Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

Systematic Review on Cyber Security in the Internet of Vehicles (IoV)

Nishu Kumari*[1], Shashank Jha[2], Beer Singh[3]

Pawan Kumar[4], Prashant[5]

[1]Department of Computer Science and Engineering, Meerut Institute of Technology, Meerut, India
[2, 4, 5] Computer Science and Application, COER University, Roorkee, Uttarakhand, India
[3]Department of Information Technology, Shree Ramswaroop Memorial College of Engineering and Management
***Corresponding Author:** Lucknownishu041mca23@gmail.com

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

The Internet of Vehicles (IoV) represents a critical evolution in intelligent transportation systems. It is a key advancement in intelligent transportation systems, where vehicles connect and communicate effectively with each other, utilizing great infrastructure that enables real-time data exchange and various advanced features. The paper spells out the attack vectors—such as MITM, DoS, spoofing and malware-based intrusions. However, it also poses some serious cybersecurity threats. This systematic literature review investigates the key security challenges in the IoV landscape and their countermeasures in VANETs through a comprehensive analysis of research conducted from 2015-2024. The review explores a range of security solutions that are currently being studied. Emphasis is focused on cryptographic protocols, machine learning based intrusion detection systems, and blockchain technologies, given their effectiveness, limitations, and suitability for resource-constrained vehicular environments. Even with the substantial progress, challenges remain in achieving real-time threat detection, ensuring interoperability, and developing lightweight yet effective security solutions. This review highlights these gaps and outlines future research directions, advocating for an integrated and adaptive cybersecurity framework according to the dynamic and heterogeneous nature of IoV networks.

Keywords: IoT, Internet of Vehicles (IoV), VANET, AI, Blockchain, Machine Learning, Cyber Security

1. Introduction

The development of the Internet of Things (IoT) has prompted the rapid growth of Internet of Vehicles (IoV), a ubiquitous network environment, which makes the vehicles can communicate with not only vehicles and road-side infrastructure, but also cloud services and users. In traditional VANETs, it can further enhance the performance by including advanced technologies, and one of these advanced technologies is IoV which integrates a number of technologies such as AI, cloud computing and big data analytics. The purpose of these inventions is to improve safety of the roadways and traffic control and to improve the driving experience. IoV will play a key role in

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

connected mobility, as the technology of autonomous vehicles, smart transportation and vehicle to everything (V2X) is quickly growing up.

But this increasing interconnection has severe cybersecurity implications as well. As IoV systems involve real-time data delivery and internet-based communication, they are a target to various cyberattacks. Security weaknesses could be exploited by malicious intruders to take control over automotive systems, to retrieve sensitive user information, or to tamper with traffic infrastructure. These kinds of events can be really quite problematic…ranging from traffic jams to potentially deadly accidents."

With the gradual maturation of the concept and development of the application of IoV in smart cities, intelligent transportation and other fields have defined the development direction of the future, the security of the network and devices IoV become essential. A full assessment of the cyber security issues in IoV is provided in this paper, including major threats, existing defenses and research prospects.

1.1 The Evolution from Vehicular Ad Hoc Networks (VANETs

IoV originated from the concept of Vehicular Ad Hoc Networks (VANETs), which focused on enabling direct communication between nearby vehicles. While VANETs laid the foundation for vehicle-to-vehicle communication, their capabilities were limited by short-range interactions and a lack of integration with larger digital systems. In contrast, IoV builds upon this model by incorporating cloud services, intelligent systems, and real-time data sharing, allowing vehicles to connect with wide traffic infrastructures and personal devices, thereby creating a smarter, more effective transportation environment.

1.2 Essential Components of IoV

1.2.1. Vehicle-to-Vehicle (V2V) Communication: V2V communication allows cars to collect relevant information pertaining to speed, GPS location, and heading. This traffic exchange greatly decreases the likelihood of collision and also aids in the smooth flow of traffic. "Vehicles might immediately alert each other about imminent dangers or sudden braking at a controlled intersection or a merging lane," the researchers hear a distant, creaking-soled Black Mirror-style voiceover say. Real-time information on congestions also enables drivers to re-route in a body efficient way, avoiding delays. This form of technology is integral for intersection safety, situational awareness, and transportation optimization.

1.2.2. Vehicle-to-Infrastructure (V2I) Communication: Vehicles can communicate with the environment through Vehicle to Infrastructure communication (or V2I), in which information is shared with traffic lights, road signs and lane markings. This exchange is essential for the optimization of the traffic performance (for minimization of the congestion). For example, smart traffic signals may be coordinated according to live traffic, so you can spend less time waiting at red lights. Strategic digital signage, dynamic lanes information get drivers where they need to go, safely, quickly. In the big picture, V2I contributes to smoother traffic flow, less congestion and better driving experiences.

1.2.3. Vehicle-to-Pedestrian (V2P) Communication: V2P communication is designed to improve safety of pedestrian, bike and other vulnerable traffic users. The devices allow vehicles to sense and

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

communicate with the people around them being on or near the road through smartphones, wearable devices, or roadside sensors. This system allows for:

• Real-time driver alerts regarding pedestrians in the vicinity,

• Mobility warnings to pedestrians on vehicle approach,

• Better Intersections and Crosswalks Security, specially in urban locations.

This two-way interaction plays an important role in the avoidance of mishaps, and supports a safer cohabitation of the road system between all users.

1.2.4. Vehicle-to-Cloud (V2C) Communication: Vehicle-to-Cloud (V2C) communications enable the exchange of data between vehicles and cloud-based systems. ‘‘That connectivity allows vehicles to receive:

A. Real-time guidance and weather updates,
B. Dynamic traffic information and routing
C. Over-the-air (OTA) services for software updates and diagnostics to included remote updates/logger downloads and programmer enable/disable.

V2C addresses the challenge of keeping vehicles in the loop, connected, and responsive to the dynamic environment and traffic conditions.

1.2.5. Vehicle-to-Services (V2S) Communication: V2S technology connects vehicles to various external service providers, supplementing the features of smart mobility. These services include:

A. Ride-hailing apps including Uber and Lyft,
B. Emergency response systems such as ambulances and breakdown,
C. Live data on fuel/charging stations and service locations.

By fusion with service networks, V2S will provide more convenient, safe, efficient traffic services for the existing new transportation systems.

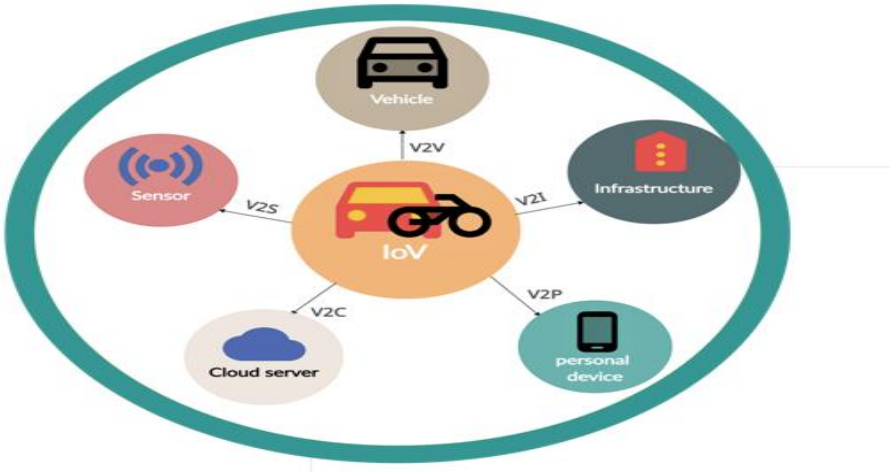

Figure.1 Components of IoV

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

As the backbone of smart city and smart transportation, the Internet of Vehicles (IoV) demands its cybersecurity to be the priority of priorities. IoV systems are tightly connected, have active communication among vehicles, roadside units, humans, cloud services, etc. However, this connectivity, as useful as it is, also brings with it a myriad of vulnerabilities. In view of these issues, the present study provides a Systematic survey on cybersecurity in IoV, discussing critical threats and existing security solutions, pointing out the future trends in the research.

2. Related Work

Several security studies have been conducted with a focus on the security concerns and the possible security solutions of the IoV, including the challenges and solutions for the security of this emerging environment.

Khezri et al. (2025), give a detailed survey on security threats to the IoV as one of the key parts of the ITS in “Security Challenges in Internet of Vehicles for ITS: A Survey”. They classify a number of attacks on data privacy, communication channel and routing protocols. VANETs and wireless communication technologies are however enablers and at the same time, the authors acknowledge that these technologies also introduce new vectors for cyber threats.

One early work in this area from Petit and Shladover studied potential cyber-attacks on automated vehicles. Their work investigated how weaknesses in technologies such as GPS, sensors and in-vehicle communication networks could be used. They also highlighted the importance of strong defines mechanisms for V2V and V2I communications [1].

Lu et al. offered a foundational study on connected vehicle technologies, presenting detailed architectural models, communication layers, and security risks. Their work laid the groundwork for understanding the complexities of maintaining both security and seamless communication in dynamic vehicular environments [2].

Khan and Salah conducted a broad review of IoT security, with a focus on adapting blockchain solutions for vehicular networks. Their study highlighted key issues like data authentication, secure sharing, and decentralized trust—proposing blockchain as a resilient mechanism for IoV environments [3][34].

Ghosh et al. presented an extensive taxonomy of security threats in CAVs such as spoofing, Sybil and DoS attack. The authors considered real-life situations and emphasized that car control systems should be designed to withstand cybersecurity attacks and then used SoS paradigm to develop an architectural framework for connected vehicles [4].

Elaborating on previous works, Petit and Simões presented security and privacy issues in V2X communication, with particular focus on the application of PKI and secure short-range communication and the discussion of location privacy [5].

Another important survey addressed IoV’s data privacy issues, and threats were categorized as message forgery, data sniffing and identity leaks. The effectiveness of cryptographic privacy-preserving authentication mechanisms has been studied as possible mitigation [6].

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

An additional review was done for defence methods including secure routing models, trust models, and anomaly detection mechanisms. The authors stressed on the complete protection from all communication layers of IoV [7].

Hussain and Zeadally in a cyber physical security review introduced an extended view by considering both network based threats and the threats initiated by the interaction between hardware and software in the vehicle [8].

Wang et al. investigated ML application in the security of IoV and how it can be used in intrusion and anomaly detection. These authors stressed the importance of lightweight, real-time ML models that are applicable to in-vehicle or edge deployment [9].

Another survey classified IoV attacks according to the architectural layers (application/network/perception) and a comparison of the existing security solutions was carried out [10]. They suggests targeted improvements for IoV environments [10].

Another submission investigated how blockchain can be integrated with IoV to facilitate secure identity management, trust establishment, and transparent data sharing. The research has shed light on the applications of blockchain-based scheme into the vehicular networks [11].

Lastly, the most recent research to our knowledge was done by Saharkhiz and Farhadi, which explored AI-powered solutions focusing on IoV security. They investigated how machine learning and deep learning approaches can be employed in threat prediction, anomaly detection, and in-vehicle response systems—emphasizing the increasing relation-ship between AI and the automotive security [12]. The growing interconnection of vehicles within the Internet of Vehicles (IoV) paradigm has intensified research into cybersecurity threats, privacy challenges, and countermeasures. Recent surveys and reviews have mapped the landscape of IoV security. Khezri *et al.* [13] provided a comprehensive overview of IoV security challenges in intelligent transportation systems (ITS), identifying attacks on data privacy, routing protocols, and communication channels. Similarly, Singh and Sharma [14] and Rahman *et al.* [17] highlighted critical privacy and trust issues, outlining countermeasures but emphasizing the need for scalable and adaptive defenses. Rony *et al.* [15] focused on trust management and machine learning-based security in IoV, while Ahmed *et al.* [16] explored the integration of sensing and computing as a security enhancer. Salah *et al.* [18] emphasized blockchain's potential in vehicular networks, whereas Alzubaidi and Elnashar [19] conducted a systematic literature review, stressing gaps in intrusion detection and secure data dissemination.

Intrusion detection (IDS) remains a dominant research focus. Li *et al.* [20] proposed a spatio-temporal feature analysis approach for detecting IoV intrusions, while Das and Mohanty [21] developed a privacy-preserving IDS framework. Shukla *et al.* [22] introduced machine learning-driven distributed IDS architectures, whereas Yang and Shami [23] applied transfer learning and CNN optimization to improve detection accuracy. Yang *et al.* [24] advanced the field with LCCDE, an ensemble IDS framework, demonstrating robustness against evolving vehicular threats. Recently, Das *et al.* [27] integrated large language models (LLMs) into IDS, representing a novel AI-driven defense mechanism for IoV. Complementing these efforts, Sebastian *et al.* [28] applied federated learning (FL) for collaborative intrusion detection, balancing accuracy and privacy across distributed vehicles. Blockchain has emerged as a promising security solution.

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

Ferrag and Maglaras [25] surveyed blockchain-based authentication approaches, identifying opportunities for decentralized trust. Rehman *et al.* [30] extended this by integrating blockchain and AI for confidentiality, integrity, and availability (CIA) assurance. Earlier works such as Hasan *et al.* [31] and Aliwa *et al.* [32] addressed V2X communication and in-vehicle network protection, laying the foundation for blockchain and ML-based advancements. Machine learning and AI techniques have also been employed to secure vehicular networks. Laghari and Ahmed [26] surveyed ML-based approaches for secure vehicular communication, while Shabbir *et al.* [29] reviewed data dissemination challenges in IoV, stressing the security implications of dynamic topologies. Taken together, these works reflect an evolution from survey-driven awareness [13], [14], [17], [18] toward AI-enhanced security mechanisms [22-24], [27], [28], and blockchain-integrated frameworks [25], [30]. Despite significant progress, challenges remain in balancing real-time detection accuracy, scalability, privacy-preservation, and resilience to emerging cyber–physical threats.

3. Architecture of IoV and Associated Security Concerns

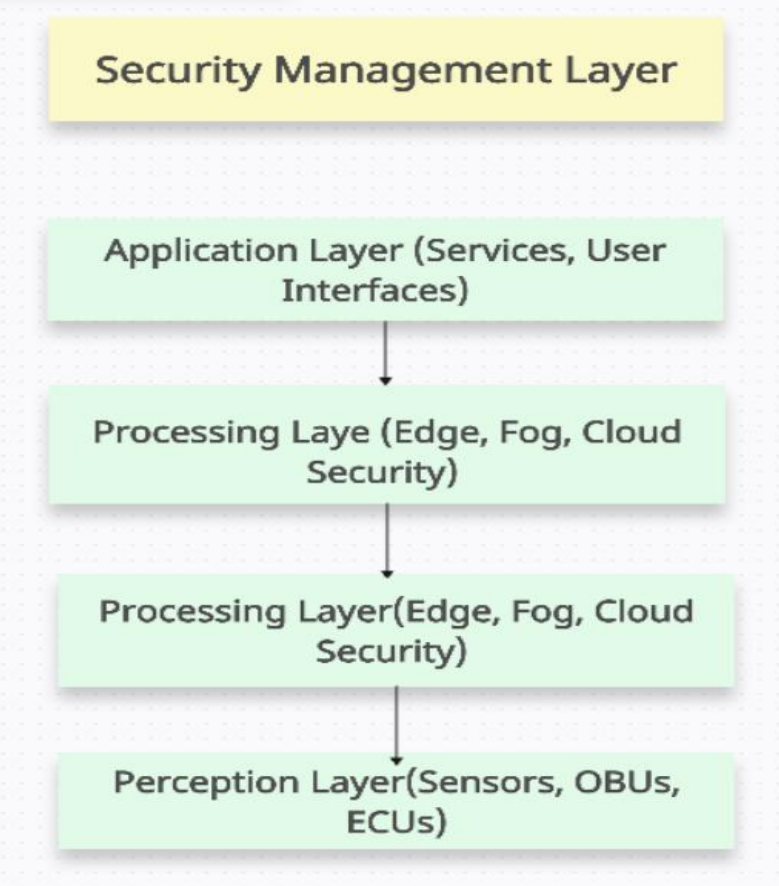

Figure. 2 Architecture of IoV

The structure of the Internet of Vehicle (IoV) is composed of several levels, it contains multiple functional parts, to realize connected, intelligent decision, and service. Each of these layers primarily has its own set of responsibilities and types of cybersecurity challenges.

3.1. Perception Layer (Vehicle Layer): This foundational layer includes all the physical and electronic components embedded within the vehicle.

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

Key Components:

A. Electronic Control Units (ECUs)

B. On-Board Units (OBUs)

C. Actuators

D. Sensors (e.g., LiDAR, radar, cameras)

Security Objectives:

A. Protection against physical tampering

B. Secure firmware updates to prevent unauthorized alterations

C. Detection and mitigation of sensor spoofing (e.g., fake obstacles or misleading traffic data)

D. Monitoring for unauthorized access or component compromise

3.2. Network Layer (Communication Layer): This layer manages data transmission between vehicles and external bodies, including infrastructure, pedestrians, and cloud systems.

Communication Technologies:

A. Dedicated Short-Range Communication (DSRC)

B. 5G / LTE / Wi-Fi

C. Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Everything (V2X)

Security Objectives:

A. Implementation of encryption and authentication protocols

B. Intrusion Detection Systems (IDS) to monitor traffic anomalies

C. Defence against Denial-of-Service (DoS) and Man-in-the-Middle (MitM) attacks

D. Use of secure routing and communication protocols

3.3. Processing Layer: This layer processes the large volumes of data collected by the vehicle and communication networks.

Key Components:

A. Edge computing devices (onboard processing units)

B. Fog nodes (e.g., Road Side Units)

C. Cloud-based platforms

Security Objectives:

A. Secure storage and processing of sensitive data

B. Use of artificial intelligence for threat detection

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

C. Implementation of access control policies

D. Privacy-preserving analytics to ensure user anonymity

3.4. Application Layer (User Interface and Services): This layer provides end-users with functionalities such as navigation, diagnostics, entertainment, and emergency notifications.

Services Provided:

A. Navigation and real-time traffic updates

B. Infotainment systems

C. Remote diagnostics and maintenance alerts

D. Emergency services

Security Objectives:

A. Strong user authentication mechanisms

B. Secure development practices to prevent app-based vulnerabilities

C. Privacy protection for user data

D. Prevention of malicious software injection

5. Security Management Layer: Functioning across all layers, this layer is responsible for enforcing cybersecurity policies, real-time monitoring, and coordinated threat response.

Core Functions:

A. Management of system-wide security policies

B. Real-time threat monitoring and automated responses

C. Use of trust frameworks such as blockchain

D. Secure Over-the-Air (OTA) updates for all components

4. Challenges of AI Integration in IoV Security

Artificial intelligence plays a pivotal role in enabling smart functionalities in IoV. However, its integration introduces a unique set of challenges:

4.1. Vulnerability to Adversarial Attacks: AI systems, especially those used for threat detection, can be manipulated through carefully crafted inputs. For example, an attacker may inject misleading data that appears benign to the AI model but carries malicious intent. These adversarial attacks can bypass detection and compromise vehicle safety.

4.2. Lack of Explainability (Black Box Problem): Many AI systems operate as "black boxes," making their decision-making processes opaque. This raises concerns about:

A. Validating the accuracy of real-time decisions

B. Diagnosing and correcting errors in critical systems

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

C. Ensuring transparency in life-or-death scenarios

This lack of interpretability can hinder accountability and system reliability.

4.3. Increased Risk from AI-Driven Automation: As AI takes on more control over vehicle functions such as braking, steering, and navigation, the potential impact of malfunctions or attacks becomes more severe:

A. Minor AI errors could lead to fatal crashes

B. Hackers gaining control over AI modules could hijack or disable vehicles remotely

This growing dependence on AI underscores the need for rigorous testing, secure design practices, and real-time threat response systems.

Attacks:

Table 1. Attacks on IoV

Attacks	Description	Solution
Vehicle to Everything Attack	Allows vehicles to connect with other vehicles, road infrastructure, pedestrians, and network services. Cyber security can exploit vulnerabilities in these communication channels to obtain unauthorized access, operate data, or interfere with vehicle operations. For example, hackers might make false traffic information to lie to drivers or shuffle the movement of traffic.	Use digital certificates and authentication. Each vehicle signs its messages using a secure key, so other vehicles can verify it's real. Use privacy-preserving techniques like counter identifiers and data minimization so that even if data is captured, it's useless.
Integrity	To ensure that the data sent over the network is accurate, free from errors, and hasn't been changed by an attacker.	We can use hashing algorithms**.** Hashing provides a unique digital fingerprint of the data, so if even a tiny part of it is altered, the hash value will be completely different—making it easy to detect tampering.
Authenticity	Make sure that the person who sent the message is the person he claims to be, not someone impersonating him.	A predefined password between the two parties that would be used to communicate.
Malware and ransomware	Malicious software such as viruses or ransomware can infect a vehicle's onboard systems. Hackers may use malware to take control of essential functions like braking, navigation or engine operation. Ransomware	Secure Software Updates. Application Whitelisting. Real-Time Malware Detection (using IDS). Isolated & Encrypted Storage. Behavior-Based Detection.

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

	attacks, where attackers latch critical systems and demand payment to restore access are particularly dangerous as they can leave vehicles untreatable until the ransom is paid.	
Denial of service attack	A DoS attack overwhelms a vehicle's communication network with excessive data requests, causing the system to slow down or completely crash. This type of attack can disrupt real-time traffic information, navigation, and safety alerts, making driving less safe and more chaotic	Use Intrusion Detection Systems (IDS) and traffic filtering techniques to detect and block abnormal behavior early.
Confidentiality	This is similar to privacy, where we need to make sure that sensitive information is protected and only authorized people can access it.	A common way to do this is through encryption**,** which turns the data into a secret code that can only be read by someone with the correct key.
Man in the Middle Attacks	In an MITM attack, a hacker privately intercepts a connection between two IoV components, such as a car and road traffic. The attacker can alter or operate messages, leading to incorrect navigation guides, false traffic alerts, or even unofficial control over vehicle functions. This type of attack is particularly wild as it can go undetected while affecting vehicle behavior in real-time.	Use end-to-end encryption and mutual authentication**.** TLS (Transport Layer Security) for secure communication. Public Key Infrastructure (PKI) to manage and verify digital certificates. Blockchain to create a trusted and tamper-proof log of all interactions.

Threads:

Table 2. Threads in IoV

Thread Type	Blockchain	ML-based IDS	PKI	Homomorphic Encryption
DoS	No	Yes	No	No

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

Spoofing	Yes	Yes	Yes	No
Data Tampering	Yes	No	Yes	Yes
Eavesdropping	No	No	Yes	Yes

5. Challenges in IoV Security

Cyber Security is playing a more important role as vehicles are increasingly linked and intelligent. The permeation of the Internet of Vehicles (IoV) — vehicles interacting with infrastructure and the Internet — into our lives offers great convenience, but also exposes the system to many security threats. The following points are the most important challenges of IoV systems security at the present:

5.1. Expanded Attack Surface: The attack surface of IoV systems has been expanded greatly by the incorporation of sensors, control units and wireless connections. Some of these vehicles are now vulnerable to a range of advanced cyber attacks, including:

A. False identities: Bogus devices or assumed identities that falsify data to deceiving vehicles into improper behavior.
B. MITM (Man in the Middle) Attacks: Wiretapping and changing the communication exchange between vehicles, infrastructure, or pedestrians.
C. DoS (Denial of Service): Attackers flood the systems and cause vital functions within the vehicle disabled.
D. Eavesdropping: Unauthorized agents listening to the communication between vehicles and infrastructures.

And the dangers are not just cyber in nature; Malfunctions in important vehicle safety systems (like the brake, steering, or traffic light control) can put human lives at stake.

5.2. Lack of standardisation and fragmentation: IoV consists of various manufacturers, service suppliers and governmental authorities, unlike traditional networking systems. Every entity may have distinct security models, resulting in the lack of compatibility, and exposing the system to security threats. The lack of a single, unified security standard is the source of increased complexity in providing security for the overall IoV ecosystem and hinders deployment of complete security solutions over all parts of the system.

5.3. Complexity of In-Vehicle Network: Modern vehicles are equipped with a large number of devices such as the Electronic Control Units (ECUs), sensors, cameras, communication modules, etc. Many of these systems communicate using older protocols (such as Controller Area Network or CAN bus) that were not originally created with security in mind. There are many technical challenges to the protection of these complex internal corporate networks:

A. Low computing power of many vehicle systems, forbidding the use of strong encryption algorithms.
B. Depends on trustful component to component communication.

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

C. Logistics for updating security procedures among millions of vehicles in the fleet presents manufacturers with a daunting challenge.

5.4. Real-Time Constraints and Performance Overheads: In IoV, the data should be processed without any delay that could be critical in autonomous vehicles. But as security mechanisms, including encryption and deep packet inspection, will inevitably introduce overhead into data processing. This raises a question: Is security more important than speed? A delay in vehicle response time may result in accidents, for example, and poor protection may leave the system vulnerable to attacks.

5.5. Vulnerability of Sensitive Data and Privacy: Vehicles collect continuously sensitive data such as real-time location, driving behavior, biometric datum (e.g. facial recognition, fingerprint for unlocking). If these streams of data are not properly secured:

A. The hackers could monitor people's movements in real time.
B. Your personal data can be exposed, sold or leaked.
C. It could expose passenger privacy, endangering both drivers and riders.

5.6. Excessive Dependence on Simulation for Testing: Most of IoV cybersecurity solutions are just tested on simulation or a closed testbed environment, which are incapable to consider all the real circumstances, such as the chaos in the road or driver's operation, or the network fault. Said even the most cutting edge security measures can be inadequate without being extensively tested in the real world in the face of real-world adversarial attacks."

5.7. Challenges of AI-based Security System in IoV: AI and ML are increasingly adopted for real-time threat detection for IoV systems, however, they have their own challenges:

A. Vulnerability to Adversarial Attacks: Hackers can feed AI systems false data (adversarial examples) to trick them into making the wrong decisions.
B. Opacity (Black Box Problem): Many AI systems are 'black boxes', meaning it is difficult to comprehend their decision-making process. Such opaqueness is concerning in high stakes scenarios like autonomous driving.
C. Critical Role of AI: As more of the car becomes controlled by AI (e.g., steering, braking, navigation), errors in the AI model will have potentially deadly implications. Such a defect could obviously be life-threatening, so it is urgent that these vulnerabilities are taken care of.

5.8. Insider Threats and Human Error: Some threats are closer than you think. There is also significant risk from insider threats, malicious or not. These threats might arise from:

A. Careless employees or contractors who release access credentials.
B. People connecting unsecured devices to in-vehicle systems.
C. Untrusted software and hardware being added by vendors during maintenance.

These human-related errors are hard to foresee and even harder to overcome, and are a major security challenge in IoV.

6. Conclusion

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

The Internet of Vehicles (IoV) represents a new paradigm for Intelligence Transportation Systems (ITS), yet it also involves an array of security concerns that call for urgent attention. This systematic review covered earlier studies, ranging from initial research into vulnerabilities in GPS, sensors, and vehicle communications to recent work on integrating blockchain and AI-based systems. The study unequivocally indicates that threats from spoofing, Sybil attacks, Denial-of-Service (DoS), data privacy violation, and routing manipulation are still significant issues for secure vehicular networking. VANETs and wireless technology enable the Internet of Vehicles (IoV) while also increasing the attack surface, noting the double-edged role of connectivity in assuring and undermining future mobility. The studies also indicate a vast variety of countermeasures, including cryptographic authentication, privacy-preserving methods, secure routing protocols, and anomaly finding models. Innovative concepts, such as decentralised blockchain-based trust models and machine learning-based intrusion detection systems, hold promise for countering new forms of attacks. Nonetheless, it is still challenging to ensure the system can scale, execute quickly enough for real-time deployment, and safeguard all communication and perception levels. In summary, there has been considerable progress made in discovering threats and coming with solutions to secure IoV further, but the field continues to evolve. A secure IoV ecosystem will ultimately rely on interdisciplinary solutions integrating encryption, distributed ledger technology, artificial intelligence, and cyber-physical system security. Future studies must then target flexible, interoperable, and resource-conserving frameworks capable of dealing with evolving threats in environments where vehicles are highly mobile. IoV can only become a reality with secure, resilient, and reliable transport networks by implementing such combined techniques.

References:

[1] Petit, J., & Shladover, S. E. (2014). Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(2), 546–556. https://doi.org/10.1109/TITS.2014.2342137

[2] Lu, N., Cheng, N., Zhang, N., Shen, X. S., & Mark, J. W. (2014). Connected vehicles: Solutions and challenges. IEEE Internet of Things Journal, 1(4), 289–299. https://doi.org/10.1109/JIOT.2014.2327587

[3] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

[4] Ghosh, S. K., et al. (2019). Security of connected and autonomous vehicles: Challenges and opportunities. Internet of Things, 5, 1–20. hass

[5] Petit, J., & Simões, E. B. (2019). Security and privacy in vehicular communications. In Handbook of Smart Vehicles (pp. xx-xx). Springer.

[6] Faisal, A., Abbas, H., & Khan, S. U. (2020). A survey of data privacy and security issues in the Internet of Vehicles. IEEE Communications Surveys & Tutorials, 22(2), 1026–1059. https://doi.org/10.1109/COMST.2019.2953364

[7] Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2020). Internet of Vehicles security: Challenges and solutions. Journal of Network and Computer Applications, 133, 1–16. https://doi.org/10.1016/j.jnca.2019.05.016

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

[8] Hussain, R., & Zeadally, S. (2020). Autonomous cars: Research results, issues, and future challenges. IEEE Communications Surveys & Tutorials, 22(2), 1275–1313. https://doi.org/10.1109/COMST.2020.2970297

[9] Wang, T., et al. (2021). Machine learning for cybersecurity in IoV: Challenges and future directions. IEEE Network, 35(2), 248–254. https://doi.org/10.1109/MNET.011.2000416

[10] Zhao, L., Li, J., & Li, H. (2022). Security and privacy in the Internet of Vehicles: Architecture, challenges and solutions. Computer Networks, 210, 108973. https://doi.org/10.1016/j.comnet.2022.108973

[11] Mohamed, A., Alrawais, A., & Shi, W. (2023). A comprehensive survey on blockchain for the Internet of Vehicles. IEEE Internet of Things Journal, 10(3), 2345–2364. https://doi.org/10.1109/JIOT.2022.3167891

[12] Saharkhiz, A. H., & Farhadi, M. (2024). Review on cybersecurity frameworks in IoV with AI integration. Future Internet, 16(1), Article 7. https://doi.org/10.3390/fi16010007

[13] A. Khezri, H. Gomez-Mourelo, M. Khan, and R. Ibrahim, "Security Challenges in Internet of Vehicles (IoV) for ITS: A Survey," Tsinghua Science and Technology, vol. 29, no. 4, pp. 637–658, 2024, doi: 10.26599/TST.2024.9010083.

[14] S. Singh and A. Sharma, "IoV security and privacy survey: issues, countermeasures, and challenges," The Journal of Supercomputing, vol. 80, no. 18, pp. 19980–20025, 2024, doi: 10.1007/s11227-024-06269-5.

[15] S. Rony, M. R. Ahmed, and R. H. Khan, "Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions," Sensors, vol. 24, no. 2, p. 368, 2024, doi: 10.3390/s24020368.

[16] M. R. Ahmed et al., "Security for the Internet of Vehicles with Integration of Sensing and Computing," Sensors, vol. 25, no. 16, p. 5119, 2025, doi: 10.3390/s25165119.

[17] A. Rahman, S. S. Islam, and S. Khan, "Security issues in Internet of Vehicles (IoV): A comprehensive survey," Array, vol. 20, p. 100325, 2023, doi: 10.1016/j.array.2023.100325.

[18] K. Salah, I. Yaqoob, and R. Jayaraman, "A comprehensive review on blockchains for Internet of Vehicles," Computer Networks, vol. 226, p. 109574, 2023, doi: 10.1016/j.comnet.2023.109574.

[19] A. Alzubaidi and A. Elnashar, "A Systematic Literature Review on Internet of Vehicles Security," arXiv preprint arXiv:2212.08754, 2022.

[20] A. Alzubaidi and A. Elnashar, "A Systematic Literature Review on Internet of Vehicles Security," arXiv preprint arXiv:2212.08754, 2022.

[21] Z. Li, J. Wang, and Y. Chen, "Intrusion Detection Method for Internet of Vehicles Based on Parallel Analysis of Spatio-Temporal Features," Sensors, vol. 23, no. 9, p. 4399, 2023, doi: 10.3390/s23094399.

Received: 2025-09-01
Accepted: 2025-09-15
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10104

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

[22] P. K. Das and S. P. Mohanty, "Privacy-Preserving Intrusion Detection System for Internet of Vehicles," in Proc. ICCCN, 2024, pp. 1–6, doi: 10.1145/3632366.3632388.

[23] A. Shukla, N. Gupta, and R. Kumar, "Machine Learning-Driven Distributed Intrusion Detection System for the Internet of Vehicles," in Proc. CEUR Workshop, vol. 3935, pp. 25–32, 2024.

[24] L. Yang and A. Shami, "A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles," arXiv preprint arXiv:2201.11812, 2022.

[25] L. Yang, A. Shami, G. Stevens, and S. De Rusett, "LCCDE: A Decision-Based Ensemble Framework for Intrusion Detection in the Internet of Vehicles," arXiv preprint arXiv:2208.03399, 2022.

[26] M. A. Ferrag and L. Maglaras, "Blockchain-Based Authentication in Internet of Vehicles: A Survey," Sensors, vol. 21, no. 24, p. 8164, 2021, doi: 10.3390/s21248164.

[27] H. A. Laghari and S. H. Ahmed, "Machine Learning Technologies for Secure Vehicular Communications: A Survey," Wireless Communications and Mobile Computing, vol. 2021, Article ID 8868355, 2021, doi: 10.1155/2021/8868355.

[28] N. Das, S. Roy, and A. K. Das, "An Integrated IDS for the Internet of Vehicles using a Large Language Model," Array, vol. 26, p. 100452, 2025, doi: 10.1016/j.array.2025.100452.

[29] A. Sebastian et al., "Enhancing Intrusion Detection in Internet of Vehicles through Federated Learning," arXiv preprint arXiv:2311.13800, 2023.

[30] N. Shabbir, M. S. Khan, and A. A. Khan, "A Survey on Data Dissemination in Internet of Vehicles Networks," Journal of Information and Telecommunication, vol. 7, no. 2, pp. 257–287, 2023, doi: 10.1080/24751839.2022.2151658.

[31] S. A. Rehman, H. Abbas, and R. Buyya, "CIA Security for Internet of Vehicles and Blockchain-AI Integration," Journal of Grid Computing, vol. 22, no. 2, p. 36, 2024, doi: 10.1007/s10723-024-09757-3.

[32] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," arXiv preprint arXiv:2003.07191, 2020.

[33] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and Countermeasures for In-Vehicle Networks," arXiv preprint arXiv:2004.10781, 2020.

[34] Seth, Ashish. "Attack and Anomaly Detection in IoT Sensors Using Machine Learning Approaches." Journal of Recent Innovations in Computer Science and Technology 2.1 (2025): 16-27. https://doi.org/10.70454/JRICST.2025.20108