International Conference on Science, Engineering & Management Trends

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

# A Review on Security in the 6G-Enabled Internet of Vehicles

**Bhagyashri M**

Research Scholar, Srinivas Institute of Engineering and Technology, Srinivas University, Mukka, Mangalore, Karnataka, India and Lecturer Selection Grade -1, Department of Computer Science and Engineering, 121-Government Polytechnic for Women, Hubli

**Abstract- Advertising has evolved from a mere transactional tool to a powerful emotional conduit that shapes consumer perceptions and behaviors. In the fast-moving consumer goods (FMCG) sector, emotional advertising has become a cornerstone strategy for building brand loyalty and enhancing brand recall. This study examines the effectiveness of emotional advertising in fostering brand recall, with a focused analysis on Cadbury Dairy Milk, one of India's most iconic chocolate brands. The research investigates how emotional cues embedded in advertisements — including nostalgia, joy, love, and familial warmth — influence the depth and durability of brand memory among consumers. A descriptive and analytical research design was adopted, employing a structured questionnaire administered to 150 respondents across urban demographics. The findings reveal that emotionally charged advertisements not only outperform rational or information-based advertisements in recall but also strengthen brand identity and consumer affinity over time. Cadbury's long-running campaigns such as 'Kuch Meetha Ho Jaaye' and 'Real Taste of Life' were found to have exceptionally high spontaneous recall rates, suggesting that consistent emotional messaging creates enduring mental imprints. The study further explores the mediating role of emotional intensity, repetition frequency, and storytelling quality in shaping recall outcomes. Managerial implications are discussed for advertising professionals and brand strategists aiming to leverage emotional intelligence in campaign design. The study contributes to the growing body of literature on affective advertising and consumer neuroscience, offering actionable insights for achieving sustainable competitive advantage through emotional brand equity.**

**Keywords- Emotional Advertising, Brand Recall, Cadbury Dairy Milk, Consumer Behaviour, Affective Advertising, FMCG Marketing**

## I. INTRODUCTION

The two technologies named in the title are arriving together. Sixth-generation cellular systems are entering early standardization through 3GPP Release 20, with first commercial deployments targeted for 2030 [3], [15], and a parallel push has moved the Internet of Vehicles from an experimental V2X concept into a near-term operational target [4], [13]. The intersection is not a polite layering of two roadmaps; it is a stress test of both. A 6G-enabled IoV is expected to deliver terabit-per-second peak rates, sub-millisecond reaction loops, near-continuous satellite-air-ground coverage, and an AI-native control plane that re-tunes itself without human supervision [2], [4], [17]. Each of those properties is also an attack surface. A terahertz beam can be jammed by a malicious roadside object. A federated



DOI: http://doi.org/10.5281/zenodo.20557249

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

training round can be poisoned by a single compromised on-board unit. A handover across SDN domains can be hijacked when the authentication tokens between controllers are weak [6]. A quantum-capable adversary, even a hypothetical one, undermines the cryptographic floor on which the rest of the stack rests [17], [18].

Vehicular networks raise the cost of getting any of this wrong. Other 6G verticals can absorb a slow recovery from a security event; a vehicle that misses a brake signal because its in-vehicle CAN bus accepted a falsified frame cannot [5]. The safety-criticality of IoV is the single feature that distinguishes 6G-IoV security from 6G security in general. A spoofed Basic Safety Message, an injected ECU command, a man-in-the-middle on a V2I link, or a poisoned global model update are not abstract risks in this setting; they map directly to collisions, fatalities, and traffic-system failure modes. The aspirational figures for IoV are large. One analysis projects 58 million autonomous-vehicle units sold globally in 2030, against 1.4 million in 2019 [14], and the corresponding security envelope has not caught up.

The recent literature has responded along two complementary directions. Empirical work has built defence frameworks on top of the new 6G primitives. Federated learning is used to keep raw vehicular data on the device while a global intrusion detector is trained collaboratively [7], [11], [15]. Blockchain is layered on roadside units to log detection results, anchor authentication artefacts, and isolate misbehaving ECUs through smart contracts [1], [5], [6]. Edge intelligence is positioned between the vehicle and the cloud so that low-latency inference is possible without exporting sensitive telemetry [7], [12], [13]. Zero-trust architectures have been proposed at both local and global granularity, with generative AI and transfer learning supplying the detection logic [10], [12]. At the cryptographic layer, succinct non-interactive proofs (zk-SNARKs) have started to replace heavier ECC-based authentication, with reported reductions of more than half in computation time and energy [6]. Survey work has produced taxonomies of the underlying threat space, comparing the relative severity of 5G-ITS and 6G-ITS attack vectors and inventorying the role of AI, RL, blockchain, and quantum-aware mechanisms across the layers of the IoV stack [4], [13], [14], [17], [18], [19].

The picture that emerges from reading these papers together is less consistent than any individual paper suggests. Most defence frameworks report detection accuracies above 99 percent on a single dataset, but evaluation under a different distribution, including a new vehicle population, a new attack family, or a different city, is rare. The threat models are often stated in a single sentence and rarely explain what the adversary cannot do. Post-quantum readiness is discussed in survey papers but is largely absent from the empirical defence designs. Safety-coupled metrics such as the latency from sensor anomaly to actuator override, the false-miss rate on safety-critical attacks under load, or identity-preservation through handover are almost never reported, even though they are the only metrics that map to the underlying purpose of the system.

**Motivation and Contribution**

A reader trying to plan a 6G-IoV defence today must move between three sub-literatures: an AI/FL-driven detection literature, a cryptographic and authentication literature, and a survey literature that does not always reach the level of design detail needed to compare options. The motivation for this review is to compress that movement. The papers reviewed here range from a 2021 transfer-learning framework that prefigured several of the building blocks of the current generation [1] to 2026 zero-touch architectures aligned with ETSI ZSM, 3GPP MANO, and O-RAN specifications [12]. Reading them as a single body shows where the field has tightened and where it has stalled.



DOI: http://doi.org/10.5281/zenodo.20557249

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

**The contributions of this review are five.**

- The reviewed methods are organized into two complementary groups along the defence-construction axis: concrete defence frameworks that propose a specific protocol, model, or architecture for 6G-IoV (intrusion detection, lightweight authentication, blockchain-anchored logging, decentralized FL, zero-trust), and surveys and cross-cutting analyses that map the threat landscape, taxonomize the attack space, and inventory enabling primitives. Two comparative tables in Section 2 make the grouping explicit.
- Defence frameworks are compared not only on headline accuracy but also on the data they were evaluated against, the threat model they assume, the role of blockchain or cryptography in the design, and the failure modes they leave unaddressed.
- Survey contributions are summarized by the scope of their coverage and by the open issues each identifies, so that a research group starting on a new 6G-IoV defence does not have to re-read seven survey articles to locate the gap most relevant to its goals.
- The research gap is discussed under four headings: opaque or shallow threat modelling, weak cross-dataset and cross-attack generalization, immature post-quantum readiness in the empirical defence designs, and the absence of safety-coupled evaluation metrics that align with the consequences of a security failure in a vehicular context.
- Future directions are framed as incremental and testable rather than as a single integrated solution: a shared 6G-IoV evaluation suite, lightweight post-quantum primitives layered on the existing FL+blockchain stacks, latency-bounded zero-trust verification across satellite-air-ground handovers, and modest red-team studies that test detection frameworks against attack families not seen during training.

## II. RELATED WORK

The recent literature on 6G-enabled IoV security can be split, broadly, between papers that propose a concrete defence component and papers that step back to map the field. Both kinds matter for system design, but they offer different evidence. The first kind tells a researcher how a particular detection or authentication mechanism behaves under a specified setup; the second tells the researcher where that mechanism sits in the larger threat space. The review follows that split.

It is useful to begin with the earliest of the reviewed defence papers, since several of its design choices have been recycled in newer work without always being acknowledged. Xu et al. [1] proposed a reputation-based transfer-learning framework for 6G-IoV in which pre-trained models exchanged between vehicles are weighted by a reputation score, with the score itself managed on a consortium blockchain so that no single vehicle can rewrite the trust ledger. A deep-learning-based auction scheme rewards high-reputation contributors. The paper predates the bulk of the 6G-IoV security literature, but two of its choices, the use of blockchain as a decentralized trust register and the tying of model selection to a reputation function, recur repeatedly in 2024 to 2026 work [5], [7], [9].

Authentication has become a more crowded sub-area than was the case in 2021. Varma and Kumar [6] respond to one of the harder design questions in distributed SDN-based vehicular networks: how to authenticate a vehicle that moves between SDN controllers without re-running the full protocol at every handover. Their scheme places authenticated information on a blockchain so that neighbouring SDN controllers no longer have to exchange topology updates over a side channel that itself becomes a single point of failure. The authentication step is performed with zk-SNARK proofs of constant size, which allows a vehicle to demonstrate possession of valid credentials without sending the credentials themselves. The reported improvement is greater than 55 percent on authentication latency, computation time, and energy efficiency relative to state-of-the-art baselines. The use of zk-SNARK is the more substantive contribution. Constant-size proofs make handover possible inside the latency


DOI: http://doi.org/10.5281/zenodo.20557249

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

budget that 6G-IoV will impose; the alternative, which is to re-run full ECC-based handshakes at every controller boundary, does not scale.

Intrusion detection inside the vehicle is a different problem and has its own active sub-literature. Nakayiza et al. [5] argue that the conventional placement of an in-vehicle IDS on the CAN bus is structurally limited, because the CAN bus lacks both authentication and encryption and cannot easily communicate with external security mechanisms such as blockchain. They move the IDS to the Telematics Control Unit, where it can interface with external networks while still observing in-vehicle traffic, and combine a Pearson Correlation Coefficient feature-selection front-end with a hybrid ML classifier. A custom Proof of Authority and Association blockchain on the roadside unit stores ECU information, detection results, and triggers automatic isolation of malicious ECUs through smart contracts. The reported detection accuracy reaches 99.9 percent on the CICIoV2024 and CAN-Intrusion datasets, with sub-second computation time and a blockchain throughput stable at sixteen transactions per second under increasing ECU density. The IDS placement question is more important than it sounds: it determines whether the in-vehicle defence can ever cooperate with the higher-layer mechanisms the 6G IoV stack relies on.

A different strand of empirical work has focused on the learning protocol rather than on the IDS placement. Zhu et al. [7] propose a Distributed Edge Intelligence framework for 6G-IoV that combines a hierarchical blockchain architecture, an asynchronous federated learning algorithm with genetic-algorithm-driven resource allocation, and a lightweight Hierarchical Edge Intelligence Consensus protocol. The asynchronous design responds to a constraint that synchronous FL ignores: in a vehicular network, the participant set is never stable, vehicles drop in and out of coverage, and a synchronous round wastes time waiting for stragglers. Tests on MNIST and SVHN show improvements over baselines in accuracy, communication efficiency, and privacy preservation. Sharma and Rani [8] take a complementary approach inside the broader 6G-IoT setting. Their stacked-hybrid IDS combines random forest, SVM, and logistic regression as base classifiers with XGBoost as a meta-learner, evaluated on the RT-IoT dataset; the reported accuracy is 99.90 percent and the precision, sensitivity, specificity, and F1 are in a similar band. The paper is not IoV-specific, but the architectural pattern of an ensemble base layer with an XGBoost meta-learner has begun to migrate into vehicular IDS work.

Hierarchical detection across the IoV stack is the contribution of Sedjelmaci et al. [9], [16]. The framework relies on edge nodes to satisfy 6G key performance indicators on trustworthiness, latency, connectivity, data rate, and energy consumption. Federated learning is combined with a non-cooperative Stackelberg security game that identifies malicious IoV devices and edge servers and selects trustworthy participants for training. A Security Information and Event Management component aggregates detection signals across security entities, IoV devices, and edge servers. The reputation-based selection step is the most interesting design choice: it concedes that a federated training round will inevitably include some compromised participants and treats the problem as a participant-selection problem rather than as a perfect-defence problem. Sedjelmaci and Ayaida [10] move further in the zero-trust direction. Their framework deploys Local Zero Trust Systems at the VANET level and a Global Zero Trust System on each 6G edge server, with detection logic powered by generative AI and transfer learning. The collaborative aspect, in which local detectors share knowledge with the global detector while the global detector pushes back distilled threat models, is presented as the first zero-trust framework for 6G-enabled VANETs to use generative AI in this role.

Decentralized federated learning is the focus of Zhang et al. [11], who deploy FL on autonomous vehicles without a central server. The framework targets the non-IID and class-imbalance problems that vehicular intrusion-detection data typically present and shows performance improvements over both FedAvg baselines and locally trained models. The paper is one of the few that explicitly addresses the practical inconvenience of vehicular FL, where the server may not be reachable and may not be



DOI: http://doi.org/10.5281/zenodo.20557249

trustworthy. Mahin et al. [12] take the orchestration question to the standardization level with their Secured and Standardized Zero-Touch 6G framework. The framework integrates zero-trust principles, blockchain-based security auditing, and AI-driven orchestration with ETSI ZSM, 3GPP MANO, and O-RAN-aligned APIs. The reported gains are a 44.9 percent latency reduction, 9.8 percent automation efficiency improvement, and 97.5 percent security detection accuracy against reference architectures. The standards-alignment story is the contribution; performance is the proof of viability.

Table 1 brings these defence frameworks together, with the methodology, advantages, and shortcomings of each.

| Reference | Methodology | Advantages | Shortcomings |
|---|---|---|---|
| [1] Xu et al., 2021 | Reputation-based transfer learning with consortium blockchain; deep-learning auction to incentivize high-reputation model contributors. | Decentralized trust management; secure participant selection for TL; early integration of incentive design. | Simulation only; no real attack dataset; no post-quantum adaptation. |
| [5] Nakayiza et al., 2025 | PCC feature selection with hybrid ML on the TCU; PoA2 blockchain on the RSU; ECU isolation via smart contracts. | 99.9% accuracy on CICIoV2024 and CAN-Intrusion; stable 16 tx/s throughput; 0.062 s blockchain latency. | Single CAN-bus attack family; no V2I or external V2X testing; no cross-population evaluation. |
| [6] Varma and Kumar, 2026 | zk-SNARK-based authentication on blockchain-enabled distributed SDVN; succinct constant-size proofs across SDN controllers. | More than 55% gain in authentication latency, computation time, and energy efficiency; SPoF mitigation. | Classical SNARK (not post-quantum); trusted-setup dependency; tested only in simulation. |
| [7] Zhu et al., 2026 | Hierarchical blockchain with asynchronous FL and GA-based resource allocation; HEIC lightweight consensus. | Tolerant of intermittent connectivity; outperforms FL baselines on MNIST and SVHN; lightweight consensus. | Evaluation datasets are non-vehicular; HEIC formal security analysis is informal; mobility model is simplified. |
| [8] Sharma and Rani, 2026 | Stacked-hybrid IDS: RF + SVM + LR base learners with XGBoost meta-learner; feature selection front-end. | 99.90% accuracy on RT-IoT with high precision and F1; lower computational cost than monolithic deep models. | 6G-IoT framing rather than IoV-specific; single dataset; no temporal or distribution-shift evaluation. |
| [9], [16] Sedjelmaci et al., 2024 | Hierarchical FL with non-cooperative Stackelberg game; SIEM aggregation; reputation-based participant selection | Balances detection accuracy against overhead; mitigates internal and external | Stackelberg equilibrium assumes a rational adversary; no quantum-adversary case; limited |



DOI: http://doi.org/10.5281/zenodo.20557249

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

| Reference | Methodology | Advantages | Shortcomings |
|---|---|---|---|
| | across edge and IoV devices. | adversaries; 6G-KPI aware. | heterogeneity in evaluation. |
| [10] Sedjelmaci and Ayaida, 2025 | Local Zero Trust Systems at VANET level and Global Zero Trust System on 6G edge servers; generative AI + transfer learning for detection. | First zero-trust framework for 6G-VANETs to use generative AI; collaborative local-global detection. | Closed-loop evaluation; no adversarial-side generative attack experiments; no post-quantum adaptation. |
| [11] Zhang et al., 2025 | Decentralized FL across autonomous vehicles without a central server; handles non-IID and class-imbalance. | Resilient to central-server failure; outperforms FedAvg and locally trained models. | Theoretical analysis simulation-based; limited attack diversity; weak cryptographic anchor for parameter exchange. |
| [12] Mahin et al., 2026 | SS-ZT6G framework: zero-trust + blockchain auditing + AI-driven orchestration; ETSI ZSM, 3GPP MANO, O-RAN aligned APIs. | 44.9% latency reduction; 9.8% automation gain; 97.5% detection accuracy; full standards alignment. | Generic Edge-AI framing; vehicular-specific evaluation absent; post-quantum readiness unexplored. |

A sceptical reading is worth carrying through. Detection numbers above 99 percent on a single dataset have become the default rather than the exception, and most of the frameworks claim them. The accuracy is largely real in the narrow sense that the published evaluation regime supports it, but the regimes themselves are narrow: the datasets are static (RT-IoT, CICIoV2024, CAN-Intrusion, MNIST, SVHN), the threat models are often homogeneous (DDoS, spoofing, ECU misbehaviour), and the cross-dataset behaviour is rarely measured. The papers that step furthest in the right direction, whether through ensemble base learners with diverse error structures [8], reputation-weighted participant selection [9], or asynchronous and connectivity-aware aggregation [7], still report results inside a single distribution. A defender deploying any of these frameworks today should expect the field-deployed accuracy to fall well below the reported figure.

The second body of the literature provides the framing that the defence papers usually lack. Moya Osorio et al. [4] published one of the first wide-angle accounts of 6G-IoV security and privacy, inventorying the roles of AI, network softwarization, network slicing, blockchain, edge computing, intelligent reflecting surfaces, backscatter communication, terahertz links, visible light communication, physical-layer authentication, and cell-free massive MIMO in providing security for vehicular networks. The breadth is the contribution; the paper does not endorse a single architecture but lays out the design space against which later defence frameworks can be located. Kim et al. [19] focus on the V2X subset and provide a CIA3 (confidentiality, integrity, availability, authentication, access control) analysis combined with a review of FL and blockchain primitives. They propose a Blockchain-enabled FL-based generic security architecture for V2X in 6G and identify research directions including 3D fog computing privacy, AR privacy, secure SDN, THz physical-layer security, SUMO-based traffic-simulation security testing, and AI-based intrusion detection.



DOI: http://doi.org/10.5281/zenodo.20557249

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

The role of AI in 6G security has received a separate survey treatment. Kumar et al. [18] make the strong claim that AI is a double-edged sword in 6G, capable of either protecting or compromising security depending on configuration, and survey distributed ledger technology, physical-layer security, terahertz communication, quantum computing, visible light communication, and distributed AI/ML in this dual role. de Alwis et al. [15] focus specifically on federated learning for 6G security and provide a layered analysis covering RAN, O-RAN, network edge, and network orchestration. They also surface the inverse problem of security threats inside the FL process itself, which is implicitly acknowledged by [9] and [10] but rarely discussed in the same paper that proposes an FL-based defence.

Reinforcement learning is the focus of Mianji et al. [14], who provide a survey of RL-based solutions for vehicular network security, privacy, and trust. Two taxonomies are used: one based on the SPT focus area and one based on the RL method. The survey is one of the few to treat trust management as a first-class concern rather than as a side effect of authentication. Abdullahi et al. [17] take a broader 6G-ITS perspective and explicitly compare the security threats in 5G-ITS and 6G-ITS, paying particular attention to the dual role of quantum technologies. Quantum key distribution and post-quantum cryptography appear on the defence side, while a quantum-capable adversary appears on the attack side. The CIA3-aligned taxonomy of attack models that the paper provides is more granular than what is offered in [19] or [4].

Edge computing and AI integration are surveyed at greater length by Bilal et al. [13], who review the role of edge computing, machine learning, and deep learning in IoV security. The paper is one of the few to bring real-world deployments and case studies to bear, which makes the gap it identifies, between the deployment readiness of EC+ML defences and the residual challenges in scalable and privacy-preserving operation, easier to ground than in a purely architectural review.

Table 2 summarises the survey and cross-cutting works.

Table 2. Surveys and cross-cutting analyses on 6G and 6G-IoV security.

| Reference | Scope of coverage | Distinctive contribution | Open issues identified |
|---|---|---|---|
| [4] Moya Osorio et al., 2022 | 6G-IoV security and privacy across AI, softwarization, slicing, blockchain, edge, IRS, backscatter, THz, VLC, PLS, cell-free mMIMO. | First broad 6G-IoV security map; wide technology enumeration. | Unified threat models; PLS-quantum interplay; standardized SPT evaluation. |
| [13] Bilal et al., 2026 | Edge computing, ML, and DL synergy in IoV security with real-world case studies. | Connects architectural review to deployment evidence; field-side gap analysis. | Scalable privacy-preserving defences; adaptive attack resilience. |
| [14] Mianji et al., 2025 | Reinforcement learning for vehicular network security, privacy, and trust; VANET to IoV transition. | Dual taxonomy by SPT focus and RL method; trust management as first-class. | Sample-efficient RL; trust quantification; cross-domain transfer. |
| [15] de Alwis et al., 2026 | Federated learning for 6G security across RAN, O-RAN, edge, and orchestration; FL-side threats included. | Layered FL-security analysis; explicit treatment of intra-FL threat surface. | Poisoning resistance; CAV-specific FL constraints; differential-privacy budgets in dynamic clients. |



DOI: http://doi.org/10.5281/zenodo.20557249

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

| Reference | Scope of coverage | Distinctive contribution | Open issues identified |
|---|---|---|---|
| [17] Abdullahi et al., 2025 | 6G-ITS security, privacy, and trust interplay; 5G-ITS vs 6G-ITS attack comparison; quantum dual role. | Granular CIA3 taxonomy; integrated quantum offence and defence view. | Multi-layer integration; post-quantum migration plan; trust quantification. |
| [18] Kumar et al., 2026 | AI's dual role in 6G; DLT, PLS, THz, quantum computing, VLC, and distributed AI/ML. | Critical (rather than descriptive) AI-security review across enabling primitives. | Trustworthy AI; AI-versus-AI defence; quantum readiness. |
| [19] Kim et al., 2024 | 6G V2X security under CIA3 with FL and blockchain primitives. | Generic FL + blockchain architecture for V2X; CIA3 sub-domain decomposition. | 3D fog privacy; AR privacy; SUMO-driven testing; THz physical-layer security. |

Taken across both tables, a few patterns are clear. The defence frameworks have converged on a small number of architectural choices: federated or transfer learning at the edge, blockchain or hierarchical blockchain for trust anchoring, and an attention-augmented or ensemble classifier for the detection step. The surveys agree that this is the right general direction but identify several open issues, including post-quantum readiness, threat-model standardization, RL-aware operation, and standardized SPT evaluation, that the defence frameworks have not yet operationalized. A genuine end-to-end study that couples a 6G-IoV defence framework to a standardized threat model, evaluates it across at least two non-overlapping datasets, and reports a safety-coupled latency metric in addition to detection accuracy is still missing from the reviewed set.

## III. RESEARCH GAP AND FUTURE DIRECTIONS

Reading the two tables side by side surfaces the gaps that any individual paper, on its own, tends to hide.

The first gap is threat-model opacity. Almost every defence framework reviewed here names a small set of attacks (DDoS, spoofing, ECU misbehaviour, data falsification, model poisoning) and then evaluates against a dataset that contains exactly that set. The adversary's capabilities are usually described in a sentence and rarely stated as what the adversary cannot do. Without a stated upper bound on adversarial capability, the published accuracy figures cannot be falsified, which makes them difficult to compare across papers. The 5G-ITS versus 6G-ITS comparison of [17] is a useful first step in standardizing the threat language, but the empirical defence designs have not yet adopted it.

The second gap is the weakness of cross-dataset and cross-attack evaluation. Frameworks that report 99.9 percent on CICIoV2024 [5] and 99.9 percent on RT-IoT [8] have, in principle, no relationship to each other on field data, and yet the literature treats both numbers as comparable evidence of strong defence. A small step forward would be the use of two datasets per paper, with at least one being out-of-distribution relative to the training data. A larger step would be a shared 6G-IoV evaluation suite that mixes V2I, V2V, in-vehicle (CAN), and edge-network traffic with a standardized attack catalogue. The current state of evidence does not allow a defender to predict how any of the reviewed frameworks would behave on a third dataset, let alone in production.

The third gap is post-quantum readiness. Quantum-resistant cryptography is mentioned in [10], [17], [18], and [4] as a 6G requirement, and the practical case is reinforced by [6], which uses zk-SNARK



DOI: http://doi.org/10.5281/zenodo.20557249

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

proofs that are themselves not, in their classical form, post-quantum secure. The defence frameworks based on FL and blockchain inherit the cryptographic floor of the underlying primitives (hash functions, signature schemes, and the elliptic-curve constructions inside the SNARK), and none of the reviewed empirical papers explicitly tests behaviour under a post-quantum substitution of those primitives. The closest the field comes is the architectural discussion in [17]. A modest near-term step is to repeat one of the existing FL + blockchain frameworks with a lattice-based signature scheme drawn from the NIST PQC standards [20] and report the change in latency, throughput, and detection accuracy.

The fourth gap concerns evaluation metrics. Detection accuracy, precision, recall, and F1 dominate the literature, with throughput and transaction latency added by the blockchain-heavy papers. None of these metrics maps directly to the safety consequence of a security failure in IoV. A vehicle whose IDS catches a CAN injection in 200 milliseconds but cannot translate that into an actuator override in another 200 milliseconds has, from the user's perspective, no defence. The reviewed papers rarely report end-to-end latency from sensor anomaly to in-vehicle response, false-miss rate on safety-critical classes (collision-avoidance, braking, steering), or identity-preservation through SDN-controller handover. The Stackelberg-game framework of [9] is an exception that quantifies a security-versus-overhead trade-off, but even there the trade-off is measured against detection accuracy rather than against safety outcomes.

A fifth, less obvious gap is the absence of red-team studies. The defence frameworks are evaluated against the same attack distributions they were trained on. Generative AI is now used to construct novel attack variants and [10] uses it on the defender's side, but the literature does not yet contain a study in which the same generative model is turned around to produce previously unseen attack instances against a published defence. A short red-team protocol would be cheap to build and would expose the difference between in-distribution accuracy and adversarial robustness.

The directions that follow from these gaps are incremental and testable. A shared 6G-IoV evaluation suite that combines V2I, V2V, in-vehicle, and edge traffic with a standardized threat catalogue would let cross-paper accuracy comparisons mean what they claim to mean. Layering post-quantum signature and proof systems onto the existing FL + blockchain stacks would let the post-quantum readiness question be answered empirically rather than at the level of survey commentary. Reporting safety-coupled latencies alongside detection accuracy is a change in evaluation style rather than a change in model design, and it costs nothing in research effort. Latency-bounded zero-trust verification across satellite-air-ground handovers, a topic that [12] and [4] both raise but neither tests, is a research target on which both the cryptographic and the AI sub-literatures could converge.

## IV. CONCLUSION

This review has read the recent 6G-enabled IoV security literature as a single pipeline whose stages (sensor data, edge learning, roadside trust anchoring, network-level authentication, and standards-aligned orchestration) are usually treated separately. The pipeline view makes the recurring gaps visible. Empirical defence frameworks now reach high reported accuracy on a single dataset but rarely cross-validate, rarely test under a quantum-capable adversary, and rarely state what their threat model excludes. Cryptographic protocols have moved towards succinct, handover-friendly authentication, but the post-quantum substitution has not yet been performed inside the running 6G-IoV stack. Surveys map the design space well but do not, on their own, close the evaluation gap that the defence papers leave. The integration problem, not any single algorithm, is the open one. A 6G-IoV defence that is evaluated on at least two datasets, under a stated threat model that includes a post-quantum adversary, with a safety-coupled latency metric reported alongside accuracy, is a feasible near-term


DOI: http://doi.org/10.5281/zenodo.20557249

target. It is also the most likely route by which the present collection of frameworks turns into a deployable layer of the 6G-IoV stack rather than a literature of high-accuracy but loosely connected results.

## REFERENCES

1. M. Xu, D. T. Hoang, J. Kang, D. Niyato, Q. Yan, and D. I. Kim, "Secure and reliable transfer learning framework for 6G-enabled Internet of Vehicles," arXiv preprint arXiv:2111.05804, Nov. 2021.
2. ITU-R, "Framework and overall objectives of the future development of IMT for 2030 and beyond (IMT-2030)," Recommendation ITU-R M.2160, Nov. 2023.
3. 3GPP, "Release 20 description," 3GPP TR 21.920, 2025.
4. D. P. Moya Osorio, I. Ahmad, J. D. Vega Sanchez, A. Gurtov, J. Scholliers, M. Kutila, and P. Porambage, "Towards 6G-enabled Internet of Vehicles: Security and privacy," IEEE Open Journal of the Communications Society, vol. 3, pp. 82-105, Jan. 2022, doi: 10.1109/OJCOMS.2022.3143098.
5. H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J.-M. Lee, "Blockchain-enhanced feature engineered data falsification detection in 6G in-vehicle networks," IEEE Internet of Things Journal, vol. 12, no. 15, pp. 30036-30052, Aug. 2025, doi: 10.1109/JIOT.2025.3569845.
6. I. M. Varma and N. Kumar, "Blockchain-based SDN-enabled lightweight authentication protocol for IoV using zk-SNARK," IEEE Transactions on Network and Service Management, vol. 23, pp. 211-224, 2026, doi: 10.1109/TNSM.2025.3613415.
7. H. Zhu, J. Wang, W. Zhu, Q. Huang, H. Xu, Z. Yu, W. Liu, and X. Xue, "Distributed edge intelligence framework for secure and efficient data sharing in 6G-IoV," IEEE Internet of Things Journal, vol. 13, no. 5, pp. 8169-8183, Mar. 2026, doi: 10.1109/JIOT.2025.3613751.
8. A. Sharma and S. Rani, "Enhancing 6G-IoT network security: A trustworthy and responsible AI-driven stacked-hybrid model for attack detection," IEEE Internet of Things Journal, vol. 13, no. 5, pp. 7777-7790, Mar. 2026, doi: 10.1109/JIOT.2025.3566403.
9. H. Sedjelmaci, N. Kaaniche, A. Boudguiga, and N. Ansari, "Secure attack detection framework for hierarchical 6G-enabled Internet of Vehicles," IEEE Transactions on Vehicular Technology, vol. 73, no. 2, pp. 2633-2643, Feb. 2024, doi: 10.1109/TVT.2023.3317940.
10. H. Sedjelmaci and M. Ayaida, "Robust zero trust systems based on collaborative AI to secure the 6G-enabled VANETs," IEEE Wireless Communications, vol. 32, no. 2, pp. 164-170, Apr. 2025, doi: 10.1109/MWC.003.2300571.
11. J. Zhang, C. Luo, Y. Jiang, and G. Min, "Security in 6G-based autonomous vehicular networks: Detecting network anomalies with decentralized federated learning," IEEE Vehicular Technology Magazine, vol. 20, no. 1, pp. 83-91, Mar. 2025, doi: 10.1109/MVT.2024.3520907.
12. M. R. H. Mahin, P. Chakraborty, N. Das, H. Kaur, H. U. Himel, J. Kaur, and A. G. Mohapatra, "Secured and standardized intelligent zero-touch 6G framework for Edge-AI applications," IEEE Communications Standards Magazine, 2026, doi: 10.1109/MCOMSTD.2026.3660159.
13. A. Bilal, K. Sharif, L. Zhu, C. Xu, F. Li, S. Bukhari, and S. Biswas, "Impact of intelligent technologies on IoV security: Integrating edge computing and AI," arXiv preprint arXiv:2604.10052, Apr. 2026.
14. [14] E. M. Mianji, G.-M. Muntean, and I. Tal, "Enhancing vehicular network security, privacy, and trust through reinforcement learning: A comprehensive survey," IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 12, pp. 21393-21420, Dec. 2025, doi: 10.1109/TITS.2025.3612202.
15. C. de Alwis, O. Aouedi, J. Xu, S. Wang, Y. Siriwardhana, T. Hewa, E. Zeydan, C. Sandeepa, and M. Liyanage, "Federated learning for 6G security: A survey on threats, solutions, and research directions," IEEE Communications Surveys & Tutorials, vol. 28, pp. 4883-4925, 2026, doi: 10.1109/COMST.2026.3663434.



DOI: http://doi.org/10.5281/zenodo.20557249

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

16. H. Sedjelmaci, N. Kaaniche, A. Boudguiga, and N. Ansari, "Secure attack detection framework for hierarchical 6G-enabled Internet of Vehicles (HAL extension)," HAL Open Science, hal-04227768, Oct. 2023.
17. A. D. Abdullahi, E. Bahrami, T. Dargahi, M. Al-Khalidi, and M. Hammoudeh, "Interplay between security, privacy and trust in 6G-enabled intelligent transportation systems," IEEE Open Journal of Intelligent Transportation Systems, vol. 6, pp. 1625-1644, Nov. 2025, doi: 10.1109/OJITS.2025.3637333.
18. R. Kumar, J. Dutta, N. Vamsi, U. S. Varri, and D. Puthal, "Next-generation security in the 6G era: The role of AI in safeguarding future networks," IEEE Access, vol. 14, pp. 17347-17371, Feb. 2026, doi: 10.1109/ACCESS.2025.3650208.
19. M. Kim, I. Oh, K. Yim, M. Sahlabadi, and Z. Shukur, "Security of 6G-enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies," IEEE Access, vol. 12, pp. 33972-34002, Mar. 2024, doi: 10.1109/ACCESS.2023.3348409.
20. National Institute of Standards and Technology, "Post-quantum cryptography standardization: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA)," NIST, 2024.



DOI: http://doi.org/10.5281/zenodo.20557249