Exploring Cyber Trends and Threats Towards V2X Connected Vehicles in Malaysia: A Systematic Literature Review

A'in Hazwani Ahmad Rizal[1], Noor Afiza Mat Razali[2]*, Sakinah Ali Pitchay[3], Taqiyuddin Anas[4]
Faculty of Defence Science and Technology, National Defence University of Malaysia,
Sungai Besi, 57000 Kuala Lumpur, Malaysia[1, 2]
Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai, 71800, Negeri Sembilan, Malaysia[3, 4]

***Abstract*—The rapid expansion of 5G enabled Vehicle to Everything (V2X) communication has evolved into an intelligent transportation system by supporting applications such as autonomous driving, real-time traffic optimization, and road safety management. However, the growing connectivity and diverse communication protocols also create major cybersecurity challenges, especially in the network tier of connected vehicles. This study conducts a systematic literature review following the PRISMA framework to examine cybersecurity threats and detection models in Malaysia's V2X ecosystem. It involves an analyzing phase towards 85 peer-reviewed studies published between 2016 and 2025. This addresses three research questions: (RQ1) What is the state-of-the-art in CVs in the aspect of network technology in Malaysia, (RQ2) What are the cybersecurity trends and threats towards CVs in the network tier, and (RQ3) What are the existing models in detecting and responding to cyber threats against CVs? Study identifies critical threats, including spoofing, jamming, and denial of service attacks, while evaluating intrusion detection systems that use machine learning, deep learning, and hybrid approaches. The existing approaches are yet to face limitations in real-time performance, contextual accuracy, and supply chain resilience under Malaysia's tropical urban conditions. This study proposes a conceptual model, the SCARF-V2X model, an NGSOC integrated concept that utilizes SIEM, SOAR, and Malaysian cyber threat intelligence platforms to enable automated detection and first-layer auto-response, specifically towards supply chain threats in CVs. The proposed model aims to improve Malaysia's V2X cybersecurity landscape and introduces a proactive and adaptive model to protect CVs against evolving cyber threats.**

Keywords*—5G; V2X; connected vehicles; cybersecurity; intrusion detection systems; anomaly detection; spoofing; DoS; network tier; machine learning

I. Introduction

The integration of fifth-generation network (5G)-enabled Vehicle-to-Everything (V2X) communication has transformed the intelligent transportation systems and enabled a real-time data exchange in smart cities, which includes autonomous driving, traffic optimization, and collision avoidance [1],[2],[3]. In Malaysia, the smart cities initiatives project like the Cyberjaya 5G testbed demonstrates the potential of these technologies, which have the potential to achieve latencies as low as 23ms for safety-critical messaging [4]. However, this hyper-connectivity also exposes the opportunities in the attack surface for cyber threats, particularly in the network tier where vehicles interact with infrastructure, cloud platforms, and other devices [5], [6],[7],[8],[9].

Malaysia's tropical urban environments introduce unique challenges to V2X security [10], including the signal attenuation from high humidity and complex multi-path propagation in dense cities such as Kuala Lumpur, Malaysia [11]. Rain attenuation creates natural 'blind spots' [10] that the malicious actors could synchronize it with the recent and advanced cyber incidents. This has been reported in Malaysia, where several cyber incidents have occurred, including ransomware attacks on Klang Valley's traffic management systems [12] and spoofed Radio Frequency Identification (RFID) and toll transactions [13], highlighting the urgent need for robust cybersecurity measures. These threats mirror the global cyber trends, which are the false message injection [14] and Distributed Denial of Service (DDoS) attacks [15], but these are exacerbated by local infrastructure gaps and the rapid adoption of heterogeneous technologies such as Dedicated Short-Range Communication (DSRC) and Cellular Vehicle-to-Everything (C-V2X) [4],[16].

Existing Intrusion Detection Systems (IDS) leverage machine learning (ML) and deep learning (DL) to identify the anomalous behaviors in the vehicular systems, yet they often fail to address the real-time performance, where high mobility in urban corridors demands detection latencies under 100ms [17], yet models like Random Forests [18] struggle with scalability. This also includes Context-aware threat intelligence, where there are several reported attacks on Malaysian telematics systems [19] that require localized detection frameworks, akin to IoT threat models in smart homes [20] or political security prediction systems [21]. Lastly, the focus on the supply chain risk, where it could compromise the On-The-Air (OTA) updates [22], necessitates solutions inspired by Industry 4.0 automation safeguards [23].

This study has seven sections, which start with Section I: Introduction. Section II outlines the Methods used in searching the relevant published papers related to these studies. Section III details the Results based on the criteria and the final list of the chosen papers to be discussed. Section IV presents the Discussion on the elements related to the research questions that have been listed in Section II. It also presents the Proposed Conceptual Model that will focus to improve the detection system in V2X communication in vehicular system within

*Corresponding author.

Malaysia ecosystem. Section V gives away Future Works to be completed to evaluate the effectiveness of the proposed conceptual model and lastly Section VI is the study's Conclusion.

This study bridges these gaps through a systematic review of 5G-V2X cybersecurity, with three research questions listed in Table I. This study synthesizes global advancements in V2X cybersecurity and contextualizes them within Malaysia's regulatory landscape and environmental constraints, thereby offering a strategic model for enhancing the resilience of the nation's connected mobility ecosystem against emerging cyber threats [36].

II. METHODS

This study employed a systematic literature review (SLR) guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework [37] to identify, evaluate, and synthesize relevant research on cybersecurity threats and detection models in Malaysia's 5G-V2X ecosystem. The methodology was designed to address three research questions (RQs) while ensuring transparency and reproducibility. Table I lists the details of the study methodology.

TABLE I. RESEARCH METHODOLOGY

Research Questions	RQ1: What is the state-of-the-art in CVs in the aspect of network technology in Malaysia? RQ2: What are the cybersecurity trends and threats towards CVs in the network tier? RQ3: What are the existing models in detecting and responding to cyber threats against CVs?
Research Dates	January 2016 – November 2025
Databases	a. IEEE Xplore b. ScienceDirect c. SpringerLink d. ACM Digital Library e. Google Scholar f. Malaysian government and industry reports
Search Criteria	**Inclusion:** a. Studies focusing on V2X communications, cybersecurity threats, and intrusion detection models in connected vehicles. b. Research conducted in Malaysia or applicable to tropical urban environments. c. Peer-reviewed journal articles, conference papers, and credible technical reports. **Exclusion:** a. Studies unrelated to vehicular networks or cybersecurity. b. Non-English publications without verified translations. c. Opinion pieces or non-peer-reviewed sources lacking empirical data.
Search Keywords	RQ1: "Connected vehicles Malaysia," "V2X network technology," "DSRC vs. C-V2X Malaysia," "5G vehicular communication" RQ2: "Cybersecurity threats connected vehicles," "V2X attack vectors," "Malaysia ransomware attacks transportation," "spoofing jamming V2X" RQ3: "Intrusion detection systems connected vehicles," "machine learning V2X security," "deep learning anomaly detection," "hybrid IDS vehicular networks"
Search Methods	**Systematic Database Queries:** a. Boolean operators (AND, OR) refined searches b. Filters applied for publication year (2016–2024) and document type **Snowballing:** a. Backwards referencing of citations in key papers to identify foundational studies. Grey Literature Review: Government reports, whitepapers, and industry case studies

Fig. 1 illustrates the flowchart for evaluating each paper by adopting the PRISMA flowchart [37]. PRISMA flowchart has been chosen in this study, as it assists in transparency and clarity of the content, specifically for this topic.

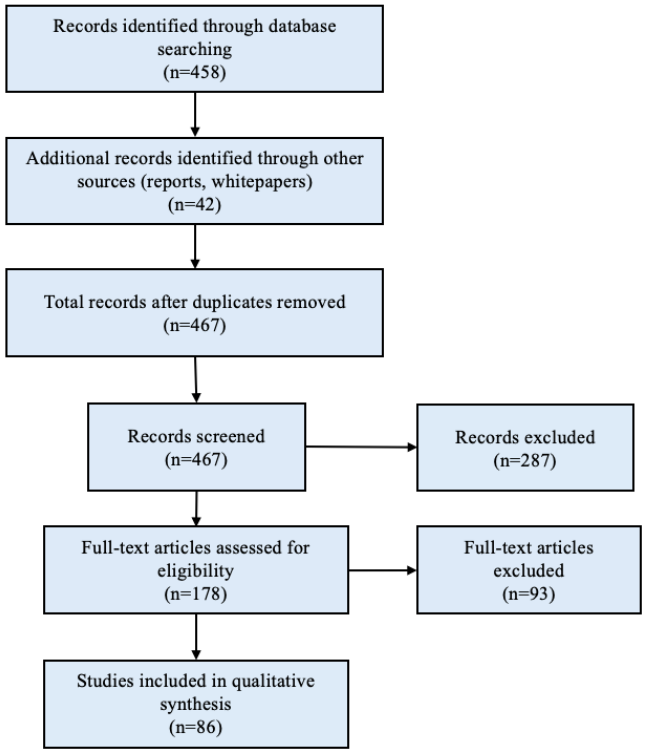

Fig. 1. The PRISMA flowchart.

III. RESULTS

From the analysis and synthesis made on the chosen papers, 86 papers have been selected from the publication years of 2013 to 2025. The year 2024 is the highest number of studies related to security in vehicular systems, as illustrated in Fig. 2. There is one published paper in 2013 that has been selected for this study, as this is the best reference for the Fuzzy Delphi Method (FDM) that has been implemented in vehicular systems [51].

The selection process in determining the published papers for this study is very crucial to preserve the quality of the literature review of the paper and the evaluation of the discussion made for the three research questions, as stated in Table I. The evaluation studies have been tailored to the situation in Malaysia, where this country is still developing and transitioning at a proper pace, and a smart city will be adopted. By referring to the adoption of different countries and assessing the relation between climate in Malaysia and the safety in autonomous vehicular systems, this can help other researchers and the nation to build a safe V2X communication within the Malaysian ecosystem. By identifying the current technology in

V2X communication adopted in Malaysia (RQ1), analyzing the impact of cyber threats against the transportation system in Malaysia as it is part of the National Critical Information Infrastructure (NCII) (RQ2) and evaluating the current methodology used to defense in V2X communication (RQ3), this paper can be one of the best reference to improve and build a resilience in smart city in Malaysia.

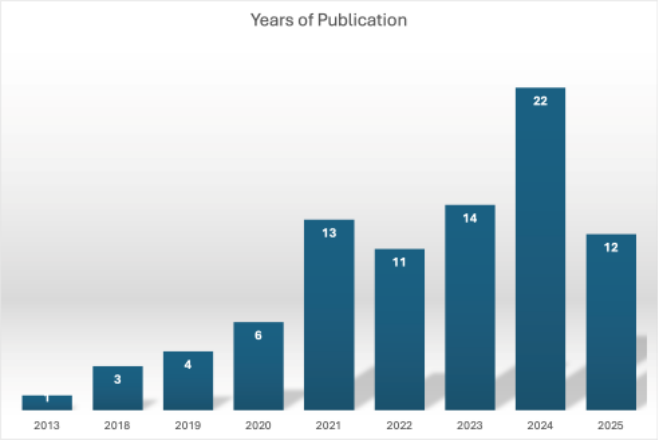

Fig. 2. Years of publication.

IV. Discussion

In this section, three main topics have been discussed in order to fulfil the three research questions in this study.

A. The State-of-the-Art CVs in the Aspect of Network Technology in Malaysia

Malaysia's CVs ecosystem has undergone a significant transformation through a strategic adoption of Dedicated Short-Range Communications (DSRC) and Cellular V2X (C-V2X) technologies, tailored to address the unique challenges of tropical urban environments [38], [12], [39]. DSRC is one of the wireless technology standards (based on IEEE802.11p), which has designed for fast and reliable communication between vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications [86]. This communication offers fast detection to protect the safety of the travelling public. On the other hand, C-V2X is a Cellular-based communication technology that enables vehicles to exchange information with other vehicles (V2V), roadside infrastructure (V2I), pedestrians (V2P), and broader networks (V2N). This cellular technology supports safer and more efficient transportation systems through the real-time sharing of data such as location, speed, and hazard notifications. This technology operates through either direct short-range links (PC5) or network-assisted connections (Uu), making it suitable for a wide range of applications, including collision avoidance, traffic optimization, and the advancement of autonomous driving systems. In C-V2X methodology, it follows the concept of edge computing, where the communication between the client (the connected vehicles) and the servers will pass through the edge nodes [27]. The utilization of edge computing has reduced the latency in data transmission, making it more reliable for critical infrastructure such as connected vehicles [27].

From the comparison testing in DSRC and C-V2X, empirical studies reveal substantial improvements in network reliability, with documented packet delivery ratios progressing from 82% to 98% across various deployment scenarios. For instance, field measurements in Kuala Lumpur's dense urban corridors demonstrate the real-world performance of DSRC [12], showcasing median latencies of 47ms ± 12ms during peak traffic conditions. However, these trials also highlight environmental challenges, as packet delivery rates drop to 68% in complex non-line-of-sight situations due to signal attenuation from high-rise structures and humidity [11]. The PLUS Expressway electronic toll collection system stands as a notable success story, achieving 99.2% vehicle identification accuracy through optimized antenna placement and dynamic power control algorithms [13].

The transition to 5G-enabled C-V2X represents a leap forward in Malaysia's connected mobility infrastructure. Controlled trials in the Cyberjaya 5G testbed have recorded end-to-end latencies as low as 23ms ± 7ms for critical safety messages which has shown a remarkable 62% reduction compared to legacy DSRC systems [4], as illustrated in Fig. 3. Similarly, Penang's Smart Traffic System has implemented LTE-V2X (Release 14) enhanced with locally developed congestion-control algorithms, maintaining 98.4% communication reliability even under extreme vehicle densities of 1,200 vehicles/km² [40]. These advancements underscore Malaysia's growing expertise in adapting global V2X standards to local conditions.

At the protocol level, Malaysian researchers have made significant contributions to optimizing the V2X stack. The Enhanced EDCA (E-EDCA) modification reduces channel access delays by 28.4% through dynamic contention window adjustments, addressing the high contention inherent in urban vehicular networks [41]. Physical layer innovations, such as adaptive 16/256-QAM modulation, improve spectral efficiency by 37% in variable channel conditions [39], while Hybrid ARQ implementations achieve 99.1% reliability for safety-critical message transmission [42]. These protocol enhancements are complemented by architectural innovations, including the Malaysian Automotive Institute's hybrid gateway prototype, which enables seamless handovers between DSRC and C-V2X technologies while maintaining switching latencies below the critical 100ms threshold [43].

Looking ahead, challenges remain in achieving seamless interoperability between disparate V2X technologies and ensuring consistent performance during Malaysia's prolonged monsoon seasons. The integration of machine learning-based traffic flow prediction models [34], [58] with V2X systems presents a promising avenue for optimizing network resource allocation in real-time [44]. As Malaysia continues to expand its 5G-V2X deployments, these innovations position the nation as a regional leader in adapting CV technologies to tropical urban environments while highlighting the need for ongoing research into climate-resilient communication protocols.

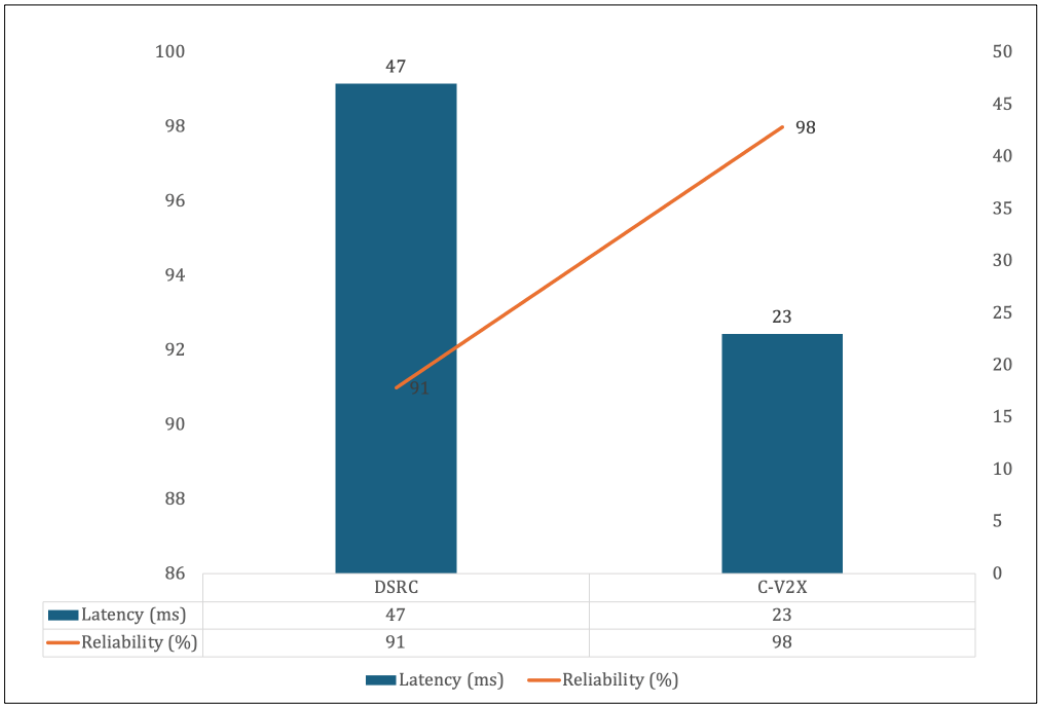

Fig. 3. The comparisons of latency and reliability in DSRC and C-V2X.

B. *Cybersecurity Trends and Threats of CV's Network Tier in Malaysia*

The rapid deployment of 5G-V2X technologies in Malaysia has introduced a complex attack surface across vehicular communication networks, cloud platforms, and IoT-enabled infrastructure [45]. While these interconnected systems enable advanced mobility solutions, they have also become targets for increasingly sophisticated cyber threats, including large-scale data breaches, ransomware attacks, and vehicular system manipulations [25], [46]. As connected vehicles evolve, they inherit the attack surfaces of both automotive and IoT systems [47], [48], [27]. The real-world cases exemplify the three primary threat categories facing Malaysia's V2X ecosystem, including communication channel exploits, telematics system breaches, and infrastructure attacks [57].

The communication layer presents particularly acute risks due to Malaysia's hybrid deployment of DSRC and C-V2X technologies. Security analyses have identified recurring patterns of false message injection attacks, where malicious actors transmit fabricated collision warnings or traffic alerts to manipulate driver behavior [14]. These attacks exploit the inherent trust models in V2X communications, where vehicles often prioritize low-latency message delivery over rigorous authentication. Concurrently, jamming attacks targeting 5G-based C-V2X signals have emerged as a persistent threat, potentially causing communication blackouts along smart highway corridors [24]. The tropical urban environment exacerbates these challenges, as signal attenuation in high-density areas like Kuala Lumpur's city center creates opportunities for intermittent jamming that may evade conventional detection systems [11].

Beyond communication channels, cloud-based telematics platforms have proven vulnerable to sophisticated intrusions [9], [49]. A 2024 breach of Prasarana's database exposed sensitive personal information, involving part of its internal systems, which may risk over hundreds of Malaysian's safety while using public transportation systems [26],[50],[51]. Forensic investigations attributed this incident to weak API authentication protocols that allowed SQL injection attacks [52]. Similarly, two major ransomware attacks hit two different transportation services involving Malaysia Airport Holdings Berhad (MAHB) and a well-known Malaysian airline, exposing thousands of sensitive personal information of their passengers [19],[53],[54]. These breaches highlight the urgent need for robust encryption and access control mechanisms in Malaysia's growing CVs ecosystem.

Various studies highlight real-world incidents involving firmware tampering [55] and malicious updates in IoT systems, which apply to V2X contexts [56], [30]. Transportation infrastructure supporting V2X networks has also emerged as a high-value target. On Malaysia's PLUS Highway network, security analysts uncovered an elaborate RFID toll payment fraud scheme that exploited cloned tags to evade charges, resulting in substantial revenue losses [13]. These incidents underscore the cascading impacts of infrastructure compromises, where single points of failure can affect thousands of vehicles and passengers daily [55].

From Table II, cyberattacks in the transportation system have impacted all layers of the OSI model from Layer 1 to Layer 7. On the other hand, from the recent reports of cyber-attacks towards transportation cases that happened specifically in Malaysia have been listed in Table III by referring to the Open Systems Interconnection (OSI) Model for a better visualization and understanding. In Table II, there are a total of nine cases related and four layers in the OSI Model impacted in the cyber incidents that occurred related to transportation and vehicular

systems, those are physical, data link, network and applications. Application layer, which is also layer 7, is the most cited attacks occurs involving the surface attack methodology. Layer 4, 5, and 6 attacks do exist in transportation systems, but they are not explicitly reported in Malaysian transportation cyberattack cases. Cases such as ransomware attacks [19], [53], [54], database compromise [52], RFID toll fraud [13]and jamming and signal distraction [11], [24] are the results of successful bypass in OSI model layer 4,5 and 6, which enable the attack.

TABLE II. CYBERATTACKS MAPPED IN OSI MODEL

OSI Layer	Layer Function in Transportation Systems	Example of Cyberattacks	Related Citation
Layer 1 Physical	Wireless signal transmission, hardware, RF environment	RF jamming (DSRC, C-V2X, 5G), GNSS spoofing, RFID tag cloning (toll systems)	[24], [69], [13]
Layer 2 Data Link	Frame delivery, MAC addressing, link-level trust	False message injection (BSM/CAM), Sybil attacks, MAC spoofing	[14], [19], [25]
Layer 3 Network	Routing and packet forwarding	Blackhole / grayhole attacks, routing manipulation, network-layer DoS	[45], [41]
Layer 4 Transport	End-to-end reliability and flow control	TCP/UDP flooding, replay amplification, session exhaustion	[42], [25]
Layer 5 Session	Session establishment and maintenance	Session hijacking, replay attacks, unauthorized session persistence	[25], [63]
Layer 6 Presentation	Data representation, encryption, key handling	Certificate manipulation, weak cryptography exploitation, message format tampering	[47], [74]
Layer 7 Application	Vehicle software, cloud platforms, APIs, OTA services	SQL injection, ransomware, malicious OTA/firmware updates, cloud API abuse	[52], [55], [49], [21]

TABLE III. MALAYSIAN TRANSPORTATION CYBERATTACKS MAPPED IN OSI MODEL

OSI Layer	Description	Related Citations	Count
Layer 1 Physical	RFID toll tag cloning / toll payment fraud	[13]	**1**
Layer 2 Data Link	False message injection (fabricated collision / traffic warnings)	[14]	1
Layer 3 Network	Jamming attacks on 5G C-V2X signals	[24], [11]	1
Layer 7 Application	Cloud telematics platform intrusion	[9], [49]	6
	SQL injection via weak API authentication	[52]	
	Ransomware attack on MAHB	[19],[53]	
	Ransomware attack on airline systems	[54]	
	Firmware tampering	[55]	
	Malicious firmware / OTA updates in IoT-V2X systems	[56],[30]	

Malaysia has responded to these challenges through a combination of regulatory measures, technological innovations, and research initiatives. The Malaysia Cyber Security Strategy (MCSS) 2020-2024 states that the 11 National Critical Information Infrastructures (NCII) and transportation is part of the sectors [36], while Automotive ISAC provides a platform for threat intelligence sharing among automakers and suppliers [35]. Industry players are deploying advanced countermeasures, including Telekom Malaysia's blockchain-based V2X authentication system [58] and PLUS Highway's machine learning-powered anomaly detection for toll transactions [13].

Emerging threats nevertheless continue to challenge these defenses. The advent of 5G network slicing introduces new attack vectors that could be exploited to disrupt emergency vehicle communications [60], while AI-powered cyberattacks using adversarial machine learning techniques pose risks of bypassing conventional security systems [61]. These evolving threats demand adaptive solutions that combine the scalability of machine learning with the rigor of formal verification methods, which is a research direction that Malaysia's automotive cybersecurity community is uniquely positioned to explore given its experience with tropical urban deployments.

C. Existing Models for Detecting and Responding to Cyber Threat Against CVs

The network tier of CVs consists of several communication and those are V2V, V2I, and V2C communications. These communications form the backbone of intelligent transportation systems but also present a critical attack surface for cyber threats. In Malaysia's evolving 5G-V2X ecosystem, where high mobility and tropical urban environments exacerbate security challenges [11], robust intrusion detection systems (IDS) must balance real-time performance with adaptability to novel attack vectors [32],[62]. This section evaluates existing detection models, their applicability to Malaysian deployments, and emerging solutions that address current gaps.

1) Traditional and machine learning based approaches: Early IDS solutions for vehicular networks relied heavily on signature-based detection, which identifies known attack patterns through predefined rules [61],[63]. While effective against documented threats like replay attacks or basic spoofing [15], these systems struggle with zero-day exploits and adaptive adversaries. The limitations of signature-based methods have spurred the adoption of machine learning (ML) techniques, which analyze network behavior to detect anomalies [31].

Studies demonstrate promising results with algorithms such as Random Forests (RF) and Support Vector Machines (SVM), achieving up to 95% accuracy in classifying malicious V2X traffic [2]. For instance, RF-based models excel in identifying false safety messages, which are a prevalent threat in Malaysia's highway systems [14]. This can occur by correlating message frequency, sender reputation, and physical plausibility checks. Machine learning-based IDS has shown promise in detecting anomalies in real-time systems [64],[18],[61]. Edge learning models further optimize detection at the network edge [65].

However, conventional ML approaches as part of defence in V2X communication face challenges where the high vehicle densities in urban corridors like Kuala Lumpur generate volatile network conditions that can trigger false positives in models trained on limited datasets [66]. Additionally, the computational overhead of techniques like K-Nearest Neighbors (KNN) may exceed the latency budgets of safety-critical applications [67], where response times under 100ms are often required [17].

2) Deep learning and hybrid architectures: To address these limitations, researchers have turned to deep learning (DL) models capable of learning complex spatial-temporal patterns in network traffic. Long Short-Term Memory (LSTM) networks have proven particularly effective for detecting time-series anomalies, such as gradual DDoS attacks that overwhelm roadside units (RSUs) with slow-rate malicious packets [68]. In the Malaysian context, where 5G-V2X deployments must handle monsoonal weather-induced signal fluctuations [11], LSTMs' ability to model temporal dependencies offers advantages over static threshold-based systems. Recent advances in GNSS-5G hybrid positioning demonstrate robust spoofing detection even during receiver maneuvers [69], suggesting potential integration with Malaysia's 5G-V2X testbed infrastructure [4].

More advanced hybrid architectures combine the strengths of multiple approaches. Yang et al.'s Multi-Tiered Hybrid IDS (MTH-IDS) [28], for instance, integrates signature matching, statistical anomaly detection [70], [62], and deep learning to achieve comprehensive coverage across vehicular network tiers [71]. When tested in environments resembling Malaysia's heterogeneous DSRC/C-V2X deployments, MTH-IDS maintained detection rates above 92% while keeping processing latency below 50ms, which shows a critical benchmark for real-time safety applications [28].

3) Emerging paradigms: federated learning and adversarial defense: Zero trust frameworks advocate continuous authentication [72], complementing Malaysia's exploration of two promising directions for Malaysia's V2X security landscape, which are federated learning and adversarial resilience. Federated learning enables collaborative model training across distributed nodes without centralised data aggregation [73], addressing privacy concerns while improving detection coverage [29]. This approach aligns with Malaysia's Auto-ISAC framework [35], where threat intelligence sharing among automakers could enhance collective defense without compromising proprietary data.

Meanwhile, the rise of AI-powered attacks [28],[61] necessitates IDS models resistant to adversarial manipulation. Techniques like Generative Adversarial Networks (GANs) [61] can simulate attack variants to harden detection systems, explore long-term protections against future computational threats [74].

This section systematically evaluates intrusion detection and response mechanisms for securing Malaysia's 5G-V2X networks against evolving cyber threats. Traditional signature-based IDSs prove inadequate against novel attacks, prompting the adoption of machine learning (ML) models like Random Forests (95% accuracy) and Support Vector Machines, though their real-time performance in high-density urban environments remains challenging. Deep learning solutions, particularly LSTM networks, address temporal attack patterns (e.g., slow-rate DDoS), while hybrid models (e.g., MTH-IDS) combine multiple techniques to achieve >92% detection rates with sub-50ms latency, which is critical for safety applications. Emerging approaches like federated learning enable collaborative threat analysis without compromising data privacy, aligning with Malaysia's Auto-ISAC framework, while adversarial ML defenses counter AI-powered attacks.

4) Proposed conceptual model: To mitigate the escalating threat of supply chain attacks within Malaysia's rapidly evolving 5G-enabled Vehicle-to-Everything (V2X) ecosystem, this study introduces the SCARF-V2X (Supply Chain Attack Resilience Framework for V2X) model. SCARF-V2X is a Security Operations Center (SOC)-integrated solution that enhances the cybersecurity posture of CVs by enabling automated detection and response to supply chain threats. Fig. 5 is the conceptual model that adopts the NIST Cybersecurity Framework as part of the model, as illustrated in Fig. 4. As V2X architectures grow in complexity, where they can incorporate components such as over-the-air (OTA) firmware updates, roadside units (RSUs), and diverse vehicular communication protocols, the adversaries are increasingly targeting these vectors to introduce malicious code or manipulate vehicular behaviour [61],[22], [68],[75].

Fig. 4. NIST cybersecurity framework 2.0.

These challenges are particularly acute in the Malaysian context, where research has highlighted significant vulnerabilities in telematics platforms and a lack of localized and context-aware intrusion detection capabilities [19], [22],[42]. Existing Intrusion Detection Systems (IDS) often lack adaptability and automation, rendering them ineffective against sophisticated, multi-stage supply chain intrusions. SCARF-V2X addresses these limitations by integrating core enterprise SOC components such as Security Information and Event Management (SIEM) [76],[85] and Security Orchestration, Automation, and Response (SOAR) into the vehicular cybersecurity stack [77]. By contextualizing these tools for automotive environments, SCARF-V2X supports real-time detection, automated containment, and collaborative threat intelligence sharing through platforms like Auto-ISAC [35], [78].

Through this integration of behavioral analytics, automation, and policy-aware response mechanisms, SCARF-V2X represents a novel approach to safeguarding 5G-CVs against emerging supply chain threats, building on frameworks for regulatory harmonization [79].

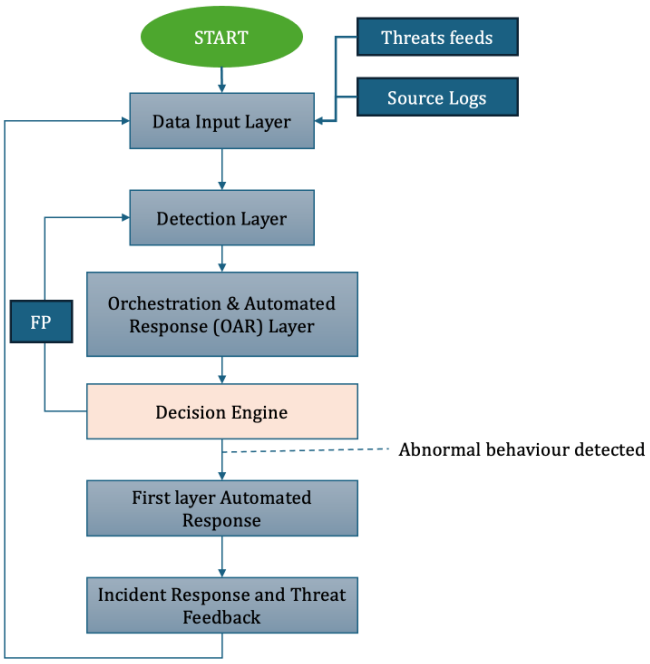

Fig. 5. The proposed conceptual model.

The framework begins with a data input layer that consolidates telemetry from both internal vehicle networks and external intelligence sources. Internally, it ingests logs from the CAN bus, V2X communication messages, and 5G traffic, which collectively offer insight into both hardware integrity and message-level anomalies [74], [80]. Externally, it integrates threat intelligence feeds from platforms such as MISP [81], Auto-ISAC, and MyCERT [59]. These sources ensure that detection efforts are continuously updated with localized Indicators of Compromise (IOCs) and emerging threat patterns relevant to Malaysia's vehicular cybersecurity landscape [35],[36].

The detection layer leverages a SIEM platform to perform log ingestion, parsing, and correlation. It applies finely tuned rules and behavioral models to identify suspicious events across the vehicular network stack. For instance, anomalies in V2X message frequencies, spoofed firmware update attempts, or inconsistent 5G session behaviors are detected through rule-based and heuristic approaches [28],[55]. SIEM also enriches its alerting mechanisms by correlating internal data with external threat intelligence, thus increasing detection precision and reducing false positives [85].

Once suspicious behavior is identified, the response layer, powered by a SOAR system, activates corresponding incident workflows. The SOAR component manages alert triage, maps detection artefacts to the MITRE ATT&CK framework, and executes automated playbooks [82]. These playbooks may include isolating compromised RSUs, rolling back OTA firmware updates, disabling Advanced Driver Assistance Systems (ADAS), or blocking communication from malicious IP addresses [80],[56]. SOAR also performs initial severity calculations to determine whether alerts warrant full-scale incident response or can be resolved through localized automation.

The decision-making engine within SCARF-V2X assesses whether an alert reflects genuine malicious behavior or a false positive. In the case of a false positive, the framework loops back to fine-tune detection rules and behavioral baselines. If the alert is validated as a true positive, a first-layer automated response is initiated. This lightweight response provides immediate mitigation actions while reducing analyst workload and response time. For higher-severity alerts, the incident is escalated for deeper investigation by analysts or original equipment manufacturer (OEM) cybersecurity teams. Such escalation includes forensic analysis, root cause determination, and long-term remediation strategies.

Several works stress the urgency for a proactive and adaptive detection framework in automotive supply chains [78], [83]. This study adopts a supply chain attack use case into the SCARF-V2X framework, as illustrated in Fig. 6. This framework also incorporates a continuous feedback loop wherein verified threat data and incident insights are shared with CTI platforms such as MISP and Auto-ISAC. This promotes collaborative defense, policy compliance, and alignment with MCSS 2020-2024 [36], [55]. Furthermore, by embedding automation, behaviour analysis, and threat intelligence within an SOC paradigm adapted for V2X, SCARF-V2X represents a novel approach to automotive cybersecurity. It surpasses traditional standalone intrusion detection models, such as GIDS (Generic Intrusion Detection System), by integrating policy-aware response automation, federated learning support, and localized threat intelligence sharing [35],[36],[84].

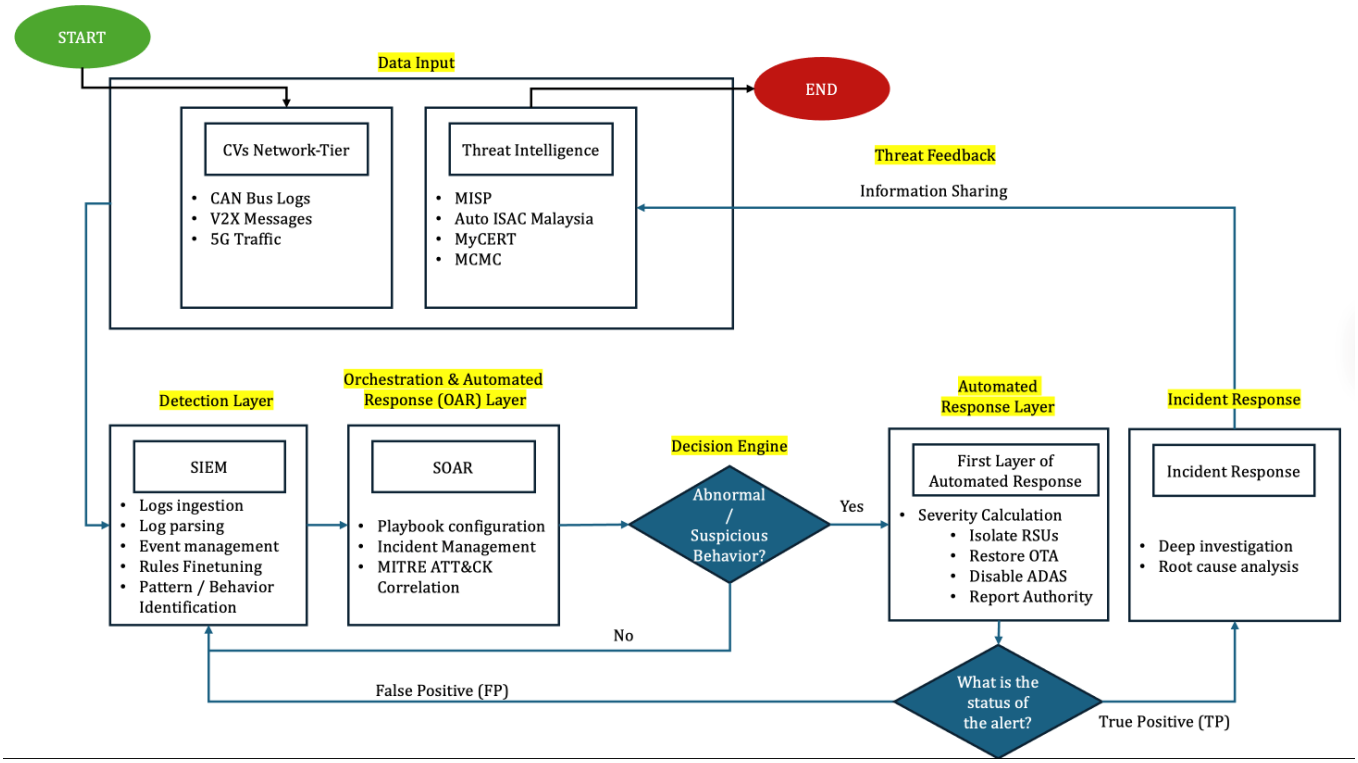

Fig. 6. Supply chain attack use case adoption in the conceptual model.

V. Future Works

As part of the research, this study will run two phases of evaluation methods to enhance the structure of the SCARF-V2X model. Those are the Fuzzy Delphi Method (FDM) and running a simulation experiment. Both evaluation and validation activities are crucial for this study, where we believe the FDM will assist in connecting the bridge between theoretical study and the industrial expert panels, while the simulation experiment will be the benchmark result of this proposed conceptual model.

A. Fuzzy Delphi Method (FDM)

The first activity is by deploying the Fuzzy Delphi Method (FDM) to evaluate each phase in conceptual model, as stated in Fig. 5 and adopting the supply chain attack simulation, as shown in Fig. 6. FDM has been chosen as part of these future work efforts, as FDM is an advanced decision-making technique that combines the traditional Delphi method with fuzzy logic to handle uncertainty and subjectivity in expert judgments. It is widely used in forecasting, policymaking, risk assessment, and consensus-building, where expert opinions may be vague or imprecise [9],[33],[51].

From the process flow of FDM illustrated in Fig. 7, the process begins after the conceptual framework has been structured and the researcher needs to select at least 10 to 15 expert panels from the related sectors, with the framework including the regulator and local Managed Security Service Provider (MSSP) and Subject Matter Experts (SME), which involves SIEM engineers and SOC Consultants. The uniqueness of FDM is the combination of the qualitative and quantitative methodology, where it balances between the need for the opinion from the industrial experts and the logics calculation, which would stabilize the final decision. Once the researcher reaches the expert consensus, the framework will proceed with the second activity in the evaluation phase.

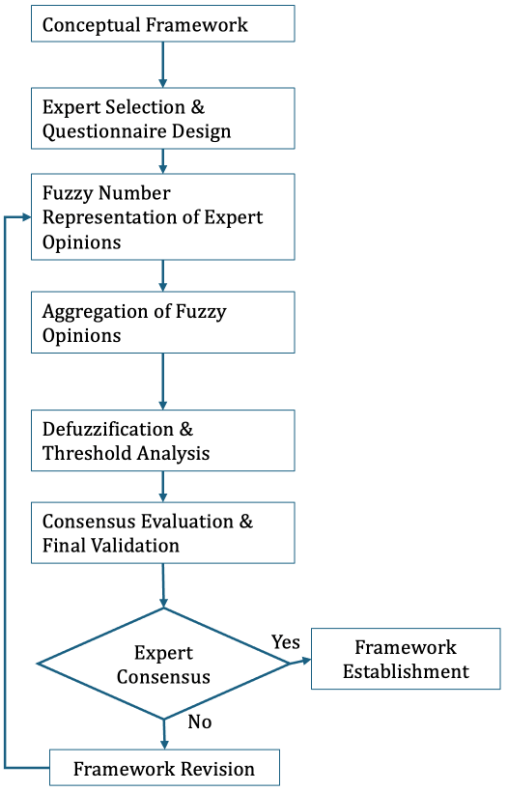

Fig. 7. Fuzzy Delphi process flow.

B. Simulation Experiment

This experiment will be run in a controlled lab environment, where the V2X logs will be recorded and used in SIEM, as illustrated in Fig. 8. The first step is to install the virtual machine (VM) that will be used to install the SIEM. All the V2X logs will be ingested into the SIEM before the parsing activity takes place. The parsing is a crucial phase as it assists in standardizing the format, which could help to columnize the information into an event. A malicious script will be created based on the use case scenario of injecting a fake OTA update through the network layer in the CVs ecosystem. Once the playbook has been created and finetuned, the malicious script will be injected into the environment, and the detection shall flag the events. The first layer of auto response from the SOAR features should be activated and notify the SIEM end users as the second layer response phase.

The stated experiment simulates the real case scenario of how the SOC and SOAR are deployed and react if there are any cyber incidents occur in the environment. The manipulated variable in this situation is the V2X logs, which are only used for research purposes and not being tested in a production environment.

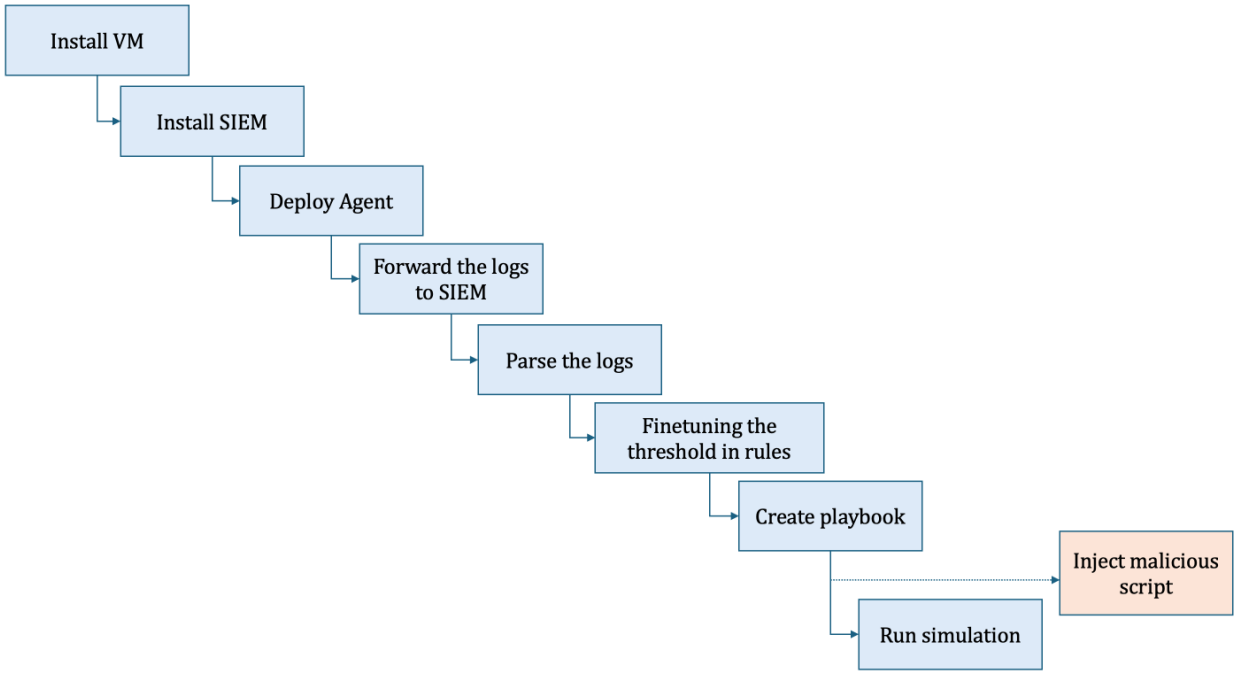

Fig. 8. The process flow to run simulation activity for SCARF-V2X model.

VI. Conclusion

The three research questions have been answered throughout the SLR approach in this study. For RQ1, the technology evolving in the CVs system has been continuously improving from the Cyberjaya testbed, and it shows an improving result from the statistics shown. The adoption of the emerging 5G networks and V2X communication in Malaysia is showing an increasing accuracy rate from the previous result. However, the threats and trends of cybersecurity attacks have been explained as part of RQ2. The trends of external attack surface towards CVs in Malaysia, especially when it involves public safety, need to be placed as a critical impact and require immediate remediation. The recent cyber-attacks that hit major national transportation systems, such as the Prasarana breach attack, Malaysia Airport Holding Berhad's (MAHB) ransomware attacks and the Malaysian airline's ransomware attack, are signs of the critical need for extra safety measures towards vehicle safety, especially CVs.

The integration of 5G-enabled Vehicle-to-Everything (V2X) communication in Malaysia represents a significant advancement in intelligent transportation systems, offering substantial benefits for autonomous driving, traffic optimization, and collision avoidance. However, this technological progress comes with heightened cybersecurity risks, particularly in the network tier where vehicles interact with infrastructure, cloud platforms, and other devices. Malaysia's unique tropical urban environment further complicates these challenges, with issues such as signal attenuation and complex multi-path propagation in dense cities like Kuala Lumpur exacerbating vulnerabilities. Recent incidents, including ransomware attacks on traffic management systems, spoofed toll transactions, and remote vehicle hijacking, underscore the urgent need for robust cybersecurity measures tailored to local conditions.

This study addresses these challenges through a systematic review of cybersecurity threats and detection models in Malaysia's 5G-V2X ecosystem. The research highlights three key contributions: a comprehensive threat taxonomy specific to Malaysian V2X networks, an evaluation of machine learning and deep learning-based intrusion detection systems, and the development of the SCARF-V2X framework. SCARF-V2X SOC tools, such as SIEM and SOAR, with localized threat intelligence and behavioral analytics, provide a proactive and automated approach to detecting and mitigating supply chain

attacks. By aligning with MCSS 2020–2024 [36] and leveraging collaborative platforms like Auto-ISAC Malaysia, the framework ensures compliance with national regulations, while enhancing the resilience of connected vehicles against evolving threats.

Despite these advancements, several areas require further exploration to strengthen Malaysia's V2X security posture. Future research should focus on integrating quantum-resistant cryptography to safeguard against emerging computational threats, as well as advancing federated learning techniques to enable privacy-preserving threat intelligence sharing among stakeholders. Additionally, the development of explainable AI models will improve transparency in automated security decisions, fostering trust in these systems.

In summary, this study provides a critical foundation for securing Malaysia's 5G-V2X ecosystem against sophisticated cyber threats. The SCARF-V2X framework, with its emphasis on automation, localized threat intelligence, and policy compliance, offers a scalable and adaptive solution for safeguarding connected vehicles in Malaysia's unique urban and environmental context. As the nation continues to advance its intelligent transportation infrastructure, ongoing innovation and collaboration will be vital to maintain a secure and resilient mobility ecosystem in the face of evolving cybersecurity challenges.

REFERENCES

[1] M. J. Khan, M. A. Khan, A. Beg, S. Malik, and H. El-Sayed, "An overview of the 3GPP identified Use Cases for V2X Services," *Procedia Comput Sci*, vol. 198, pp. 750–756, 2022.

[2] T. Seetamonee and G. Bekaroo, "Modern detection techniques of false data injection attacks in v2x communication: A critical analysis," in *International Conference on Innovations and Interdisciplinary Solutions for Underserved Areas*, Springer, 2023, pp. 66–80.

[3] Z. Zheng, M. Zhou, Y. Chen, M. Huo, and D. Chen, "Enabling real-time road anomaly detection via mobile edge computing," *Int J Distrib Sens Netw*, vol. 15, no. 11, p. 1550147719891319, 2019.

[4] N. I. Jasim, S. Shamini, M. A. Al-Sharafi, M. A. Mahmoud, M. Ibrahim, and A. Hassan, "Adoption and Implementation Trends of Vehicle-to-Everything (V2X) Technologies: A Comprehensive Bibliometric Analysis," in *Current and Future Trends on AI Applications: Volume 1*, Springer, 2025, pp. 329–344.

[5] A. Cartwright and E. Cartwright, "The economics of ransomware attacks on integrated supply chain networks," *Digital Threats: Research and Practice*, vol. 4, no. 4, pp. 1–14, 2023.

[6] Zhang, Xinyu & Li, Junxian & Zhou, Jingyi & Zhang, Shiyan & Wang, Jingyuan & Yuan, Yi & Liu, Jiale & Li, Jun. (2025). Vehicle-to-Everything Communication in Intelligent Connected Vehicles: A Survey and Taxonomy. Automotive Innovation. 8. 10.1007/s42154-024-00310-2.

[7] Avcı, İ.; Koca, M. Intelligent Transportation System Technologies, Challenges and Security. Appl. Sci. 2024, 14, 4646. https://doi.org/10.3390/app14114646

[8] O. C. Agbo, "Machine Learning Based Intrusion Detection Framework for CAN Bus Vulnerabilities in Modern Vehicles," 2024.

[9] N. Zainuddin, R. Yusuff, and G. Narayana Samy, "Assessing Cloud Computing Security Threats in Malaysian Organization Using Fuzzy Delphi Method," 2022, pp. 252–263. doi: 10.1007/978-3-031-00828-3_25.

[10] M. Rzooki, M. Alhilali, J. Din, and L. Hong Yin, "Rain attenuation statistics over 5G millimetre wave links in Malaysia," vol. 14, p. 1012, May 2019, doi: 10.11591/ijeecs.v14.i2.pp1012-1017.

[11] C.-S. Kim, J.-S. Kim, J.-Y. Hong, J.-S. Lim, and Y.-J. Chong, "Propagation characteristics of urban and highway vehicle-to-everything (V2X) channels at 5.9 GHz," in *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, 2021, pp. 872–876.

[12] N. I. Ramli, A. F. M. Fuad, M. F. Ibrahim, and M. I. M. Rawi, "VANET Performance Evaluation for Malaysian Urban Federal Highway," in *International Conference on Computational Science and Technology*, Springer, 2022, pp. 659–671.

[13] Z. L. Lim, "Adoption Of RFID Toll Payment Among Consumers On Highways In Penang Malaysia," *Research in Management of Technology and Business*, vol. 4, no. 2, pp. 12–22, 2023.

[14] N. A. M. Razali, N. Shamsaimon, M. Wook, and K. K. Ishak, "Conceptual model for connected vehicles safety and security using big data analytics," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, pp. 281–290, 2020.

[15] M. Islam, M. Chowdhury, H. Li, and H. Hu, "Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention," *Transp Res Rec*, vol. 2672, no. 19, pp. 66–78, 2018.

[16] L. Liang, H. Ye, and G. Y. Li, "Spectrum sharing in vehicular networks based on multi-agent reinforcement learning," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 10, pp. 2282–2292, 2019.

[17] Mubark B Jedh, Jian Kai Lee, and Lotfi ben Othmane, "Evaluation of the Architecture Alternatives for Real-time Intrusion Detection Systems for Connected Vehicles," *ARVIX Org*, Jan. 2022.

[18] S. A. A. Hakeem and H. Kim, "Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security," *IEEE Transactions on Intelligent Transportation Systems*, 2025.

[19] H. A. Ameen *et al.*, "A deep review and analysis of data exchange in vehicle-to-vehicle communications systems: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions," *IEEE Access*, vol. 7, pp. 158349–158378, 2019.

[20] S. N. S. A. Sham, K. K. Ishak, N. A. M. Razali, N. M. Noor, and N. A. Hasbullah, "IoT Attack Detection Using Machine Learning and Deep Learning in Smart Home," *JOIV: International Journal on Informatics Visualization*, vol. 8, no. 1, pp. 510–519, 2024.

[21] N. A. M. Razali *et al.*, "Political security threat prediction framework using hybrid lexicon-based approach and machine learning technique," *IEEE Access*, vol. 11, pp. 17151–17164, 2023.

[22] Omar Yang, "Emerging Threats to the Automotive Supply Chain From Ransomware Groups," 2024.

[23] M. R. A. Bakar, N. A. M. Razali, M. Wook, M. N. Ismail, and T. M. T. Sembok, "Exploring and developing an industrial automation acceptance model in the manufacturing sector towards adoption of Industry4. 0," *Manufacturing Technology*, vol. 21, no. 4, pp. 434–446, 2021.

[24] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5G new radio: A review," in *2020 10th annual computing and communication workshop and conference (CCWC)*, IEEE, 2020, pp. 1010–1015.

[25] M. M. Hamdi *et al.*, "A review on various security attacks in vehicular ad hoc networks," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 5, pp. 2627–2635, Oct. 2021, doi: 10.11591/eei.v10i5.3127.

[26] Emir Zainul, "Prasarana confirms cybersecurity breach, assures no disruption to public transport services," *The Edge Malaysia*, Kuala Lumpur, Aug. 26, 2024.

[27] K. K. Ishak, N. A. Mat Razali, N. A. Malizan, G. Sulong, and M. G. Md Johar, "Smart Cities' Cybersecurity and IoT: Challenges and Future Research Directions.," *IAENG Int J Comput Sci*, vol. 51, no. 7, 2024.

[28] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles," *IEEE Internet Things J*, vol. 9, no. 1, pp. 616–632, 2021.

[29] S. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT Edge Devices," *IEEE Internet Things J*, vol. PP, p. 1, Jul. 2021, doi: 10.1109/JIOT.2021.3100755.

[30] Q. Zhang, H. Wen, Y. Liu, S. Chang, and Z. Han, "Federated-reinforcement-learning-enabled joint communication, sensing, and

computing resources allocation in connected automated vehicles networks," *IEEE Internet Things J*, vol. 9, no. 22, pp. 23224–23240, 2022.

[31] N. Matrazali, N. Shamsaimon, K. Ishak, S. Ramli, M. F. Mohamad Amran, and S. Sukardi, "Gap, techniques and evaluation: traffic flow prediction using machine learning and deep learning," *J Big Data*, vol. 8, Dec. 2021, doi: 10.1186/s40537-021-00542-7.

[32] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Vehicular Communications*, vol. 21, p. 100198, 2020.

[33] N. Zainuddin, R. Yusuff, and G. Narayana Samy, "Assessing Cloud Computing Security Threats in Malaysian Organization Using Fuzzy Delphi Method," 2022, pp. 252–263. doi: 10.1007/978-3-031-00828-3_25.

[34] L. S. Zaabar, K. K. Ishak, and N. A. M. Razali, "Enhancement of Kansei Model for Political Security Threat Prediction Using Bi-LSTM," in *International Conference on Kansei Engineering & Emotion Research*, Springer, 2024, pp. 116–128.

[35] Automotive Information Sharing and Analysis Center, "Enhancing Automotive Cybersecurity - 2024 Report," 2024.

[36] Malaysia National Security Council, "Malaysia Cyber Security Strategy 2020-2024," Malaysia, 2020.

[37] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *bmj*, vol. 372, 2021.

[38] M. Mizmizi *et al.*, "6G V2X technologies and orchestrated sensing for autonomous driving," *arXiv preprint arXiv:2106.16146*, 2021.

[39] W. Zhuofei, S. Bartoletti, V. Martinez, and A. Bazzi, "Adaptive repetition strategies in IEEE 802.11 bd V2X networks," *IEEE Trans Veh Technol*, vol. 72, no. 6, pp. 8262–8266, 2023.

[40] R. Bera, "Smart Automotive System With CV2X-Based Ad Hoc Communication," *Cloud and IoT-Based Vehicular Ad Hoc Networks*, pp. 293–323, 2021.

[41] H. Zhang, W. Tian, and J. Liu, "Improving EDCA for efficient channel access in vehicular communications," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 72–77, 2018.

[42] A. Ahmed, A. Al-Dweik, Y. Iraqi, H. Mukhtar, M. Naeem, and E. Hossain, "Hybrid automatic repeat request (HARQ) in wireless communications systems and standards: A contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2711–2752, 2021.

[43] H. Alabdouli, M. S. Hassan, and A. Abdelfattah, "Enhancing Route Guidance Through Integrated V2X Communication and Transportation Systems: A Comprehensive Review," in *2024 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*, IEEE, 2024, pp. 1–6.

[44] S. Sundar, K. Pundalik, and U. Unnikrishnan, "Contextual Study of Security and Privacy in V2X Communication for Architecture & Networking Products," SAE Technical Paper, 2024.

[45] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2725–2764, 2020.

[46] N. F. Abdullah, T. E. Shen, A. A. Samah, and R. Nordin, "Internet of Vehicles Based On Cellular-Vehicle-To-Everything (C-V2X)," *International Journal of Integrated Engineering*, vol. 15, no. 5, pp. 244–252, 2023.

[47] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw*, vol. 34, no. 2, pp. 37–45, 2020.

[48] H. Yakan, I. Fajjari, N. Aitsaadi, and C. Adjih, "Federated learning for v2x misbehavior detection system in 5g edge networks," in *Proceedings of the Int'l ACM Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2023, pp. 155–163.

[49] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey," *ACM Comput. Surv.*, vol. 55, no. 11, Feb. 2023, doi: 10.1145/3570954.

[50] S. L. Kok and S. Siripipatthanakul, "The challenges and opportunities of Geely: A marketing case study," Tech. Rep, 2023.

[51] S. Cafiso, A. Di Graziano, and G. Pappalardo, "Using the Delphi method to evaluate opinions of public transport managers on bus safety," *Saf Sci*, vol. 57, pp. 254–263, 2013, doi: https://doi.org/10.1016/j.ssci.2013.03.001.

[52] Y. Takahito *et al.*, "A Survey of Security and Privacy Issues in V2X Communication Systems," *ACM Comput Surv*, vol. 55, Aug. 2022, doi: 10.1145/3558052.

[53] Samantha Tan Chiew Tieng and Muhammad Adil Muzaffar Mohd Fisol, "Ransomware Strike on MAHB Highlights Need For Stronger Cyber Defenses - Experts," *Bernama*, 2025.

[54] Surin Murugiah, "AirAsia hit by ransomware attack, five million passenger and employee data compromised," *theedgemarkets.com*, 2022. [Online]. Available: https://theedgemalaysia.com/article/airasia-hit-ransomware-attack-5-million-passenger-and-employee-data-compromised

[55] A. Kovacevic and N. Gligoric, "Enhancing Security of Automotive OTA Firmware Updates via Decentralized Identifiers and Distributed Ledger Technology," *Electronics (Basel)*, vol. 13, no. 23, p. 4640, Nov. 2024, doi: 10.3390/electronics13234640.

[56] S. Chatterjee, "Machine Learning and 5G Network Communication for Internet of Vehicles," 2024, *vol*.

[57] A. Giannaros *et al.*, "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 493–543, Aug. 2023, doi: 10.3390/jcp3030025.

[58] TM One, "TM One Securing Digital Transactions With Blockchain In Indonesian Market," *TM Official Website*, 2021.

[59] LebahNET Dashboard. (n.d.). *CyberSecurity Malaysia – Honeynet Project*. Retrieved January 24, 2026, from https://dashboard.honeynet.org.my/

[60] M. Islam, M. Chowdhury, H. Li, and H. Hu, "Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention," *Transp Res Rec*, vol. 2672, no. 19, pp. 66–78, 2018.

[61] L. Chi *et al.*, "Adversarial attacks on autonomous driving systems in the physical world: a survey," *IEEE Transactions on Intelligent Vehicles*, 2024.

[62] Chitoor Venkat Rao Ajay Kumar, Parnam Venkatagirish, Sai Srinivas Patibandla, and Sai Srinivas Patibandla, "Real Time Anomaly Detection and Intrusion Detection for Safeguarding Intra-Vehicle Communication Powered by AI," *World Journal of Advanced Research and Reviews*, vol. 25, no. 1, pp. 1992–2000, Jan. 2025, doi: 10.30574/wjarr.2025.25.1.0283.

[63] S. Jin, J.-G. Chung, and Y. Xu, "Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, IEEE, May 2021, pp. 1–5. doi: 10.1109/ISCAS51556.2021.9401087.

[64] A. Boualouache and T. Engel, "A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1128–1172, 2023.

[65] L. Bai, Z. Huang, Y. Ge, R. Yu, L. Wang, and X. Cheng, "Cellular Vehicle-to-Everything (C-V2X) Testing: From Theory to Practice," *IEEE Netw*, 2025.

[66] M. Driss, I. Almomani, Z. Huma, and J. Ahmad, "A federated learning framework for cyberattack detection in vehicular sensor networks," *Complex & Intelligent Systems*, vol. 8, Mar. 2022, doi: 10.1007/s40747-022-00705-w.

[67] B. John, "Machine Learning-Based Anomaly Detection in V2V and V2X Networks," 2025.

[68] B. Lampe and W. Meng, "A survey of deep learning-based intrusion detection in automotive applications," *Expert Syst Appl*, vol. 221, p. 119771, 2023.

[69] L. Bai, C. Sun, A. G. Dempster, W. Feng, and C. Zhuang, "Robust GNSS spoofing detection against UE maneuver in a GNSS-5G mmWave hybrid positioning system," *IEEE Sens J*, 2024.

[70] S. Aziz *et al.*, "Anomaly detection in the internet of vehicular networks using explainable neural networks (xNN)," *Mathematics*, vol. 10, no. 8, p. 1267, 2022.

[71] M. Nazeer, A. Alasiry, M. Qayyum, V. K. Madhan, G. Patil, and P. Srilatha, "Enhancing Cyber Security in Autonomous Vehicles: A Hybrid XG Boost-Deep Learning Approach for Intrusion Detection in the CAN Bus," *Journal Européen des Systèmes Automatisés*, vol. 57, no. 5, pp. 1295–1304, Oct. 2024, doi: 10.18280/jesa.570505.

[72] M. Annabi, A. Zeroual, and N. Messai, "Towards zero trust security in connected vehicles: A comprehensive survey," *Comput Secur*, p. 104018, 2024.

[73] A. Selamnia, B. Brik, S. M. Senouci, A. Boualouache, and S. Hossain, "Edge computing-enabled intrusion detection for c-v2x networks using federated learning," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, IEEE, 2022, pp. 2080–2085.

[74] Y. Gong and B.-J. Hu, "A Quantum-Resistant Key Management Scheme Using Blockchain in C-V2X," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[75] N. M. I. Chowdhury and R. Hasan, "How Trustworthy are Over-The-Air (OTA) Updates for Autonomous Vehicles (AV) to Ensure Public Safety?: A Threat Model-based Security Analysis," in *2024 IEEE World Forum on Public Safety Technology (WFPST)*, IEEE, 2024, pp. 87–92.

[76] M. N.-E. Saulaiman *et al*., "Developing SIEM and Log Management for Automotive Network in a Simulated Environment," in *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, IEEE, Sep. 2024, pp. 000239–000244. doi: 10.1109/SISY62279.2024.10737536.

[77] M. Niyomdi and J. Oluoch, "A Comprehensive Security Orchestration, Automation, and Response System (SOAR) for Connected and Autonomous Vehicles (CAVs)," in *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2025, pp. 1–14. doi: 10.1109/ICAIC63015.2025.10849039.

[78] National AI Office (NAIO), "AI-Enhanced Traffic Monitoring and Toll Management," Kuala Lumpur, 2025.

[79] B. J. Asaju, "Standardization and regulation of V2X cybersecurity: analyzing the current landscape, identifying gaps, and proposing frameworks for harmonization," *Advances in Deep Learning Techniques*, vol. 4, no. 1, pp. 33–52, 2024.

[80] E. Farsimadan, L. Moradi, and F. Palmieri, "A Review on Security Challenges in V2X Communications Technology for VANETs," *IEEE Access*, vol. 13, pp. 31069–31094, 2025, doi: 10.1109/ACCESS.2025.3541035.

[81] S.-L. Eljaala, M. Laine, N. Okko, E. Pacil, and J. Rajamäki, "MISP Management Models for Effective Threat Intelligence in Cybersecurity," *European Conference on Cyber Warfare and Security*, vol. 24, no. 1, pp. 884–888, Jun. 2025, doi: 10.34190/eccws.24.1.3536.

[82] I. H. Sarker, H. Janicke, A. Mohsin, A. Gill, and L. Maglaras, "Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects," *ICT Express*, vol. 10, no. 4, pp. 935–958, Aug. 2024, doi: 10.1016/j.icte.2024.05.007.

[83] M. Raciti and G. Bella, "A threat model for soft privacy on smart cars," in *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 2023, pp. 1–10.

[84] Siberkasa, "Cyber Threat Intelligence: In Need Or In Trend," MCMC, 2024.

[85] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, Jul. 2021, doi: 10.3390/s21144759.

[86] Federal Communications Commission, "Dedicated Short-Range Communications (DSRC) Service." [Online]. Available: https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service [Accessed: 07-Jan-2025]