internet of things and support vector machine. *Int J Smart Home.* 2015;9(4):97–106. doi:10.14257/ijsh.2015.9.4.10.
57. Hassan M, Kabir ME, Islam MK, Alam E, Rambe AH, Jusoh M, et al. Mapping the machine learning landscape in autonomous vehicles: a scientometric review of research trends, applications, challenges, and future directions. *IEEE Access.* 2025;13(9):182036–77. doi:10.1109/access.2025.3620637.
58. Datta SK, Costa RPF, Härrä J, Bonnet C. Integrating connected vehicles in Internet of things ecosystems: challenges and solutions. In: *Proceedings of the 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*; 2016 Jun 21–24; Coimbra, Portugal. p. 1–6.
59. Zhang H, Lu X. Vehicle communication network in intelligent transportation system based on Internet of things. *Comput Commun.* 2020;160(7):799–806. doi:10.1016/j.comcom.2020.03.041.
60. Kaur K, Garg S, Kaddoum G, Kumar N, Gagnon F. SDN-based Internet of autonomous vehicles: an energy-efficient approach for controller placement. *IEEE Wirel Commun.* 2019;26(6):72–9. doi:10.1109/mwc.001.1900112.
61. Yan B, Wang G, Yu J, Jin X, Zhang H. Spatial-temporal Chebyshev graph neural network for traffic flow prediction in IoT-based ITS. *IEEE Internet Things J.* 2022;9(12):9266–79. doi:10.1109/jiot.2021.3105446.
62. Zhu F, Lv Y, Chen Y, Wang X, Xiong G, Wang FY. Parallel transportation systems: toward IoT-enabled smart urban traffic control and management. *IEEE Trans Intell Transp Syst.* 2020;21(10):4063–71. doi:10.1109/tits.2019.2934991.
63. Hassan M, Turjo TD, Rambe AH, Jusoh M, Islam MK, Rahman MMH, et al. A comprehensive survey of adaptive traffic signal control: methods, applications, challenges, and future research. *Arch Comput Methods Eng.* 2026. Online first. doi:10.1007/s11831-026-10574-y.
64. Boukerche A, Soto V. An efficient mobility-oriented retrieval protocol for computation offloading in vehicular edge multi-access network. *IEEE Trans Intell Transp Syst.* 2020;21(6):2675–88. doi:10.1109/tits.2020.2991376.
65. Goswami P, Mukherjee A, Hazra R, Yang L, Ghosh U, Qi Y, et al. AI based energy efficient routing protocol for intelligent transportation system. *IEEE Trans Intell Transp Syst.* 2022;23(2):1670–9. doi:10.1109/tits.2021.3107527.

66. Feng Y, Mao G, Chen B, Li C, Hui Y, Xu Z, et al. MagMonitor: vehicle speed estimation and vehicle classification through a magnetic sensor. *IEEE Trans Intell Transp Syst.* 2022;23(2):1311–22. doi:10.1109/tits.2020.3024652.
67. Pau G, Campisi T, Canale A, Severino A, Collotta M, Tesoriere G. Smart pedestrian crossing management at traffic light junctions through a fuzzy-based approach. *Future Internet.* 2018;10(2):15. doi:10.3390/fi10020015.
68. Heideker A, Silva D, Kamienski C, Trotta A. Achieving seamless IoT interoperability through data plane programmability. In: *Proceedings of the 22nd IEEE Consumer Communications and Networking Conference (CCNC 2025)*; 2025 Jan 10–13; Las Vegas, NV, USA. New York, NY, USA: IEEE; 2025. p. 1–6.
69. Porru S, Misso FE, Pani FE, Repetto C. Smart mobility and public transport: opportunities and challenges in rural and urban areas. *J Traffic Transp Eng.* 2020;7(1):88–97. doi:10.1016/j.jtte.2019.10.002.
70. Son H, Jang J, Park J, Balog A, Ballantyne P, Kwon HR, et al. Leveraging advanced technologies for (smart) transportation planning: a systematic review. *Sustainability.* 2025;17(5):2245. doi:10.3390/su17052245.
71. Perković T, Šolić P, Zargariasl H, Čoko D, Rodrigues JJPC. Smart parking sensors: state of the art and performance evaluation. *J Clean Prod.* 2020;262(6):121181. doi:10.1016/j.jclepro.2020.121181.
72. Gunawan I, Nguyen T, Hallo L. Public–private partnerships (PPPs) for smart transport infrastructure development: a promising approach and potential risks. In: *Proceedings of the 8th International Conference on Sustainable Urban Development.* Berlin/Heidelberg, Germany: Springer; 2024. p. 19–36.
73. Waqar A, Alshehri AH, Alanazi F, Alotaibi S, Almujiabah HR. Evaluation of challenges to the adoption of intelligent transportation system for urban smart mobility. *Res Transp Bus Manag.* 2023;51(3):101060. doi:10.1016/j.rtbm.2023.101060.
74. Karkhanis P, Dajsuren Y, van den Brand M. Designing a reference architecture for the C-ITS services. In: *Proceedings of the 17th European Conference on Software Architecture (ECSA 2023)*; 2023 Sep 18–22; Istanbul, Turkey. Cham, Switzerland: Springer; 2023. p. 117–32.
75. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. *IEEE Internet Things J.* 2014;1(1):22–32. doi:10.1109/jiot.2014.2306328.
76. Tzika-Kostopoulou D, Nathanail E, Kokkinos K. Big data in transportation: a systematic literature analysis and topic classification. *Knowl Inf Syst.* 2024;66(8):5021–46. doi:10.1007/s10115-024-02112-8.
77. Sysoev A, Khabibullina E, Kadasev D, Voronin N. Heterogeneous data aggregation schemes to determine traffic flow parameters in regional intelligent transportation systems. *Transp Res Procedia.* 2020;45(3):507–13. doi:10.1016/j.trpro.2020.03.063.
78. Braga M, Santos MY, Moreira A. Integrating public transportation data: creation and editing of GTFS data. In: *Proceedings of the 2014 World Conference on Information Systems and Technologies (WorldCIST)*; 2014 Apr 15–18; Funchal, Portugal. Berlin/Heidelberg, Germany: Springer; 2014. p. 53–62.
79. Samper-Zapater JJ, Gutiérrez-Moret J, Rocha JM, Martínez-Durá JJ, Tomás VR. Semantic modelling approach for safety-related traffic information using DATEX II. *Information.* 2024;15(1):3. doi:10.3390/info15010003.
80. Hassebo A, Tealab M. Global models of smart cities and potential IoT applications: a review. *IoT.* 2023;4(3):338–57. doi:10.3390/iot4030017.
81. Arabiat A, Altayeb M. Assessing the effectiveness of data mining tools in classifying and predicting road traffic congestion. *Indones J Electr Eng Comput Sci.* 2024;34(2):1295–303. doi:10.11591/ijeecs.v34.i2.pp1295-1303.
82. Uprety I, Agnello G, Zhao X. Supporting deep learning based autonomous driving applications on resource-constrained devices. In: *Proceedings of the 2nd IEEE International Conference on Mobility, Operations, Services and Technologies (MOST 2024)*; 2024 May 1–3; Dallas, TX, USA. p. 42–9.
83. Mehrannia P, Moghadam AA, Basir OA. A dempster-shafer sensor fusion approach for traffic incident detection and localization. In: *Proceedings of the 21st IEEE International Conference on Intelligent Transportation Systems (ITSC 2018)*; 2018 Nov 4–7; Maui, HI, USA. p. 3911–6.
84. Znidi F, Morsy M, Rathore H. Future on wheels: safeguarding privacy in tomorrow's connected vehicles-future-SP. *IEEE Access.* 2024;12(1):179857–78. doi:10.1109/access.2024.3505158.
85. Andraško J, Hamulák O, Mesarčík M, Kerikmäe T, Kajander A. Sustainable data governance for cooperative, connected and automated mobility in the european union. *Sustainability.* 2021;13(19):10610. doi:10.3390/su131910610.

86. Vogt J, Schotten HD. Challenges in protocol standardization for intelligent transport systems. In: Proceedings of the 2023 IEEE Vehicle Power and Propulsion Conference (VPPC); 2023 Oct 24–27; Milan, Italy. New York, NY, USA: IEEE; 2023. p. 1–8.
87. Moradi-Pari E, Tian D, Bahramgiri M, Rajab S, Bai S. DSRC versus LTE-V2X: empirical performance analysis of direct vehicular communication technologies. *IEEE Trans Intell Transp Syst.* 2023;24(5):4889–903. doi:10.1109/tits.2023.3247339.
88. Stanley KD, Mignano J, Blumenthal MS. Public welfare and emerging technology: balancing interests in automated vehicle regulations across six jurisdictions. In: *Lecture notes in mobility.* Berlin/Heidelberg, Germany: Springer; 2024. p. 32–48.
89. Sivanantham K, Praveen PB. Automotive vehicle data security service in IoT using ACO algorithm. In: *Supervised and unsupervised data engineering for multimedia data.* Hoboken, NJ, USA: Wiley; 2024. p. 93–110.
90. Paschalidis E, Zhai S, Guo J, Wei T, Liu P, Chen H. The twofold role of legal liability misattribution on intention to buy automated vehicles: a survey in China. *Int J Hum-Comput Interact.* 2024;40(16):4288–99. doi:10.1080/10447318.2023.2212220.
91. Yao Q, Li T, Yan C, Deng Z. Accident responsibility identification model for Internet of vehicles based on lightweight blockchain. *Concurr Comput Pract Exp.* 2024;39(1):58–81. doi:10.1111/coin.12529.
92. Monreale A, Pellungrini R. A survey on privacy in human mobility. *Trans Data Priv.* 2023;16(1):51–82.
93. Sanchez TW, Brenman M, Ye X. The ethical concerns of artificial intelligence in urban planning. *J Am Plan Assoc.* 2025;91(2):294–307. doi:10.1080/01944363.2024.2355305.
94. Cohen R. Governance of public-private partnerships: lessons from the Italian experience in transportation projects. In: *Competitive government: public private partnerships.* Berlin/Heidelberg, Germany: Springer; 2022. p. 223–41.
95. Hansen MM, Dahiya B. Traffy fondue: a smart city citizen engagement. *Front Sustain Cities.* 2025;7:1491621. doi:10.3389/frsc.2025.1491621.
96. Docherty I, Marsden G, Anable J. The governance of smart mobility. *Transp Res Part A Policy Pract.* 2018;115(4):114–25. doi:10.1016/j.tra.2017.09.012.
97. Oti IC, Gharaibeh NG. A note on assessment of transportation infrastructure data management practices. *Public Work Manag Policy.* 2020;25(2):132–50. doi:10.1177/1087724x19869940.
98. Seo J, Kwak J, Kim S. Development for high-assurance software update management system complying with UN R156. *IEEE Access.* 2024;12(1):135811–30. doi:10.1109/access.2024.3426591.
99. Mossberger K, Cho S, Cheong PH, Kuznetsova D. The public good and public attitudes toward data sharing through IoT. *Policy Internet.* 2023;15(3):370–96. doi:10.1002/poi3.343.
100. Cottrill CD, Jacobs N, Markovic M, Edwards P. Sensing the city: designing for privacy and trust in the Internet of things. *Sustain Cities Soc.* 2020;63(5):102453. doi:10.1016/j.scs.2020.102453.
101. S. DR, B. A. Bridging the gap: innovations in ITS for rural mobility challenges. In: *Urban mobility and challenges of intelligent transportation systems.* Hershey, PA, USA: IGI Global Scientific Publishing; 2025. p. 147–68.
102. Verma SK, Verma R, Singh BK, Sinha RS. Management of intelligent transportation systems and advanced technology. In: *Energy, environment, and sustainability.* Berlin/Heidelberg, Germany: Springer; 2024. p. 159–75.
103. Muneera CP, Karuppanagounder K. Economic impact of traffic congestion—estimation and challenges. *Eur Transp Transp Eur.* 2018;68(5):1–19.
104. Jin J, Rafferty P. Does congestion negatively affect income growth and employment growth? Empirical evidence from US metropolitan regions. *Transp Policy.* 2017;56(6):27–36. doi:10.1016/j.tranpol.2016.12.003.
105. Bleviss DL. Transportation is critical to reducing greenhouse gas emissions in the United States. *Wiley Interdiscip Rev Energy Environ.* 2021;10(2):e390. doi:10.1002/wene.390.
106. Shilpa S, Jyothi N, Rao AN, Velivela A, Sagar YA, Reddy MSRL. Sustainability in the Internet of things: environmental impacts and green technologies. In: *Cognitive science and technology.* Berlin/Heidelberg, Germany: Springer; 2025. p. 93–104.
107. Gittleman M, Monaco K. Truck-driving jobs: are they headed for rapid elimination? *ILR Rev.* 2019;73(1):3–24. doi:10.1177/0019793919858079.

108. Silla A, Rämä P, Leden L, Van Noort M, De Kruijff J, Bell D, et al. Quantifying the effectiveness of ITS in improving safety of VRUs. *IET Intell Transp Syst.* 2017;11(3):164–72. doi:10.1049/iet-its.2016.0024.
109. Inoue D, Okada A, Matsumori T, Aihara K, Yoshida H. Traffic signal optimization on a square lattice with quantum annealing. *Sci Rep.* 2021;11(1):3303. doi:10.1038/s41598-021-82740-0.
110. Zhang D, Zheng H, Yue W, Wang X. Advancing ITS applications with LLMs: a survey on traffic management, transportation safety, and autonomous driving. In: Hu M, Cornelis C, Zhang Y, Lingras P, Ślęzak D, Yao J, editors. *Rough sets.* Cham, Switzerland: Springer Nature; 2024. p. 295–309.
111. Fowler DS, Maple C, Epiphaniou G. A practical implementation of quantum-derived keys for secure vehicle-to-infrastructure communications. *Vehicles.* 2023;5(4):1586–604. doi:10.3390/vehicles5040086.
112. Stavdas A, Kosmatos E, Maple C, Hugues-Salas E, Epiphaniou G, Fowler DS, et al. Quantum key distribution for V2I communications with software-defined networking. *IET Quantum Commun.* 2024;5(1):38–45. doi:10.1049/qtc2.12070.
113. Ali I, Chen Y, Pan C, Zhou A. ECCHSC: computationally and bandwidth efficient ECC-based hybrid sign-encryption protocol for secure heterogeneous vehicle-to-infrastructure communications. *IEEE Internet Things J.* 2022;9(6):4435–50. doi:10.1109/jiot.2021.3104010.
114. Dharminder D, Kumari S, Kumar U. Post quantum secure conditional privacy preserving authentication for edge based vehicular communication. *Trans Emerg Telecommun Technol.* 2021;32(11):e4346. doi:10.1002/ett.4346.
115. Hassan M, Narupiti S, Bhuiyan T, Hassan MM. Leveraging large language models to investigate the decoy effect in route choice behavior. In: *Proceedings of the 2025 International Conference on Sustainable Technology and Engineering (i-COSTE); 2025 Dec 2–4; Alexandria, VA, USA.* New York, NY, USA: IEEE. p. 1–6.
116. Sun Y, Wu L, Wu S, Li S, Zhang T, Zhang L, et al. Attacks and countermeasures in the Internet of vehicles. *Ann Telecommun.* 2017;72(5–6):283–95. doi:10.1007/s12243-016-0551-6.
117. Zheng K, Hou L, Meng H, Zheng Q, Lu N, Lei L. Soft-defined heterogeneous vehicular network: architecture and challenges. *IEEE Netw.* 2016;30(4):72–80. doi:10.1109/mnet.2016.7513867.
118. Qiu T, Wang X, Chen C, Atiquzzaman M, Liu L. TMED: a spider-web-like transmission mechanism for emergency data in vehicular ad hoc networks. *IEEE Trans Veh Technol.* 2018;67(9):8682–94. doi:10.1109/tvt.2018.2841348.
119. Aliyu A, Abdullah AH, Kaiwartya O, Cao Y, Lloret J, Aslam N, et al. Towards video streaming in IoT environments: vehicular communication perspective. *Comput Commun.* 2018;118(12):93–119. doi:10.1016/j.comcom.2017.10.003.
120. Han G, Wan L, Shu L, Feng N. Two novel DOA estimation approaches for real-time assistant calibration systems in future vehicle industrial. *IEEE Syst J.* 2017;11(3):1361–72. doi:10.1109/jsyst.2015.2434822.
121. Lin K, Li C, Fortino G, Rodrigues JJPC. Vehicle route selection based on game evolution in social Internet of vehicles. *IEEE Internet Things J.* 2018;5(4):2423–30. doi:10.1109/jiot.2018.2844215.
122. Liu R, Liu A, Qu Z, Xiong NN. An UAV-enabled intelligent connected transportation system with 6G communications for Internet of vehicles. *IEEE Trans Intell Transp Syst.* 2023;24(2):2045–59. doi:10.1109/tits.2021.3122567.
123. Sun Z, Liu Y, Wang J, Li G, Anil C, Li K, et al. Applications of game theory in vehicular networks: a survey. *IEEE Commun Surv Tutor.* 2021;23(4):2660–710. doi:10.1109/comst.2021.3108466.
124. Gupta N, Manaswini R, Saikrishna B, Silva F, Teles A. Authentication-based secure data dissemination protocol and framework for 5G-enabled VANET. *Future Internet.* 2020;12(4):63. doi:10.3390/fi12040063.
125. Bathla G, Bhadane K, Singh RK, Kumar R, Aluvalu R, Krishnamurthi R, et al. Autonomous vehicles and intelligent automation: applications, challenges, and opportunities. *Mob Inf Syst.* 2022;2022:7632892. doi:10.1155/2022/7632892.
126. Bui KHN, Jung JE, Camacho D. Game theoretic approach on real-time decision making for IoT-based traffic light control. *Concurr Comput Pract Exp.* 2017;29(11):e4077. doi:10.1002/cpe.4077.
127. Lidkea VM, Muresan R, Al-Dweik A. Convolutional neural network framework for encrypted image classification in cloud-based ITS. *IEEE Open J Intell Transp Syst.* 2020;1:35–50. doi:10.1109/ojits.2020.2996063.
128. Silva R, Iqbal R. Ethical implications of social Internet of vehicles systems. *IEEE Internet Things J.* 2019;6(1):517–31. doi:10.1109/jiot.2018.2841969.

129. Salazar-Cabrera R, de la Cruz ÁP, Molina JMM. Proof of concept of an IoT-based public vehicle tracking system, using LoRa (long range) and intelligent transportation system (ITS) services. *J Comput Netw Commun.* 2019;2019:9198157. doi:10.1155/2019/9198157.
130. Sharma N, Chauhan N, Chand N. Security Challenges in Internet of Vehicles (IoV) environment. In: *Proceedings of the 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*; 2018 Dec 15–17; Jalandhar, India. p. 203–7.
131. Mahrez Z, Sabir E, Badidi E, Saad W, Sadik M. Smart urban mobility: when mobility systems meet smart data. *IEEE Trans Intell Transp Syst.* 2022;23(7):6222–39. doi:10.1109/tits.2021.3084907.