Towards Secure Internet of Things-Enabled Intelligent Transportation Systems: A Comprehensive Review

Changxia Lu[1]*, Fengyun Wang[2]
Heze Vocational College, Heze 274000, Shandong, China[1]
Heze Engineering Technician College, Heze 274000, Shandong, China[2]

***Abstract*—The Internet of Things (IoT) constitutes a technological evolution capable of influencing the establishment of smart cities in a wide range of fields, including transportation. Intelligent Transportation Systems (ITS) represent a prominent IoT-enabled solution designed to enhance the efficiency, safety, and sustainability of transport networks. However, integrating IoT with ITS introduces significant security challenges that need to be addressed to ensure the reliability of these systems. This research aims to critically analyze the current state of IoT-integrated ITS, identify security threats and vulnerabilities, and evaluate existing security measures to propose robust solutions. Utilizing a comprehensive review methodology that includes literature analysis and expert interviews, we identify key achievements and pinpoint critical security gaps. Our findings indicate that while substantial progress has been made in securing ITS, significant challenges remain, particularly regarding scalability, interoperability, and real-time data processing. The study proposes enhanced security protocols and methods to mitigate these risks, contributing to the development of more secure and resilient IoT-enabled ITS.**

***Keywords*—Internet of Things; intelligent transportation; security; logistics**

I. Introduction

The Internet of Things (IoT) seamlessly transforms real-world objects, vehicles, home appliances, etc., into digital ones [1]. With IoT, ordinary things can instantly collect, share, and analyze data by integrating sensors, actuators, and communication technologies [2]. These gadgets, commonly known as intelligent things, can connect to each other independently or through centralized platforms, creating an ever-changing and widespread ecosystem [3]. The main goal of IoT is to optimize productivity, streamline processes, and provide practical information by leveraging the uninterrupted data stream from these connected devices [4]. The IoT has a far-reaching impact on various areas, including smart homes, cities, industrial applications, and healthcare systems [5]. It can revolutionize our interactions with the natural world and bring improvements by enabling continuous communication and cognitive analysis of data [6].

Intelligent Transportation System (ITS) combines multiple technologies to improve transport networks' effectiveness, safety, and environmental friendliness [7]. ITS uses information and communications technology to enhance the effectiveness and control of various transportation methods [8]. This includes multiple transport networks such as highways, trains, airlines, and sea connections [9]. ITS covers multiple applications, including real-time traffic monitoring, the operation of traffic signals that adapt to changing conditions, automated vehicle systems, and services that provide information to travelers [10, 11]. ITS strives to combat congestion, minimize travel times, improve safety through accident prevention systems, and advocate for environmentally friendly behavior through data-driven solutions. The integration of sensors, communication networks, and intelligent algorithms promotes a responsive and adaptable transport infrastructure [12].

The IoT is essential to ITS as it can completely transform and boost transportation networks' efficiency, safety, and utility [13]. The IoT combines physical objects, sensors, and communication technologies, enabling instant data collection and exploration [14]. In the ITS context, this connectivity allows for unprecedented levels of automation and responsiveness [15]. IoT empowers vehicles and infrastructure components to communicate, providing real-time traffic management, proactive maintenance, and flexible control systems [16]. Real-time monitoring to monitor traffic conditions, infrastructure health, and vehicle behavior increases decision-making accuracy, reduces congestion, and improves safety [17]. Furthermore, the IoT facilitates the development of intelligent transport networks, where data-driven analytics empower authorities and users to make informed decisions and ultimately promote sustainable and resilient urban mobility. Integrating IoT technology into ITS improves operation effectiveness [18].

Deploying IoT-enabled ITS poses numerous challenges, particularly in terms of security. The interconnection of IoT devices in transport networks introduces a variety of potential vulnerabilities that different types of attacks can exploit [19]. Unauthorized access, data breaches, and cyber-physical attacks can jeopardize transport infrastructure security and reliability. Privacy concerns also arise from IoT devices, which generate sensitive data such as location information and travel history [20]. Keeping this data confidential and secure is crucial. In addition, the wide range of devices in ITS leads to difficulties in compatibility and standardization. This makes building consistent security procedures more complex. As transportation systems become increasingly dependent on the IoT, it is critical to prioritize security concerns. This is necessary to maintain

public trust, protect critical infrastructure, and promote advanced and connected transport networks [21].

The present study aims to achieve several key objectives to enhance the understanding and advancement of ITS enabled by IoT technology. The study's primary goal is to comprehensively analyze the current status of IoT applications in the transportation industry, focusing on their contribution to intelligent logistics and improved mobility. In addition, the study identifies and examines the security barriers associated with IoT integration in transportation, with a particular focus on risks, weaknesses, and privacy issues. Third, it aims to explore and evaluate the security mechanisms and protocols developed to address these difficulties and provide insights into the most effective methods for ensuring IoT-powered ITS reliability and strength. The survey also presents successful schemes and practical applications, giving an overview of the practical elements of implementing secure IoT solutions in transportation. The study achieves these goals by providing a comprehensive resource for determining the future of safe and efficient ITS.

The remainder of the paper is arranged in the following manner. Section II describes the IoT environment in the ITS context and outlines an overview of critical elements and functions. Section III provides a thorough analysis of IoT-enabled ITS security challenges. Section IV examines a range of security methods and protocols, covering intrusion detection, encryption, and authentication systems. Section V focuses on forecasting future advances and outlines future research directions for IoT-secure applications in transportation. Section VI concludes the paper.

II. Background

The IoT ecosystem in ITS represents a complex integration of interconnected components and technologies to transform the transportation industry. This ecosystem consists of intelligent vehicles, infrastructure components, communication networks, and central control systems, all working together to make transport networks more efficient, safe, and sustainable [22]. Intelligent vehicles are critical components of the IoT-based ITS ecosystem. These vehicles are equipped with multiple sensors, including GPS, accelerometers, and cameras, that constantly collect and send real-time data about their condition, location, and environment. The voluminous data received is the key to making well-founded decisions and adapting the transport system flexibly [23].

The infrastructure components in the IoT environment consist of a network of intelligent traffic lights, road sensors, and monitoring systems. These components are strategically placed throughout the transport network. These components collect and examine data about vehicle movement, road conditions, and hazards. The smooth integration of these components enables a comprehensive understanding of the traffic ecosystem and allows authorities to proactively address dynamic circumstances, optimize traffic signals, and improve overall traffic management. Communication networks are critical for connecting the many components of the IoT ecosystem and facilitating information transfer between automated vehicles and infrastructure. Efficient and reliable communication is crucial for the immediate coordination and synchronization of various components within the transport system. Central control systems serve as a cognitive operations center, analyzing incoming data, formulating intelligent judgments, and issuing instructions to improve performance, minimize congestion, and optimize traffic flow [24].

A. IoT-Enabled ITS Architecture

When implementing an IoT-based ITS, it is necessary to consider a wide range of transportation infrastructures, vehicles, and objects. This approach focuses exclusively on advancing particular business requirements, altering current transportation networks, integrating shared information resources, and simultaneously transforming unique company demands. To incorporate the IoT into ITS, it is crucial to establish a well-designed architecture for an ITS inside the IoT framework. The IoT-based intelligent transportation architecture consists of three layers: identification, network, and application, as depicted in Fig. 1.

The primary role of the identification layer is to gather precise traffic data promptly. The use of various sensors and communication networks primarily determines traffic information. These include video capture tools, ultrasonic detectors, microwave radar sensors, temperature measurement devices, and pressure sensors. Upon the transmission of sensor data across Wireless Sensor Networks (WSNs), the process of data aggregation is eventually finalized [25].

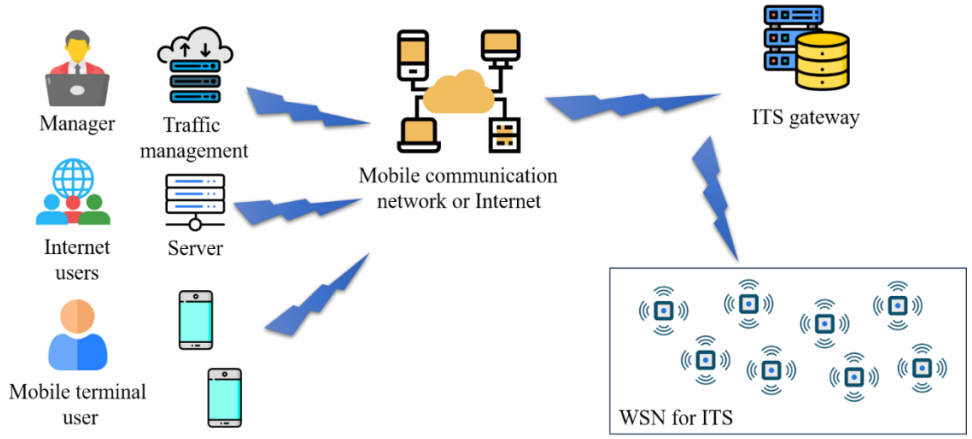

Fig. 1. Architecture of IoT-based ITS.

The primary objective of the network layer is to guarantee traffic data transmission with a significant degree of dependability and protection. The network layer must be able to create a link between application and sensor layers [26]. Communication networks with significant capacity are necessary for effective and reliable information transfer. There are two kinds of communication networks: wireless and wired access networks. Wireless access networks incorporate traditional cell phone networks and Wireless Local Area Network (WLAN) systems that may be used with mobile sensing devices. Wired access networks rely on telephone lines and Ethernet channels, which are well-suited to facilitating tools like traffic junction cameras and subterranean detecting coils.

The application layer processes, analyzes, and uses traffic data gathered by traffic-aware networks and provides diverse intelligent traffic services [27]. The application layer encompasses several systems, such as illustrations, including prototype systems for government and social applications and industrial and corporate applications. Common uses encompass sophisticated traffic management systems and live traffic data services. A system may consist of an advanced electronic toll-collecting system, a public transit management system, and a cutting-edge car.

WSNs are self-organizing networks designed explicitly for ITS tasks. These networks generally include sensor nodes deployed within a designated area for environmental tracking. These nodes are equipped with indicators, inbuilt processing units, and radio transmitters, allowing them to carry out activities such as collecting traffic information, analyzing data, and forwarding it [28]. These nodes establish a network to oversee and analyze environmental data or traffic items inside the designated detection region by utilizing wireless connection and self-organization. Subsequently, the gathered data and information are transferred to the convergence node to carry out specific monitoring duties as specified. The ITS gateway is the intermediary between two separate networks, granting connectivity to general and traffic-aware networks.

Moreover, it facilitates the transformation of communication protocols and the management of networks between the two networks. Once traffic data gathered by the monitoring system is sent to the public network via the gateway, it becomes accessible to the traffic control system that processes data, evaluation, preservation, and reaction actions.

B. Architectural Design of Vehicle Communication Networks

Mobile communication networks typically encompass communication between vehicles and roadside facilities. Roadside facilities include fixed nodes like petrol pumps, comfort service locations, and speed control signs, which are considered a specific type of mobile node. In terms of overall network architecture, there is no fundamental distinction [29]. Mobile Ad-hoc Networks (MANETs) are transient networks consisting of mobile devices sharing the same service set, lacking an Access Point (AP) to connect them. This type of network emphasizes self-organization, distributed, mobile, wireless, and multi-hop communication without using base station equipment. The network's dynamic links allow free movement, resulting in a topology that changes quickly and unpredictably. MANETs function as standalone networks or connect to the broader Internet.

MANETs comprise mobile nodes, which can function as main routers or ordinary nodes distributed across various platforms such as aircraft, aircraft, vessels, buses, cars, people, etc. [30]. This results in the following attributes: 1) Restrictions on connectivity and bandwidth, primarily arising from the constrained wireless channel compared to wired channels; 2) A constantly evolving network structure due to the continuous movement of vehicles; 3) Energy constraints on mobile terminals necessitate energy conservation and reliable energy supply considerations; 4) Poor network security, attributed to public and distributed wireless networks, makes them highly susceptible to interception attempts. The application of mobile self-organizing networks extends across both civilian and military sectors. In the military, troops, vessels, aircraft, and other elements may create decentralized networks utilizing mobile node technology, which improves dependability by distributing the network's functions. MANETs are versatile and have a self-organizing character, making them useful in many civilian settings such as vehicle communication networks, private local networks, emergency rescue services, and workplace meetings.

In the current network protocol architecture, two widely recognized models are the standard Open Systems Interconnection (OSI) protocol and the TCP/IP model widely applied to computer networks. In MANETs, each mobile node establishes its wireless network, introducing distinctions from wired networks operating over the TCP/IP protocol. While the Vehicular Ad Hoc Network (VANET) falls under the category of MANET, the protocol settings at each layer exhibit notable differences. VANET emphasizes the predictability of vehicular trajectories and the impact of obstacles in urban environments. Fig. 2 compares the architecture of the OSI, TCP/IP, VANET, and MANET protocols. Network protocol design for vehicle communication is built upon the TCP/IP model. Subsequent discussions discuss the structure, properties, and current studies on the different tiers within vehicle communication systems.

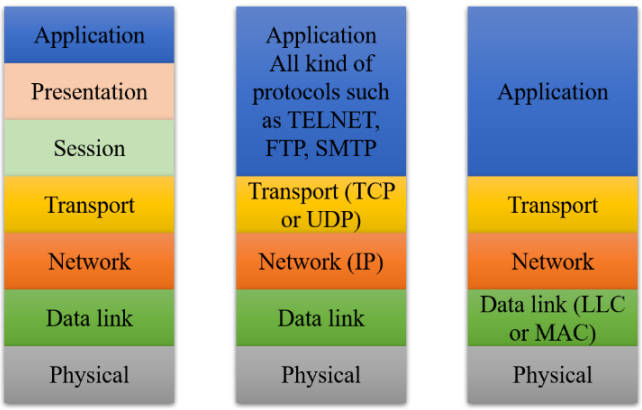

Fig. 2. OSI, TCP/IP, MANET, and VANET architectures.

In VANETs, the physical and Medium Access Control (MAC) layers are commonly grouped and referred to as a PHY/MAC layer. Various frequency bands, such as high-frequency, microwave, millimeter, and infrared wavelengths, are employed in vehicular communications. The Federal

Communications Commission (FCC) in the United States has assigned a specific frequency range of 75MHz, called Dedicated Short-Range Communication (DSRC), for vehicular connection. This frequency range spans from 5.850GHz to 5.925GHz. Similar allocations have been made in Europe and Japan. The PHY/MAC layer in in-vehicle communication networks encounters several challenges. These challenges encompass maintaining reliable communication among vehicles, efficiently allocating broadcast spectrum, adjusting to variations in node density, and ensuring Quality of Service (QoS) for emergency applications within a wireless environment.

The network layer of VANETs focuses on routing protocols, drawing inspiration from MANETs research but incorporating features suitable for traffic communication scenarios. VANETs are characterized by linear networks, fast-moving nodes with predictable trajectories, and the ability to obtain node positions using GPS. Rapid changes in network topology due to high-speed movement pose challenges in establishing and maintaining communication links. There are several types of routing protocols, including location-based (GPSR, MDDV), multicast (MAODV, MOLSR), and unicast (DSR, AODV).

The VANET network protocol design follows the TCP/IP paradigm; however, modifications are required to address the constraints of conventional TCP protocols in wireless networks. Studies have shown that TCP protocols may not be suitable for VANETs, especially when there is a lot of network congestion. Although some enhanced TCP protocols apply to VANETs, most studies focus on User Datagram Protocol (UDP) connections. The security of VANETs is of utmost importance due to their direct influence on the well-being of individuals. The security usages of VANET protocols are subject to stringent requirements that prioritize dependability, confidentiality, and authenticity of sent data throughout communication.

C. Integration of Mobile Model and Network Simulation Software

For VANETs to utilize vehicle movement models, compatibility with network simulation software is essential. Most historical and contemporary mobile models employed by research institutions fall into this category, as illustrated in Fig. 3. Simulation software generates different scenes before simulation, analyzing them according to predetermined path formats. The motion scenes remain unmodifiable, leading to a lack of interaction between the network and mobility domains. In recent years, increased demands for interaction, driven by specialized applications in vehicle communication, have fostered improved collaboration between these domains.

The embedded technique addresses the absence of protocols by facilitating collaboration between networks and movement domains, as shown in Fig. 4. This solution features a straightforward and effective interface between the network and mobile models, leveraging validated driving patterns and carefully following established protocols. Vehicle self-organizing network simulation has emerged as an essential area of study.

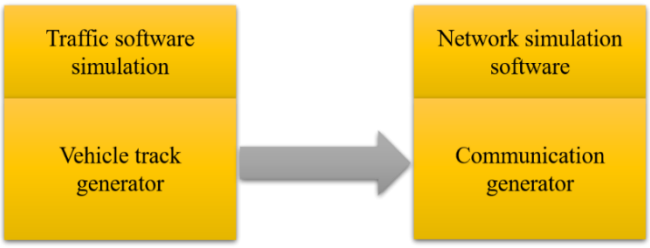

Fig. 3. Illustration of vehicle movement models used in VANET simulation software.

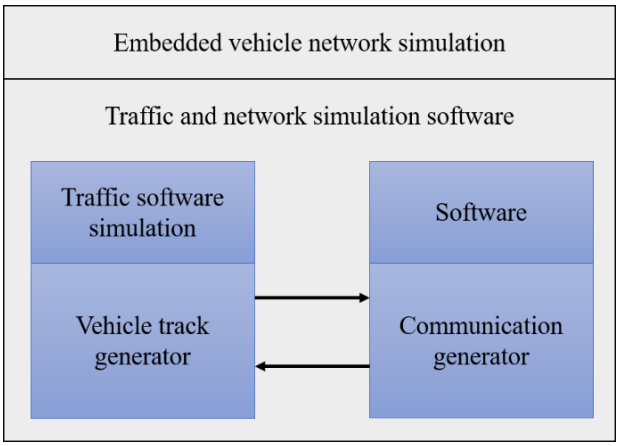

Fig. 4. Integration of embedded technique for collaboration between network and movement domains.

Fig. 5 depicts incorporating conventional network simulation software into mobile applications or specialized traffic simulation software via standardized interfaces. The increasing integration of simulation software results in novel applications, including safe transportation solutions. Initially, application simulations in the early stages were mostly centered around the network. However, as vehicle self-organizing network applications have progressed, there has been a change in emphasis towards simulating vehicle mobility in these applications. Although research is now moving towards the integration and interplay of different approaches, the three methodologies, namely isolated, blended, and embedded, persist in simultaneous existence. The isolated technique is preferred for its broad applicability and simplicity, especially in traffic management and safety, where scholars tend to prefer combining and integrating methods.

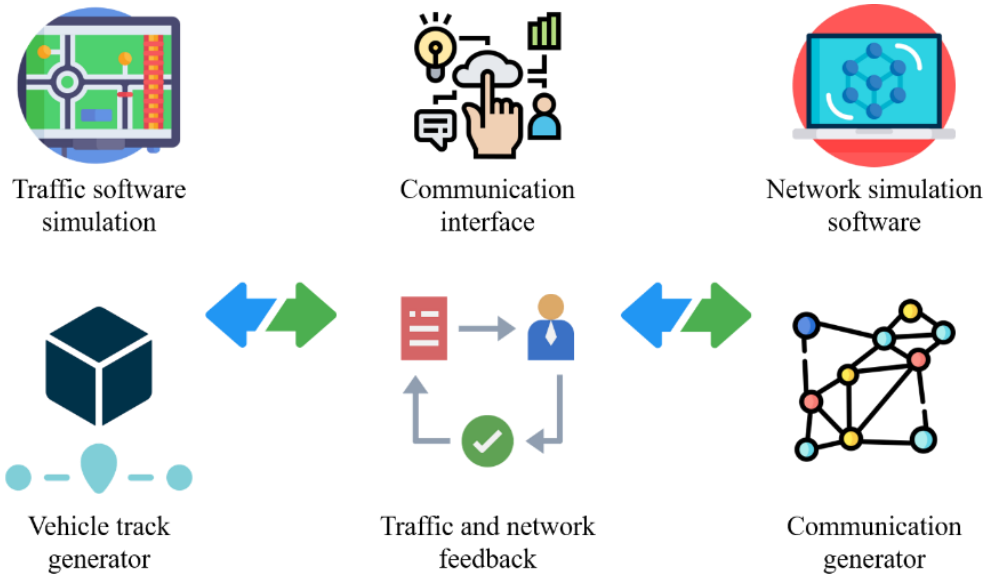

Fig. 5. Integration of conventional simulation software for networks with mobile models or specialized traffic simulation software.

III. Security Challenges in IoT-Enabled ITS

This section covers the complex security concerns in the context of IoT-enabled ITS. As illustrated in Fig. 6, incorporating IoT technology into transportation infrastructure has several prospects for enhanced efficiency and innovation while simultaneously introducing new possibilities for malicious activities and vulnerabilities. As connectivity between vehicles, sensors, and infrastructure rises, protecting these systems from unscrupulous individuals and illegal entry becomes more complex. The security difficulties in IoT-powered ITS present numerous challenges, including maintaining data transmission integrity and defending against cyber-physical attacks. These concerns are constantly changing and need constant attention. Through analyzing these challenges and examining possible methods to reduce their impact, our objective is to provide valuable knowledge on strengthening the capacity of IoT-enabled transportation networks to cope with and maintain their functionality in the presence of ever-changing cyber threats.

A. Vulnerabilities in Connected Devices

The widespread adoption of IoT devices in the ITS sector exposes various vulnerabilities. Intelligent automobiles, road infrastructure, and communication networks are susceptible to cyber assaults. Device setups that are not secure, delayed software upgrades, and inadequate authentication techniques can create vulnerabilities that allow hostile actors to undermine the integrity and performance of connected transportation components. Resolving these vulnerabilities is crucial for enhancing the overall security of transportation systems driven by IoT technology.

Urban traffic congestion is a significant issue in modern cities, and ITS is being researched to address this issue. Zhang and Lu [11] used OPNET Modeler software to develop a vehicle tracking scheme, analyzing vehicle communication networks in an IoT-based system. Simulation experiments showed that low-speed vehicles can improve wireless network coverage, especially when roadside units are kept between 500m and 600m away. The AODV protocol proved more appropriate for network communication requirements than the DSR protocol, improving overall performance.

Anand, et al. [31] presented a threat architecture for IoT devices, concentrating vulnerabilities in a three-layer baseline design. They investigate weaknesses taken advantage of in different assault areas and assess the difficulties in measuring them. The research also examines ITS and secure energy management in smart grids, specifically emphasizing IoVT applications. Implementing the suggested framework into current apps raises concerns among developers over potential security risks inside the system, underscoring the need to address these weaknesses in IoT devices.

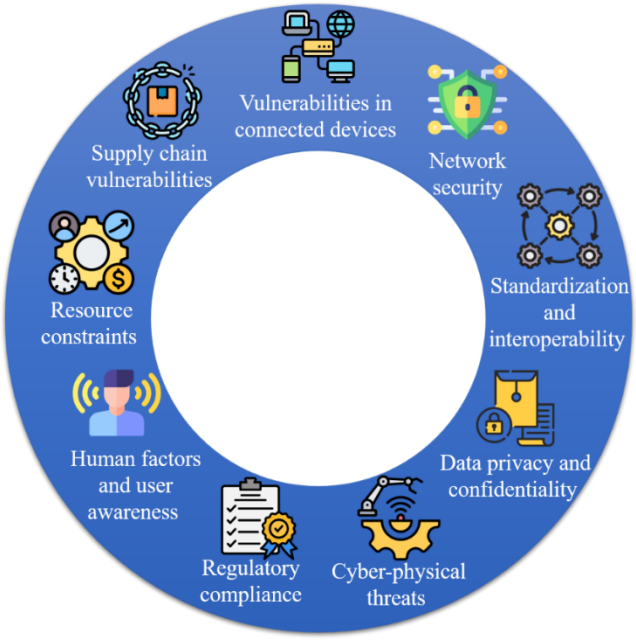

Fig. 6. Security challenges in IoT-enabled ITS.

Ribeiro, et al. [32] have proposed a deep-learning algorithm for enhancing traffic behavior security. They present a policy gradient approach to identifying vehicular misuse, using a triple network replay method to maximize convergence rates. The model is tested on accurate urban maps with 5G or 6G communications, cellular networks, and VANET in a software-defined network. Compared to related studies, the results show improved accuracy prediction, cumulative reward, and convergence rate. The proposed deep learning algorithm improves ITS by increasing the accuracy of predictions, reducing communication delays, and adjusting traffic paths to accommodate congestion.

Alladi, et al. [33] developed a set of deep learning-based misbehavior classification approaches for intrusion detection in IoV networks using LSTM and CNNs. The DCLEs, deployed on vehicular edge servers, identify 18 behaviors with higher F1-scores. The proposed classifiers were compared with existing studies on edge server simulation testbeds. Rani and Sharma [34] propose an ITS framework for IoT-based vehicular network traffic in smart cities using tree-based decision trees, random forests, extra trees, and XGBoost machine learning models. Simulation results show a high level of detection accuracy and low computational requirements.

B. Data Privacy and Confidentiality Concerns

The significant volume of sensitive data collected by IoT devices in the transportation industry, including real-time location information and driving behavior, raises important concerns regarding data privacy and confidentiality. Unauthorized access to this data can lead to identity theft, illegal spying, and misuse of personal information [35]. Utilizing robust encryption techniques and implementing stringent access controls are crucial to safeguard user privacy and instill confidence in the secure deployment of IoT in transportation.

Belhadi, et al. [36] have developed a secure and scalable system for detecting knowledge from urban traffic data using blockchain learning technology and a threaded GPU. The system uses optimizations and a reinforcement deep learning algorithm to merge local knowledge into global knowledge. Experiments on well-known data show the framework outperforms baseline solutions for outlier detection. Tang, et al. [37] presented a flexible and privacy-preserving query protocol for ITS, utilizing matrix decomposition techniques for flexible route organization and ciphertext state operation for route protection. The scheme improves computational and communication overhead, making it suitable for resource-constrained vehicles.

Das, et al. [38] propose blockchain-based identity generation and management methods to deal with security concerns in ITS applications. The solution ensures the validity of Personal Identification Information (PII) and the application's usability, making it suitable for vehicle administration in ITS. Thapliyal, et al. [39] developed SAKP-ITS, a secure authentication protocol for IoV-enabled ITS, demonstrating resistance to potential threats and outperforming competitors in communication, computation, and security metrics. The protocol's practical implementation is also presented to test its effect on critical performance attributes.

C. Network Security Risks

The interconnectivity of IoT devices is primarily dependent on communication networks. Nevertheless, this mutual dependency gives rise to network security vulnerabilities, such as denial-of-service (DoS) assaults, man-in-the-middle attacks, and eavesdropping. Implementing encryption, intrusion detection, and prevention tools can be crucial steps to limit risks and ensure the robustness of the transportation network. Bi, et al. [40] utilized the cryptographic-integrated steganography methodology for secure communication on an IoT-enabled cloud platform for urban transportation. The algorithm produces code for privacy, converts data into a specific format, and uses encryption keys to protect confidential data. The findings demonstrate efficient and secure data sharing.

The development of ITS has led to the development of communication frameworks for addressing security concerns related to intelligent sensors. Rawashdeh, et al. [41] proposed an efficient query-as-a-service communication scheme that incorporates fog computing concepts, communication standards that ensure data integrity and security evaluation tailored to mobile vehicles in ITS applications. The data-driven approach allows entities to share data structures instead of data itself, reducing the communication burden and allowing misinformation tolerance. Experiments have shown superior performance concerning data granularity, detection rate, false-detection rate, and probability of query failure, overcoming traditional cloud-based models' limitations. Table I shows summary of security measures and protocols in IoT-enabled ITS.

TABLE I. SUMMARY OF SECURITY MEASURES AND PROTOCOLS IN IOT-ENABLED ITS

Security measure	Advantages	Limitations
Authentication	Enhances user and device identity verification	Implementation complexity and potential for false positives
Encryption	Secures data in transit and at rest	Computational overhead and potential compatibility issues
IDPS	Continuous monitoring and threat detection	False positives/negatives and resource-intensive
Secure communication protocol	Lightweight and secure data exchange	Protocol compatibility and potential latency issues
Firmware updates and patch management	Addresses vulnerabilities promptly	Operational disruptions during updates and user compliance
RBAC	Granular control over user and device access	Complexity in role assignment and potential misconfigurations

Shen, et al. [42] propose the IoT-assisted Innovative Data Integrity Verification Scheme (IoT-IDIVS) to integrate transportation system data and exchange information effectively. The system aligns GPS data with passenger and schedule information to maintain reliability. The IoT-IDIVS has improved measurement costs and coordination costs, with experimental results showing a packet loss rate of 21.3%, average service delay of 26.9%, data transmission ratio of 95.5%, throughput bit of 92.3%, traffic congestion ratio of 92.6%, error rate of 17.9%, successful delivery rate of 92.57%, and energy optimization of 97.12%.

Altaf, et al. [43] investigate the Beacon Non-Transmission (BNT) attack in ITS, where the attacker is a source vehicle. They propose two lightweight techniques to detect BNT attacks: one based on beacon loss distribution and loss due to channel error and another using autocorrelation function (ACF) to identify shortish and longish attacks. They also propose a random inspection model to balance detection accuracy with limited computational resources. Extensive simulations show the lightweight nature of both techniques and the effectiveness of ACF-based techniques.

D. Lack of Standardization and Interoperability

The lack of established security protocols and interoperability standards across various IoT devices in transportation limits the development of unified security solutions. Implementing universal security measures can be problematic in heterogeneous systems due to the varied degrees of protection [44]. Developing universal standards and protocols that provide secure communication, authentication, and data integrity is crucial for building a robust security framework for IoT-enabled mobility.

Baker, et al. [45] propose a lightweight framework for smart transportation systems, integrating blockchain for authentication and fog computing for efficient and secure transportation. They consider future technologies of 5G and Beyond 5G (B5G) and argue that integrating these technologies, federated learning, blockchain, and edge computing provides the perfect platform for an intelligent transportation system. The framework is evaluated by comparing it to the current cloud-based approach in iFogSim, and the blockchain-based authentication is estimated using a customized implementation. The simulation results show superior security, latency, and energy consumption performance.

Smart cities, particularly in China, are rapidly developing globally, with over 1000 cities undergoing development as of 2017. However, there is a lack of uniform understanding of these systems, potentially affecting their evaluation and planning. Self-organizing system theory can help explain these cities. Yan, et al. [46] conducted qualitative data analyses and developed a comprehensive system framework for smart cities, focusing on smart devices, Information and Communications Technology (ICT), and developmental mechanisms. They used China's smart transportation systems as a case study.

Singh, et al. [47] highlighted the importance of digitalization in highways for a sustainable environment. It categorizes digitalization into five subcomponents: bright highway lighting, traffic and emergency management, renewable energy sources, bright display, and AI. The study proposes an architecture for intelligent highway lighting, traffic, and emergency management, integrating AI for road safety and recommending innovative reflectors, renewable energy adoption, vehicle-to-vehicle communication, and intelligent lampposts for highway implementation.

Dahooie, et al. [48] developed a portfolio matrix to identify IoT applications in urban transportation based on sustainable development and feasibility. They used a hybrid multi-criteria approach, identifying seventeen applications and evaluating their impact on sustainable development. The results showed bike and car sharing as the top priorities for investment in developing countries.

E. Physical Security and Cyber-Physical Threats

In addition to virtual threats, IoT-enabled transportation systems have physical security problems. The manipulation of sensors or disruption of communication between automated vehicles presents a concrete danger in the form of cyber-physical assaults. To strengthen the overall resilience of IoT-enabled transportation infrastructure, it is crucial to ensure the physical security of IoT equipment, including tamper-resistant designs and installing redundant systems. These methods help to prevent cyber-physical threats. To tackle these complex security concerns, a comprehensive solution is needed that integrates technical breakthroughs, regulatory frameworks, and collaborative efforts among companies in the sector.

Traditional risk assessment processes often overlook the importance of physical and cyberspace in IoT-enabled transportation infrastructure. Ntafloukas, et al. [49] propose a new approach for cyber-physical attacks against IoT-based wireless sensor networks. This involves identifying novel cyber-physical characteristics such as threat source, vulnerability, and types of physical impacts. Monte Carlo simulations and sensitivity analysis show that 76.6% of simulated cases have high-risk scenarios and control barriers can reduce cyber-physical risk by 71.8%. The approach is beneficial for stakeholders who are incorporating the cyber domain into risk assessment procedures.

Ntafloukas, et al. [50] propose a new vulnerability assessment approach for transportation networks, combining physical and cyberspace. They use a Bayesian network attack graph and a probability indicator to model vulnerability states. The approach measures network efficiency after removing the highest probability-based nodes. Monte Carlo simulations and sensitivity analysis show vulnerability depends on successfully exploiting vulnerabilities in both cyber and physical spaces. The approach is helpful for stakeholders incorporating cyber domains into vulnerability assessment procedures.

Rajawat, et al. [51] explored the possibility of using a blockchain-based security assurance architecture to protect intelligent roadways and autonomous vehicles within the framework of ITS. The suggested model adopts a semi-distributed approach in deploying blockchain to provide a decent IoV service while maintaining appropriate security measures. The intelligent roads and innovative parking management experiments demonstrate that the suggested

model accomplishes efficient data transmission and decreased latency. This opens up possibilities for using blockchain technology in the IoV for a reliable and trustworthy ITS.

F. Supply Chain Vulnerabilities

The complex supply chain that produces IoT devices for transportation systems presents additional security obstacles. Adversaries might take advantage of weaknesses in the manufacturing process to introduce corrupted components or firmware into devices. To maintain the integrity of the supply chain in IoT-enabled transportation, it is crucial to implement strict quality assurance measures, secure sourcing processes, and ensure transparency. This is necessary to prevent the inclusion of compromised parts that might potentially jeopardize the entire security of the system.

Abizar, et al. [52] developed an innovative energy-based SESLPP technique for sustainable urban city roads, preserving source location privacy while maintaining an accurate reputation based on trust, speed, distance, and acceleration. The method uses an analytical network process for optimal phantom node selection, considering intersections, and provides an optimal platform for smart city communication networks.

The internet has profoundly affected the demand and supply of materials, increasing competition in the industrial industries. Using Industrial IoT (IIoT) in intelligent manufacturing and logistics is crucial for advancing Industry 5.0. It aims to reduce time and cost, enhance customer happiness, and boost organizational profitability. Bhargava, et al. [53] presented an IoT model incorporating intelligent logistics and transportation management to enhance logistics efficiency, improve customer experience, and save costs. The methodology significantly enhanced overall performance by 77% to 98%, resulting in heightened customer satisfaction, increased process efficiency, and reduced operational expenses. The novel IIoT-based architecture provides enhanced energy efficiency and minimal latency performance.

G. Resource Constraints

Most IoT devices used in transportation operate with constrained processing capacity, memory, and energy resources. These limitations may prevent the installation of resilient security solutions. Achieving a harmonious equilibrium between efficient resource utilization and adequate security measures is essential. To effectively tackle security concerns in resource-limited IoT devices, it is crucial to develop lightweight security protocols, minimize resource utilization, and integrate energy-efficient encryption techniques.

Rehman, et al. [54] proposed an intelligent vehicular algorithm using an IoT system (SVA-IoT) to improve transportation systems. The algorithm ensures reliability, reduces device overhead, optimizes routes, and increases intelligence. It also establishes a secure communication structure by identifying authentic devices. The technique was tested through simulated experiments, showing significant improvement over existing work in route optimization and data privacy.

Gadekallu, et al. [55] developed a Moth-Flame Optimization-based ensemble machine learning model for classifying the IDS dataset in ITS. The model uses standard-scaler method normalization and optimal features, trained using linear regression, random forest, and XGBoost algorithms.

The increasing number of vehicles on roads leads to congestion and safety issues. WSN can help address these issues by reducing communication overhead. Gaber, et al. [56] introduced a bio-inspired, trust-based cluster head selection approach for WSN in ITS. The model is energy-efficient, achieves a more extended network lifetime, and has a high average trust value under different malicious node percentages (30% and 50%).

H. Human Factors and user Awareness

Human factors heavily influence the security concerns in IoT-enabled mobility. User actions, such as using easily guessable passwords or vulnerability to deceptive phishing attacks, can potentially undermine the system's overall security. To tackle security concerns connected to humans in the IoT context, promoting user awareness, offering training on cybersecurity best practices, and creating user-friendly security interfaces are crucial.

Din, et al. [57] developed a Context-Aware Cognitive Memory Trust Management System (CACMTM) for ICPTS, utilizing game theory to model trust interactions. The system combines evaluation, decision, update, and knowledge modules to provide a reliable trust management solution for Customer-Centric Communication and Networked Control for ICPTS (CNC-ICTS). The system uses a multi-dimensional trust evaluation model that considers historical behavior, reputation, and contextual information. The system also incorporates a blockchain-secured logging mechanism for security, transparency, and accountability.

Karthikeyan and Usha [58] propose a secure IoT-ITS framework using cognitive science to address risks in the IoT-ITS environment. The framework aims to differentiate legitimate users from malicious ones and perform real-time data analysis. The study aims to resolve security demands without compromise, utilizing cognitive science to distinguish legitimate users from malicious ones.

Strimovskaya and Bochkarev [59] proposed a model for total transportation time (TTT) estimation, considering factors like customer satisfaction, sustainable development, and social aspects. This model enhances transportation system flexibility and planning. The research emphasizes the importance of considering multiple factors in integrated transportation systems planning and control. The model's numerical example for multimodal international conveyance demonstrates its role in information management and control in multi-object systems.

I. Regulatory Compliance and Legal Frameworks

Deploying safe IoT-enabled transportation systems is difficult due to the intricate nature of regulatory compliance and legal frameworks. Uncertainties over jurisdiction, differing regulatory norms, and the absence of a unified legal framework might impede endeavors to implement consistent security measures. Partnerships between industry players and politicians are crucial to establishing precise and enforceable laws that tackle the distinct security problems linked to IoT in transportation while promoting innovation and interoperability.

He, et al. [60] propose a risk prediction-based access control mechanism using a Wasserstein Distance-based Combined Generative Adversarial Network (WCGAN). The model solves gradient disappearance and pattern collapse problems, with a prediction accuracy of 86.3% when training with 5000 nodes. This model improves pattern collapse accuracy and can be used in IoT-based ITS to control access rights, ensure information resource security, and reduce communication delays. The research provides a reference for safe IoV communication.

Even though current solutions for IoT security intended for ITS applications exhibit significant progress, they do not come without drawbacks. These solutions might not be easily scalable to suit a rapidly evolving business. With numerous connection solutions, it becomes hard to have strong security measures to handle the constant flow of connected devices. Recent alternatives are inadequate for optimization as the structure grows, and this is where weaknesses occur as the structure rises. For instance, many lightweight cryptographic algorithms are helpful for IoT devices due to limited resources, and they are not as efficient in scaling up in large numbers. To cope with such scalability problems, security solutions need to be more elastic and resilient.

Another essential attribute that remains a weakness in most IoT models is the compatibility of security protocols between different IoT devices and systems. The absence of unified security measures entails each manufacturer developing their devices with varying security measures, creating a weakness in the whole system's security. The security policies facing these environments are heterogenic and do not allow a comprehensive defense, which creates difficulties in achieving uniformity of the necessary level of protection. However, the requirements for real-time data processing in ITS are as follows: Improving security can sometimes compromise response time and thus has considerable drawbacks, especially for safety-critical applications such as self-driving cars and real-time traffic control. The question of achieving the right level of security while meeting the prerequisites for real-time and high-speed processing is still one of the most challenging in the field.

IV. Discussion

The study outlined and discussed several security issues associated with IoT-based ITS systems. In the transportation system, IoT poses several risks, including outsiders' access, threats to internal data, and other malicious cyber-physical threats. These threats primarily stem from the enhanced interconnection between cars, on-board sensors, and road systems that provide more opportunities for an adversary. This research underscores the importance of more frequent scans and changes to IT security measures to deal with such threats.

Authentication is crucial for ensuring the security of IoT-enabled ITS. By implementing robust authentication techniques, the network may be accessed only by authorized devices and users. Typical authentication methods encompass biometrics, cryptographic certificates, and multi-factor authentication. Biometric techniques, such as fingerprint or facial recognition, may enhance user-specific authentication, while cryptographic certificates provide a secure means of identifying devices inside the IoT network.

Ensuring data security while being transmitted and stored is paramount in IoT-enabled ITS. Encryption methods, such as Transport Layer Security (TLS) for communication channels and Advanced Encryption Standard (AES) for data storage, protect against interception and unwanted entry. By employing robust encryption techniques, the transportation network guarantees the secrecy and reliability of sensitive data shared among devices and systems.

Symmetric key encryption, also known as secret-key cryptography, utilizes an identical key for both encryption and decryption. This technique guarantees the protection of sensitive information by transforming the original text into an encrypted form that can only be decrypted with a mutually agreed-upon key. Nevertheless, the difficulty is in safely disseminating and monitoring the confidential keys. Popular algorithms like AES employ symmetric key encryption to secure sensitive data, files, and communications.

Intrusion Detection and Prevention Systems (IDPS) are vital in identifying and mitigating security threats inside the IoT ecosystem. These systems continually track network traffic and device activity, detecting abnormalities or malicious behaviors. Once detected, the IDPS can promptly generate warnings or autonomously implement preventative measures, protecting against unauthorized entry, data breaches, and other security breaches.

Selecting and implementing secure communication protocols is crucial for preserving data integrity and preventing cyber-attacks. Protocols like MQTT and CoAP provide efficient and secure communication between IoT devices and infrastructure. These protocols include encryption and authentication elements, guaranteeing the secrecy and legitimacy of data sent inside the transportation system.

Transport Layer Security (TLS) and its precursor, Secure Sockets Layer (SSL), are cryptographic protocols created to ensure communication security across a computer network. The TLS and SSL protocols guarantee the secrecy and accuracy of information sent between apps. By encrypting the communication channel, they prevent unauthorized access and eavesdropping, ensuring that sensitive information remains protected during transmission.

Maintaining regular updates to device firmware and effectively managing patches are crucial security practices for reducing vulnerabilities. Implementing up-to-date security patches and firmware upgrades for IoT devices is essential for mitigating vulnerabilities and strengthening the overall resilience of the transportation system. A reliable patch-tracking system is critical for upholding the security of the many devices in the IoT-enabled ITS.

Role-Based Access Control (RBAC) provides a crucial security solution for managing and controlling user rights and privileges in the IoT environment. RBAC ensures that only authorized entities can perform certain activities by giving individuals and devices unique roles and access levels. The ability to have precise control over access helps mitigate the danger of unauthorized entry, minimize the potential for harmful actions, and bolster the overall security of ITS.

V. Recommendations and Future Directions

The section presents suggestions for improving security, privacy, and system efficiency in IoT-enabled ITS networks. We provide comprehensive strategies to enhance resilience against cyber-attacks and assure the safety, intelligence, and interconnectedness of transportation systems. The suggestions include improving security standards and adopting cutting-edge technology, which will provide the groundwork for a forward-thinking conversation about the future of ITS.

Integrating blockchain into IoT-enabled transportation systems faces challenges related to scalability, high energy consumption, and the need for consensus mechanisms. These challenges must be addressed to ensure the feasibility and efficiency of blockchain implementation. IoT-specific blockchain architectures should be explored to develop scalable and energy-efficient consensus algorithms. Blockchain integration can be enhanced by optimizing smart contracts and exploring hybrid solutions that utilize centralized and decentralized elements.

Security concerns arise from the distributed nature of edge computing, where devices process data locally. Critical challenges are ensuring secure communication, access control, and protection against edge device compromise. The development of security frameworks and encryption techniques for edge computing requires further study in the future. Developing intrusion detection systems appropriate for edge environments and implementing effective access control mechanisms can strengthen security.

Machine learning-based anomaly detection systems may face challenges related to false positives, adaptability to dynamic environments, and the need for large labeled datasets. Anomaly detection algorithms should be improved in accuracy and adaptability. Machine learning can be enhanced by leveraging unsupervised learning approaches, exploring transfer learning methods, and developing techniques to handle evolving threats.

The emergence of quantum computing challenges conventional cryptography methods, requiring creating and incorporating cryptographic solutions that can withstand quantum attacks. The future of cryptography should focus on designing and implementing quantum-safe algorithms. Several promising areas for developing quantum-resistant algorithms include post-quantum cryptography, lattice-based cryptography, and hash-based cryptography.

Physical attacks on IoT devices, such as tampering with sensors or communication links, pose significant challenges to maintaining the stability and security of transportation systems. Researchers should investigate mechanisms for preventing physical attacks, such as tamper-resistant hardware, secure bootstrapping, and physical layer security solutions. IoT-enabled transport systems can be more resilient by implementing robust authentication and encryption techniques.

IoT devices often function with restricted processing capacity and power sources, making it difficult to apply security measures requiring significant resources. Research efforts should be directed towards developing lightweight and energy-efficient security protocols. Resource constraints can be addressed while maintaining robust security measures by utilizing efficient key management strategies, optimizing cryptographic algorithms, and leveraging hardware-based security mechanisms.

Ensuring privacy in the collection, storage, and processing of sensitive data within IoT-enabled transportation systems presents challenges related to data anonymization, secure data sharing, and compliance with privacy regulations. The development of advanced privacy-preserving data management techniques, such as homomorphic encryption, differential privacy, and federated learning, should be explored in research. Data privacy can be protected, and data utility can be maximized by implementing secure data-sharing frameworks with granular consent mechanisms.

Traditional authentication methods may be susceptible to identity theft and credential-based attacks, necessitating more secure and user-friendly authentication solutions. User authentication should incorporate behavioral biometrics, such as keystroke dynamics and gait analysis. Authenticating users with these biometric factors provides seamless, non-intrusive experiences that enhance security.

Developing a one-size-fits-all security solution for the diverse range of IoT-enabled devices and applications in transportation is challenging due to varied operational requirements and resource constraints. Hybrid security models that combine centralized and decentralized approaches should be explored in future research. Security measures tailored to the characteristics of each IoT device or application can optimize security without adding unnecessary overhead to resource-constrained devices.

The ethical implications of security measures, such as surveillance and data collection, must be carefully considered to avoid unintended consequences and potential misuse. Security solutions should be designed with ethical considerations in mind. Data collection and usage can be controlled transparently and accountable based on user preferences to address moral concerns and promote responsible IoT-enabled transportation.

VI. Conclusion

The incorporation of IoT technology into ITS offers significant opportunities for improving efficiency, safety, and sustainability in urban and highway transportation. Nevertheless, IoT technology's considerable capacity for change is accompanied by noteworthy security obstacles that desire efficient solutions to guarantee the dependability and durability of IoT-enabled transportation networks. By examining security measures such as authentication mechanisms, encryption mechanisms, intrusion detection and prevention systems, secure communication protocols, device firmware updates and patch management, role-based access control, and other strategies, we have emphasized the significance of thorough and proactive security strategies. Participants might implement robust security measures and follow strict standards to limit the dangers of cyber threats, unauthorized access, data breaches, and cyber-physical attacks. This can assist in establishing trust and confidence in IoT-based transportation systems. Moreover, it is essential to cooperate

among policymakers, industry stakeholders, researchers, and cybersecurity specialists to formulate uniform security frameworks, facilitate information sharing, and develop a culture of awareness about cybersecurity. To maximize the benefits of intelligent transportation in the digital era, it is crucial to prioritize ongoing research and innovation in cybersecurity technologies and processes. This is necessary to protect IoT-enabled ITS networks.

REFERENCES

[1] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research," Journal of Network and Computer Applications, vol. 97, pp. 23-34, 2017.

[2] B. Pourghebleh, V. Hayyolalam, and A. A. Anvigh, "Service discovery in the Internet of Things: review of current trends and research challenges," Wireless Networks, vol. 26, no. 7, pp. 5371-5391, 2020.

[3] W. Liu, "QoS-aware resource allocation method for the internet of things using triplet and heterogeneous earliest finish time algorithms," Proceedings of the Indian National Science Academy, pp. 1-9, 2023.

[4] B. Pourghebleh and V. Hayyolalam, "A comprehensive and systematic review of the load balancing mechanisms in the Internet of Things," Cluster Computing, pp. 1-21, 2019.

[5] M. Soori, B. Arezoo, and R. Dastres, "Internet of things for smart factories in industry 4.0, a review," Internet of Things and Cyber-Physical Systems, 2023.

[6] B. Kaur et al., "Internet of things (IoT) security dataset evolution: Challenges and future directions," Internet of Things, p. 100780, 2023.

[7] Z. Lv and W. Shang, "Impacts of intelligent transportation systems on energy conservation and emission reduction of transport systems: A comprehensive review," Green Technologies and Sustainability, vol. 1, no. 1, p. 100002, 2023.

[8] M. Bargahi, H. Barati, and A. Yazici, "Relationship between Criticality and Travel Time Reliability in Transportation Networks," in 2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC), 2023: IEEE, pp. 2479-2484, doi: https://doi.org/10.1109/ITSC57777.2023.10421885.

[9] K. Zuo et al., "Security enhanced privacy-preserving data aggregation scheme for intelligent transportation system," The Journal of Supercomputing, pp. 1-28, 2024.

[10] G. G. Devarajan, U. Kumaran, G. Chandran, R. P. Mahapatra, and A. Alkhayyat, "Next Generation Imaging Methodology: An Intelligent Transportation System for Consumer Industry," IEEE Transactions on Consumer Electronics, 2024.

[11] H. Zhang and X. Lu, "Vehicle communication network in intelligent transportation system based on Internet of Things," Computer Communications, vol. 160, pp. 799-806, 2020.

[12] F.-Y. Wang et al., "Transportation 5.0: The DAO to safe, secure, and sustainable intelligent transportation systems," IEEE Transactions on Intelligent Transportation Systems, 2023.

[13] Y. Cui and D. Lei, "Design of highway intelligent transportation system based on the internet of things and artificial intelligence," IEEE Access, 2023.

[14] B. Pourghebleh, N. Hekmati, Z. Davoudnia, and M. Sadeghi, "A roadmap towards energy-efficient data fusion methods in the Internet of Things," Concurrency and Computation: Practice and Experience, p. e6959, 2022.

[15] P. Whig, A. Velu, R. R. Nadikattu, and Y. J. Alkali, "Role of AI and IoT in Intelligent Transportation," in Artificial Intelligence for Future Intelligent Transportation: Apple Academic Press, 2024, pp. 199-220.

[16] J. Srinivas, A. K. Das, M. Wazid, and A. V. Vasilakos, "Designing secure user authentication protocol for big data collection in IoT-based intelligent transportation system," IEEE Internet of Things Journal, vol. 8, no. 9, pp. 7727-7744, 2020.

[17] L. Guevara and F. Auat Cheein, "The role of 5G technologies: Challenges in smart cities and intelligent transportation systems," Sustainability, vol. 12, no. 16, p. 6469, 2020.

[18] B. K. Mohanta, D. Jena, N. Mohapatra, S. Ramasubbareddy, and B. S. Rawal, "Machine learning based accident prediction in secure iot enable transportation system," Journal of Intelligent & Fuzzy Systems, vol. 42, no. 2, pp. 713-725, 2022.

[19] C. Liu and L. Ke, "Cloud assisted Internet of things intelligent transportation system and the traffic control system in the smart city," Journal of Control and Decision, vol. 10, no. 2, pp. 174-187, 2023.

[20] S. Verma, S. Zeadally, S. Kaur, and A. K. Sharma, "Intelligent and secure clustering in wireless sensor network (WSN)-based intelligent transportation systems," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 13473-13481, 2021.

[21] N. Yuvaraj, K. Praghash, R. A. Raja, and T. Karthikeyan, "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)," Wireless personal communications, vol. 123, no. 2, pp. 1733-1752, 2022.

[22] P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, K.-K. R. Choo, and Y. Park, "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," IEEE Transactions on Vehicular Technology, vol. 70, no. 2, pp. 1736-1751, 2021.

[23] S. Dhingra, R. B. Madda, R. Patan, P. Jiao, K. Barri, and A. H. Alavi, "Internet of things-based fog and cloud computing technology for smart traffic monitoring," Internet of Things, vol. 14, p. 100175, 2021.

[24] A. Gohar and G. Nencioni, "The role of 5G technologies in a smart city: The case for intelligent transportation system," Sustainability, vol. 13, no. 9, p. 5188, 2021.

[25] M. Mohseni, F. Amirghafouri, and B. Pourghebleh, "CEDAR: A cluster-based energy-aware data aggregation routing protocol in the internet of things using capuchin search algorithm and fuzzy logic," Peer-to-Peer Networking and Applications, pp. 1-21, 2022.

[26] W. Liu, "IoT-based multi-channel information integration method for wireless sensor networks," Proceedings of the Indian National Science Academy, vol. 89, no. 3, pp. 705-714, 2023.

[27] H. Xue, Z. Zhang, and Y. Zhang, "A novel cluster-based routing protocol for WSN-enabled IoT using water-cycle algorithm," Proceedings of the Indian National Science Academy, vol. 89, no. 3, pp. 724-730, 2023.

[28] Z. Xiao et al., "Tensor and Confident Information Coverage based Reliability Evaluation for Large-scale Intelligent Transportation Wireless Sensor Networks," IEEE Transactions on Vehicular Technology, 2023.

[29] S. H. Gopalan, V. Vignesh, D. U. S. Rajkumar, A. Velmurugan, D. Deepa, and R. Dhanapal, "Fuzzified swarm intelligence framework using FPSOR algorithm for high-speed MANET-Internet of Things (IoT)," Measurement: Sensors, vol. 31, p. 101000, 2024.

[30] V. K. Quy, V. H. Nam, D. M. Linh, and L. A. Ngoc, "Routing algorithms for MANET-IoT networks: a comprehensive survey," Wireless Personal Communications, vol. 125, no. 4, pp. 3501-3525, 2022.

[31] P. Anand, Y. Singh, A. Selwal, P. K. Singh, R. A. Felseghi, and M. S. Raboaca, "Iovt: Internet of vulnerable things? threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications towards smart grids," Energies, vol. 13, no. 18, p. 4813, 2020.

[32] D. A. Ribeiro, D. C. Melgarejo, M. Saadi, R. L. Rosa, and D. Z. Rodríguez, "A novel deep deterministic policy gradient model applied to intelligent transportation system security problems in 5G and 6G network scenarios," Physical Communication, vol. 56, p. 101938, 2023.

[33] T. Alladi, V. Kohli, V. Chamola, and F. R. Yu, "A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems," Digital Communications and Networks, vol. 9, no. 5, pp. 1113-1122, 2023.

[34] P. Rani and R. Sharma, "Intelligent transportation system for internet of vehicles based vehicular networks for smart cities," Computers and Electrical Engineering, vol. 105, p. 108543, 2023.

[35] M. A. Tofighi, B. Ousat, J. Zandi, E. Schafir, and A. Kharraz, "Constructs of Deceit: Exploring Nuances in Modern Social Engineering Attacks," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2024: Springer, pp. 107-127, doi: https://doi.org/10.1007/978-3-031-64171-8_6

[36] A. Belhadi, Y. Djenouri, G. Srivastava, and J. C.-W. Lin, "SS-ITS: Secure scalable intelligent transportation systems," The Journal of Supercomputing, vol. 77, pp. 7253-7269, 2021.

[37] L. Tang, M. He, L. Xiong, N. Xiong, and Q. Luo, "An efficient and privacy-preserving query scheme in intelligent transportation systems," Information Sciences, vol. 647, p. 119448, 2023.

[38] D. Das, K. Dasgupta, and U. Biswas, "A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems," Computers and Electrical Engineering, vol. 105, p. 108535, 2023.

[39] S. Thapliyal, M. Wazid, D. Singh, A. K. Das, and S. H. Islam, "Robust authenticated key agreement protocol for internet of vehicles-envisioned intelligent transportation system," Journal of Systems Architecture, vol. 142, p. 102937, 2023.

[40] D. Bi, S. Kadry, and P. M. Kumar, "Internet of things assisted public security management platform for urban transportation using hybridised cryptographic-integrated steganography," IET Intelligent Transport Systems, vol. 14, no. 11, pp. 1497-1506, 2020.

[41] M. Rawashdeh, Y. Alshboul, M. G. A. Zamil, S. Samarah, A. Alnusair, and M. S. Hossain, "A security framework for QaaS model in intelligent transportation systems," Microprocessors and Microsystems, vol. 90, p. 104500, 2022.

[42] X. Shen, Y. Lu, Y. Zhang, X. Liu, and L. Zhang, "An Innovative Data Integrity Verification Scheme in the Internet of Things assisted information exchange in transportation systems," Cluster Computing, vol. 25, no. 3, pp. 1791-1803, 2022.

[43] F. Altaf, K. Prateek, and S. Maity, "Beacon Non-Transmission attack and its detection in intelligent transportation systems," Internet of Things, vol. 20, p. 100602, 2022.

[44] S. Shokouhi, B. Mu, and M.-W. Thein, "Optimized Path Planning and Control for Autonomous Surface Vehicles using B-Splines and Nonlinear Model Predictive Control," in OCEANS 2023-MTS/IEEE US Gulf Coast, 2023: IEEE, pp. 1-9.

[45] T. Baker, M. Asim, H. Samwini, N. Shamim, M. M. Alani, and R. Buyya, "A blockchain-based Fog-oriented lightweight framework for smart public vehicular transportation systems," Computer Networks, vol. 203, p. 108676, 2022.

[46] J. Yan, J. Liu, and F.-M. Tseng, "An evaluation system based on the self-organizing system framework of smart cities: A case study of smart transportation systems in China," Technological Forecasting and Social Change, vol. 153, p. 119371, 2020.

[47] R. Singh et al., "Highway 4.0: Digitalization of highways for vulnerable road safety development with intelligent IoT sensors and machine learning," Safety science, vol. 143, p. 105407, 2021.

[48] J. H. Dahooie, A. Mohammadian, A. R. Qorbani, and T. Daim, "A portfolio selection of internet of things (IoTs) applications for the sustainable urban transportation: A novel hybrid multi criteria decision making approach," Technology in Society, vol. 75, p. 102366, 2023.

[49] K. Ntafloukas, D. P. McCrum, and L. Pasquale, "A cyber-physical risk assessment approach for Internet of Things enabled transportation infrastructure," Applied Sciences, vol. 12, no. 18, p. 9241, 2022.

[50] K. Ntafloukas, L. Pasquale, B. Martinez-Pastor, and D. P. McCrum, "A Vulnerability Assessment Approach for Transportation Networks Subjected to Cyber–Physical Attacks," Future Internet, vol. 15, no. 3, p. 100, 2023.

[51] A. S. Rajawat, S. Goyal, P. Bedi, C. Verma, E. I. Ionete, and M. S. Raboaca, "5G-Enabled Cyber-Physical Systems for Smart Transportation Using Blockchain Technology," Mathematics, vol. 11, no. 3, p. 679, 2023.

[52] Abizar, H. Farman, B. Jan, Z. Khan, and A. Koubaa, "A smart energy-based source location privacy preservation model for Internet of Things-based vehicular ad hoc networks," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 2, p. e3973, 2022.

[53] A. Bhargava, D. Bhargava, P. N. Kumar, G. S. Sajja, and S. Ray, "Industrial IoT and AI implementation in vehicular logistics and supply chain management for vehicle mediated transportation systems," International Journal of System Assurance Engineering and Management, vol. 13, no. Suppl 1, pp. 673-680, 2022.

[54] A. Rehman, T. Saba, K. Haseeb, G. Jeon, and T. Alam, "Modeling and optimizing IoT-driven autonomous vehicle transportation systems using intelligent multimedia sensors," Multimedia Tools and Applications, pp. 1-15, 2023.

[55] T. R. Gadekallu, N. Kumar, T. Baker, D. Natarajan, P. Boopathy, and P. K. R. Maddikunta, "Moth–Flame Optimization based ensemble classification for intrusion detection in intelligent transport system for smart cities," Microprocessors and Microsystems, vol. 103, p. 104935, 2023.

[56] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, "Trust-based secure clustering in WSN-based intelligent transportation systems," Computer Networks, vol. 146, pp. 151-158, 2018.

[57] I. U. Din, K. A. Awan, and A. Almogren, "Secure and Privacy-Preserving Trust Management System for Trustworthy Communications in Intelligent Transportation Systems," IEEE Access, 2023.

[58] H. Karthikeyan and G. Usha, "A secured IoT-based intelligent transport system (IoT-ITS) framework based on cognitive science," Soft Computing, pp. 1-11, 2023.

[59] A. Strimovskaya and A. Bochkarev, "Algorithmic framework for enhancement of information control in integrated transportation systems," Journal of Industrial Information Integration, vol. 35, p. 100512, 2023.

[60] Y. He, M. Kong, C. Du, D. Yao, and M. Yu, "Communication Security Analysis of Intelligent Transportation System Using 5G Internet of Things From the Perspective of Big Data," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2199-2207, 2022.