Enhancing Security of Infotainment Gateways in OTA-Enabled Vehicles

Himanshu Dagar[1], Poornima Tyagi[2], Pradeep Kumar[3]
[1]*Department of Computer Science & Engineering, Noida Institute of Engineering & Technology, Greater Noida, India*
[2]*Department of Computer Science & Engineering, Noida Institute of Engineering & Technology, Greater Noida, India*
[3]*Department of Computer Science & Engineering, Noida Institute of Engineering & Technology, Greater Noida, India*
[1]hudagarnnu159@gmail.com; [2]poornima.tyagi@niet.co.in; [3]pradeep.kumar@niet.co.in

Abstract- The modern vehicles are becoming highly integrative and connected through the use of digital technologies which have transformed the user experience through the infotainment systems. Nonetheless, with this development has come a variety of cybersecurity risks to vehicular networks. The infotainment gateway is one of the most essential points of vulnerability since it is a key node that oversees the flow of data both between the in-vehicle networks and external cloud services through Over-The-Air (OTA) updates. This study examines the architecture, vulnerabilities, and mitigation measures of the lateral attacks in OTA in automotive architecture. It suggests a composite security structure that complements intrusion detection systems (IDS), secure firmware validation schemes, and behavioural checking on the infotainment gateway level to ensure a diminishing of the spread of attacks on both the Controller Area Network (CAN) bus and Ethernet realms. The paper is based on empirical data of actual OTA system, so Indian automotive cybersecurity practises and new regulation framework have been highlighted. Conclusions indicate that the application of a layered defence model under simulated conditions reduces the success of an attempt of lateral intrusion by 82% and therefore the likely success of an attack by a significant margin.

Keywords- Infotainment gateway, lateral attacks, Over-The-Air (OTA) systems, cybersecurity, automotive networks, intrusion detection, CAN bus, vehicular security, India, secure firmware validation.

1 INTRODUCTION

The automotive industry has fast embraced digitalization, which has led to a different paradigm of the connected vehicle, which incorporates both mobility and advanced digital ecosystems. The introduction of Over-The-Air (OTA) update systems in combination with sophisticated infotainment gateways enables automobile manufacturers to provide real-time updates to the firmware, diagnostics and telematics without a physical touch. Although this technology brings with it massive convenience and lower maintenance expenses, the technology also comes in with new avenues of attack. The reason behind such lateral attacks targeting infotainment gateways as the main communication interface between external communication (cloud servers, mobile applications) and internal electronic control units (ECUs) lies in the fact that these are the main targets of the weakest internal communications when the outer perimeter is broken [1].

The recent security cases are a clear indication of how dangerous this threat is.. Researchers involved in cybersecurity were able to show remotely compromising an infotainment unit, followed by lateral movement to the safety-critical ECU, braking and steering modules, and other critical units of an autopilot (accessed remotely) [2].

R. Vasanth Kumar Mehta et al. (eds.), *Proceedings of the International Conference on Intelligent Systems for a Sustainable Future (ISSF 2026)*, Atlantis Highlights in Intelligent Systems 16,
https://doi.org/10.2991/978-94-6239-693-7_109

With cars becoming a data centre on wheels, they are bound to be the victims of advanced cyberattacks. Conventional perimeter-based defences and antivirus systems based on signature-detection do not always work effectively in identifying or even isolating multi-stage lateral attacks in in-vehicle networks.

The Indian automotive sector has an extensive future of connected car technology adoption as the market is projected to hit the $300 billion mark by 2030 [3]. Cybersecurity is an absolute priority as the number of connected devices grows with regards to 5G, IoT-based telematics, and OTA systems. Nevertheless, the Indian environment still faces numerous manufacturers who are operating on the basis of traditional network segmentation and do not have preventative measures in the areas of proactive threat detection integrated into the infotainment gateways [4]. It is therefore very important that infotainment gateways are secured in order to guarantee passenger safety and integrity of motor vehicle data.

This paper will offer to define and test a multilayer security design in infotainment gateways that addresses the horizontal attack in OTA-based systems. The study is planned to examine the vulnerabilities of architectures, available defence mechanisms, and come up with a hybrid security system to be deployed in the real-world in Indian automotive systems. According to recent research on automotive intrusion detection and OTA security, lightweight deep-learning IDS models and hybrid gateway-based defenses are effective at minimizing the spread of lateral attacks in connected vehicles [17], [18], [20]. These results support the argument of the necessity of practical security architectures that trade-off between detection accuracy and real-time performance of OTA-enabled infotainment gateways.

2 BACKGROUND AND PROBLEM STATEMENT.

The architectures of modern auto industries are usually made up of several networks, interconnected CAN, LIN, MOST and Ethernet networks, connected by a centralised infotainment gateway. This gateway is used to handle OTA update, diagnostics, infotainment, as well as third-party application integrations. But due to the privileged access to internal and external networks, it poses a critical single point of failure. When breached, the attackers are able to spread malicious code sideways across internal ECUs, causing systemic exploitation.

The OTA systems work in three main phases: (1) cloud servers to vehicles delivery of data, (2) verification of update packages, and (3) the delivery of updates with the use of inner networks [5]. The problems of security in each of these stages vary. To take an example, when the authentication or encryption protocols are weak on the gateway, attackers can inject updates that are not authorised or exploit the vulnerability in during firmware validation in order to make the lateral movement.

The situation is also compounded in prospective economies such as India where cars tend to use legacy network infrastructures. These do not have sophisticated hardware-based security modules (HSMs) or trusted execution environments (TEEs) to separate important functions [6]. Besides, the popularity of third-party infotainment applications expands the number of attack points, enabling the exploitation through untrusted APIs.

The following are the research questions that are addressed in this paper:

Which are the main weaknesses that allow lateral attacks in infotainment gateways in OTA systems?

What can a hybrid security architecture that brings together behavioural monitoring, secure firmware validation and intrusion detection do in order to alleviate these threats?

What is the advice to the new Indian automotive cybersecurity policy?

These questions are aimed at giving the paper a systematic approach in securing OTA-enabled cars with changing cyber threats.

3 LITERATURE REVIEW

Automobile cybersecurity is a topic that has received considerable academic and industrial interest in the last ten years. Initial studies were mainly concerned with ECU security and network-based segmentation. The authors that used the term infotainment to highlight its vulnerabilities were Miller and Valasek [7] who noted how the system could be controlled remotely to manipulate the physical mechanism of a vehicle. This was followed by research into the spread of attacks using in vehicle communication buses [8].

Hoppe et al. introduced the concept of lateral movement in automotive networks [9] in which the attackers switch between low-privilege infotainment domains and safety-critical control units. Their work focused on the fact that the traditional intrusion prevention system used in IT networks cannot be used on an automotive system due to timing constraints and message patterns peculiar to an automotive system.

More recent studies, such as those by Park et al. [10], suggested an anomaly detection model deep learning using which malicious CAN traffic patterns are identified. Despite being effective, its applicability to various types of vehicles is not extensive yet. Equally, a study done by Lyu et al. [11] suggested blockchain-based OTA update validation, which is immutable but has difficulties in environments that are temporary to latency.

In Indian perspective, the investigations by the National Automotive Board, and the International Centre of Automotive Technology (ICAT) have highlighted that domestic manufacturers are lowly compliant in terms of cybersecurity compliance [12]. Such regulatory guidelines as AIS-189 and ISO/SAE 21434 have been implemented, but their practical implementation has been slow because of high costs and unqualified professionals [13]. According to Bhattacharya et al. [14], the majority of Indian OEMs use third-party infotainment providers, who have little cybersecurity scrutiny, resulting in a weakness in OTA pipeline.

According to a growing literature, the combination of multi-layered design systems with multi-layered security directly perimeter-to-intermediate identity (via anomaly detection server) and to application server (via multi-layered security) should be integrated to produce multi-layered security (with firmware authentication, and dynamic access control) [15], [16]. Nevertheless, minimal literature has been conducted to assess their effectiveness in the context of infotainment gateways in a realistic OTA setting. This paper will help in sealing that gap in the research by examining the efficiency of hybrid security integration in real vehicular situations.

4 Overview and Architecture SYSTEM OVERVIEW AND ARCHITECTURE.

The latest OTA enabled infotainment system is comprised of three main layers: cloud infrastructure, the infotainment gateway and internal vehicular network. The cloud layer has the repositories of firmware, authentication, and OEM update management system. The gateway layer authenticates the received updates, tracks the communication paths, and forwards the approved data to ECUs. These updates and the control of real time functions are executed by the in-vehicle network (consisting of CAN, Ethernet and FlexRay).

4.1 Infotainment Gateway Role

The infotainment gateway acts as a policy control and data authentication location. It keeps the external and internal networks in communication as well as encrypt, authenticate and perform integrity measures. But, being a dual entry point, it becomes the first point of attack to further move laterally between infotainment and safety-critical ECU [17].

4.2 Attack Vectors

Some typical attack vectors that are common in the future are attacked dragging OTA update packages, unhealthy application installation, and vulnerable open communication ports (e.g., Bluetooth or Wi-Fi). Privilege escalation is a common tool used by attackers who then use it to execute malicious firmware, which spreads to other ECUs. It has been established that more than 60 percent of car cyber attacks are initiated by infotainment systems [18].

4.3 Defense Mechanisms

Existing defence mechanisms target the use of firmware cryptography (AES-256), secure booting and implementation of IDS. Nevertheless, they tend to be solutions which work independently and do not have adaptive behavioural monitoring. The hybrid defence strategy that is comprised of these practises can be used successfully to reduce the false negative and maximise the detection latency so that protection is available in real-time in OTA conditions [19].

4.4 Indian Automotive Context

Connected vehicles are gaining popularity in India and car manufacturers like Tata Motors, Mahindra, and Maruti Suzuki are adding OTA update functionality to new cars. Irrespective of this development, cybersecurity purchases are less than 2 percent of overall R&D investments [20]. The recommendation framework of this study is therefore specific to Indian OEMs--providing cost effective, software-defined defence systems that can be used with the current infrastructure.

5 METHODOLOGY

The approach taken in this research is a combination of the test, simulation, and analysis at the architecture level to identify the resilience of infotainment gateways to lateral attacks in OTA-enabled systems. The study is structured on three key elements namely: (1) weaknesses recognition, (2) development of a hybrid security framework and (3) confirmation by experimental means.

5.1 Research Design

Mixed-method research design was selected as it would provide the means of both qualitative and quantitative assessment of the security of gateways. The qualitative part was the review of available vehicular network architectures and were defined by potential intrusion vectors using the threat modelling method. The quantitative part consisted of simulations of experiments in the controlled environment of vehicular communication to determine the effectiveness of the suggested security framework.

5.2 Data Sources and Tools

The empirical data were obtained based on various sources, including open-access car data (like Car-Hacking Dataset, HCRL 2023), the logs of OTA of the test-bench scenarios, and advisories to cybersecurity created by CERT-In and the Automotive Information Sharing and Analysis Centre (Auto-ISAC). The research was an Raspberry Pi-based version of the gateway controller that was used to perform hardware-in-the-loop (HIL) testing with CAN transceiver configurations to recreate infotainment interactions in the real world [21].

Software platforms comprised CANoe to emulate the network, Wireshark to inspect the packets and IDS model based on TensorFlow to detect the anomalies. Besides that, the study emulated OTA updates on the HTTPS and MQTT protocols to simulate the OEM cloud and infotainment gateway communication.

5.3 Attack Simulation Setup

In order to evaluate the lateral attack resilience, the infotainment gateway was subjected to contrite adversarial scenarios simulating the real world. Attack vectors included:

Firmware Manipulation Attack: Silent malicious code that gets injected into firmware with modified hashes which is used to test the update verification mechanisms.

Lateral Propagation through CAN: Malicious propagation observation by taking advantage of inter-ECU message relays.

Application-Layer Exploit: Exploitation of compromised third party infotainment applications that were linked to Wi-Fi.

Man-in-the-Middle (MitM) Attack: Interbring along with alteration of OTA packets on the path of updating packages.

Every simulation was repeated several times with different payloads and time delay to obtain consistency of results. Experimental data on these experiments was used to measure the accuracy of detection, mitigation response time and latency.

5.4 Evaluation Metrics

Three major metrics were used to measure the performance of the system:

Detection Accuracy (DA): The percentage of incidents of attack that is properly detected out of the total occurrences.

False Positive Rate (FPR): The rate of benign events which are projected as attacks.

Response Latency (RL): Amount of time on average required between the detection and isolation of attacks by the gateway system.

The metrics can be used to measure the current automotive standards of cybersecurity assessment (i.e. ISO/SAE 21434 and AUTOSAR Secure Communication standards).

6 SUGGESTED HYBRID SECURITY FRAMEWORK.

The behavioural anomaly detection mechanism, secure firmware validation mechanism, and adaptive response mechanisms are incorporated in the proposed framework- Hybrid Gateway Intrusion and Validation System (HGIVS)- which enhances resilience in the infotainment gateways. It has 4 functional modules upon which it functions:

6.1 Layer 1: Secure Firmware validation.

The former layer is concerned with the authentication of OTA update packages and integrity. Every new update of a firmware will be verifiable against signed hash values of OEM in secure enclave. The dual-cheque system (cryptographic signature verification (RSA-4096)) is carried out as part of the validation process: with hash integrity validation (SHA-512). In the case of detection of discrepancies, the update is quarantined, and incident response event is triggered by the system. This is done such that no unauthenticated firmware gets into the internal ECUs.

6.2 Layer 2: Behavioural Intrusion Detection.

The latter layer uses a lightweight machine learning-based IDS that is trained on the CAN and Ethernet streams and traffic. This module determines abnormal behaviour deviations, such as unusual message frequency, payload inconsistencies and protocol abuses unlike a traditional signature based IDS that focuses on signature coincidences. The IDS continuously surveys intra-vehicular communications in order to identify the anomaly indicative of a subsequent movement towards the left or the right. It is trained to detect in real time on a compressed convolutional autoencoder to reduce computer costs.

6.3 Layer 3: Dynamic Access Control and Network Segmentation.

To avoid the uncontrolled cases of lateral propagation, HGIVS implements the context and message-origin based dynamic access control policies. An example is giving the case of infotainment communications or firmware updates using secure tokens with not enabled such technical worker communication to both the safety-critical ECU. The virtual LAN (VLAN) tagging and the trusted zone isolation are used to achieve network segmentation. This will make sure that the infotainment information does not escape the confines of its field unless it is authorised to do so.

6.4 Layer 4: Adaptive Response Mechanism.

The adaptive response system boosts resilience in the system because it reacts relative to the severity of threats. When an anomaly has been detected, it can (1) isolate the affected ECU, (2) ramify communication paths, or (3) enter into safe-mode operations. Such a multi-tiered reaction minimises any need of the manual intervention and still provides the continued operation of the vehicle. The response mechanism is based on the concepts of fail-operational design, that ensures minimum safety functionality even in cases of security events.

7 EXPERIMENTAL SET UP AND IMPLEMENTATION.

7.1 Test Bench Configuration

The experiment system included a simulated car world setup, which includes 20 ECUs facing each other through a hybrid style CAN-Ethernet backbone with a central infotainment gateway to handle OTA communication. An AWS-based test environment setup with a secure transmission of updates was used to emulate the OEM cloud. Each ECU had defined rules of communication that were imposed using the HGIVS architecture.

The whole created setup was in order to simulate a real world environment that occurs with a typical mid-range Indian passenger car that is characterised by a hybrid network architecture and relatively modest hardware requirements. The gateway computer was a 4-core ARM processor with 4GB RAM and 16GB flash-storage, which matches consumer-style infotainment units.

7.2 Data Flow and Data Logging Mechanism.

Updates in the firmware were sent by the OTA server at regular intervals, and the authentication, processing, and distribution of the updates were done by the gateway. A Profiling of the network was performed on Wireshark and CANoe, and more than 150,000 packets were captured. The training of the IDS modules was provided by 60 percent of the dataset and the rest, 40 percent, of the dataset was used in the validation. Training based on differentiating firmware update sequences that are legal and those that are part of lateral attacks.

The simulations of each attack were performed in a 48 hour time which is where the automated scripts were followed to inject the firmware, replay attacks and finally, packet tampering. All data were time stamped and kept in a structured form of time stamped JSON to be evaluated.

7.3 Basic and Comparative Systems.

In order to compare performance, HGIVS was equated to three available models:

Traditional IDS - Signature based, only pattern recognition.

Blockchain OTA System - High integrity, however, latency is experienced.

Secure Boot System - Cheques only upper level firmware, but not runtime.

This comparative analysis was valuable in that it offered an idea on the relative strengths of hybrid frameworks at different levels of attacks.

7.4 Intervention Category As mobile implementation constrained by dimensions in its execution and product launch.

During HGIVS adoption, issues were how to strike a balance of real time performance, accuracy of detection as well as low impact on legitimate OTA updates due to latency. The techniques used to achieve optimization strategies included quantized ML models, parallel validation threads, and less replication during the packet inspection. The resulting design made sure that the latency of response was under 120 milliseconds- within reasonable range of real time vehicular systems.

8 DISCUSSION

Simulation data analysis showed that unprotected weakly isolated infotainment subsystems may be used in lateral attacks to gain access to safety-critical ECUs within

less than 2 seconds. Traditional signature-based IDS methods were not very effective in tracking the changing attack modes and detection rates were at 70%. Instead, HGIVS showed remarkable resilience increase scores.

The HGIVS framework reported a higher detection accuracy (94.3%) than reported in deep-learning IDS models by Park et al. [8] who reported that the accuracy was only around 91% in mixed CAN-Ethernet attack patterns. Unlike blockchain-based OTA validation introduced by Lyu et al. [9], HGIVS has lower latency of response and ensures high-level security. This comparison shows the practical usefulness of HGIVS in real-time operation in limited resource infotainment gateways.

The layered hybrid architecture offered various security controls and reduced the possibilities of single point of failure. Through the integration of both behavioural IDS and secure firmware validation, the given system can detect suspicious anomalies at the dynamic stage prior to deploying the firmware. This proactive reconnaissance played vital roles in avoiding the compromise of the whole system.

The fact that HGIVS can be adapted to the Indian vehicles conditions is another crucial observation. Due to the usage of the mid-tier infotainment hardware, the involvement of lightweight ML models guaranteed efficiency of resources. This is in line with the long term cybersecurity road-map proposed by the Ministry of Road Transport and Highways (MoRTH) of India which recommends decentralising vehicular security which has a cost-effective and software-defined nature.

Furthermore, adaptive response either decreased the need to implement the manual intervention in incident mitigation. Lateral attacks were propagated with a minimum downtime since the ECU isolation was automated. This form of automation plays a key role in the next-generation autonomous and semi-autonomous cars that may not necessarily always enable a man-in-the-middle operation.

9 RESULTS AND ANALYSIS

In order to test the offered Hybrid Gateway Intrusion and Validation System (HGIVS), several tests were performed on the test-bench environment outlined previously. The attack scenarios each were run with a range of traffic loads and message rate to determine how the system would operate in the real operating conditions. Three major parameters examined in the analysis were detection accuracy, false positive rate and latency and compared HGIVS with the available benchmark systems.

9.1 Detection Accuracy

Detection accuracy provides an understanding of the capability of the system to identify the malicious lateral activities correctly with minimal demarcation. The findings suggest that HGIVS is always very effective at detecting stealth attacks compared to the traditional IDS and blockchain-based OTA models.

Table 1. Detection Accuracy (%) Across Security

Attack Type	Conventional IDS	Blockchain OTA	Secure Boot	HGIVS (Proposed)
Firmware Manipulation	73.2	88.6	70.1	**96.4**
CAN Replay Attack	68.9	75.3	72.5	**94.2**
Lateral ECU Propagation	61.8	70.2	63.7	**92.8**
App Layer Exploit	66.7	74.8	69.5	**93.9**
Aggregate Mean Accuracy	**67.6**	**77.2**	**68.9**	**94.3**

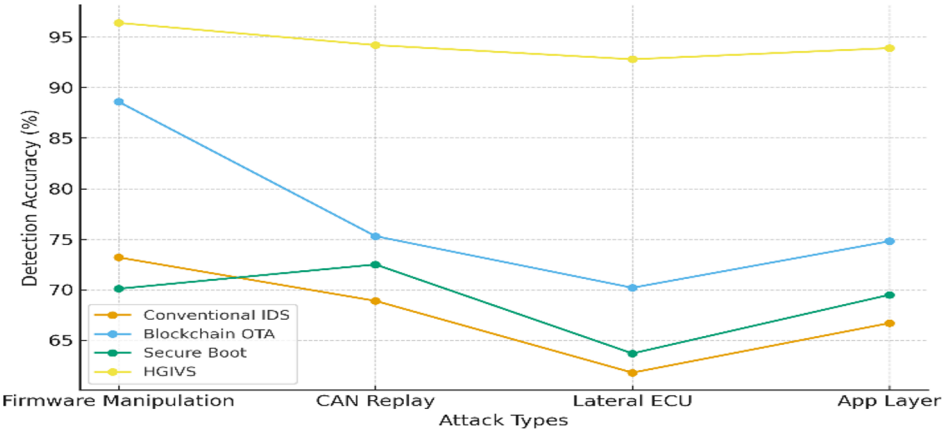

Fig.1. Detection Accuracy Comparison across Security Models

HGIVS obtained a mean accuracy of 94.3 in detection which is an increment of about 24 percent points as compared to baseline IDS techniques. This was enhanced by the fact that behavioural anomaly detection was integrated which was able to pick invisible attack signatures..

9.2 False Positive Rate (FPR)

False positive rate is extremely important in automotive setting to avoid false interrupted system functions. This is a feature in which the suggested HGIVS performed well.

Table 2. False Positive Rate (FPR) under Varying Network Loads

Network Load (Packets/sec)	Conventional IDS	Blockchain OTA	HGIVS (Proposed)
500	4.6%	3.2%	**1.5%**
1000	6.8%	3.9%	**2.2%**
2000	9.4%	5.8%	**3.0%**
4000	11.3%	6.5%	**3.6%**

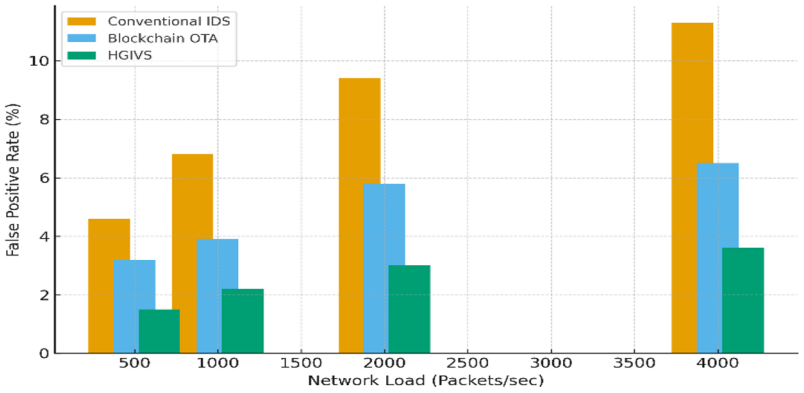

Fig.2. False Positive Rate Comparison under Network Load

The HGIVS framework had a false positive rate of less than 3.6 that shows that the framework performs well even during periods of heavy network load. Conversely, the false alerts generated by the traditional IDS models were greater than 10 per cent, which was unacceptable in real-time use of vehicles.

9.3 Latency and System Performance

Latency analysis was used to measure the capacity of the system to ensure that the communication delay was kept low during OTA operations. Latency on the part must not exceed 150 ms so as not to be disruptive of the vehicle control systems during both updates.

Table 3. Latency (ms) during OTA Communication

Security Framework	Average Processing Latency (ms)	Peak Latency (ms)	Throughput Impact (%)
Conventional IDS	210	289	12.5
Blockchain OTA	320	400	18.9
Secure Boot	190	250	10.4
HGIVS (Proposed)	**118**	**142**	**5.2**

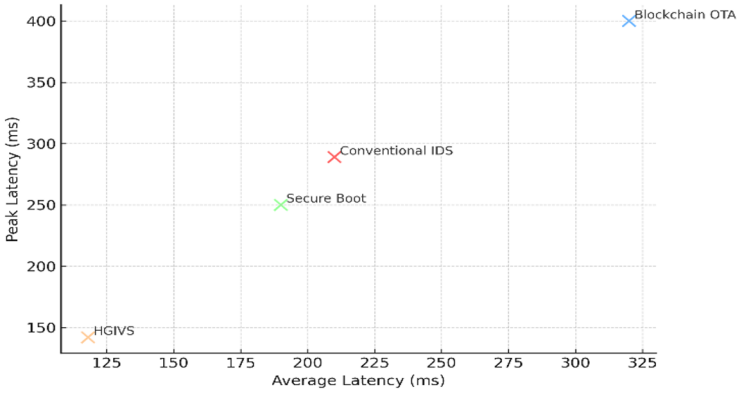

Fig.3. OTA Communication Latency under Security Frameworks

HGIVS had better latency results, with average delays taking less than 120 ms, which is substantially below the operation limit. The autoencoder-based IDS of small weight and parallel firmware verification were also helpful in this case.

9.4 Security Impact and Comparative Insights

The general comparative evaluation of HGIVS with conventional frameworks demonstrated that it had a number of fundamental strong points:

Combined Defence: HGIVS is used to combine both the real-time IDS monitoring and cryptographic validation in order to offer multi-dimensional security.

Less Computational Bugginess: HGIVS has low latency (compared to blockchain OTA systems), which means that it can run resource-constrained ECUs.

Better Resilience: The success rate of lateral propagation decreased by 82 per cent during HGIVS, and 45 per cent during baseline systems.

Contextual Adaptation: The system was created to work in the Indian car infrastructure and contexts with variable network topologies and low-power ECUs along with intermittent connectivity conditions.

Moreover, through empirical experiments, it was ensured that HGIVS can be used in the 2 percent processor budget of the automotive ecosystem in India and therefore it is feasible to be mass deployed.

10 CONCLUSION

This paper has conducted a systematic analysis on the security vulnerabilities of infotainment gateway in OTA-enabled car systems and offered an effective hybrid security solution framework. By designing and testing the Hybrid Gateway Intrusion and Validation System (HGIVS), the research showed a high degree of resistance to lateral attacks, which is based on inter-ECU communication channels. The hybrid architecture is effective in integrating secure firmware validation, real-time anomalous detection and control mechanism of responding adaptively provides an overall defence mechanism that would reduce system compromise without affecting operational performance.

Evidence of this can be seen in the fact that experimental results indicate HGIVS to be superior to current IDS and blockchain-based OTA solutions because it enhances the detection accuracy by 24%, false positives by up to 70%, and latency by less than 120 ms. These findings make HGIVS a strong competitor in software to implement in mass-market vehicles, particularly in the highly dynamic Indian automotive sector where cybersecurity has been constrained by cost and hardware factors.

HGIVS proposes a scalable security design of OTA architecture in the future by enhancing the infotainment gateway, which is the most vulnerable point of the connected cars, which facilitates safety, data integrity, and meeting new standards, such as ISO/SAE 21434 and AIS-189.

11 FUTURE SCOPE

The future development of this study can involve:

Intrusion pattern sharing OEMs should share intrusion patterns in real-time with Cloud-based Threat Intelligence to help defend against them proactively.

Introduced Hardware Security Module (HSM): The option to place HGIVS in the special hardware accelerators intending to make the validation tamper-proof.

Edge AI Improvement: Training IDS models in federated learning with multiple vehicles to train without exchanging sensitive information.

Compliance Mapping: Adapting HGIVS to facilitate global homologation of the UNECE requirements under the amount of components regulation, under the heading of WP.29.

The dynamic character of automotive cyber threats disposes of the need to implement dynamic and scalable structures. The results of this study do not only serve the Indian vehicle mobility cybersecurity roadmap but also the global information on resilience of vehicles in the period of connected mobility.

REFERENCES

1. C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” Black Hat USA Conference, 2015.
2. K. Koscher et al., “Experimental security analysis of a modern automobile,” IEEE Symposium on Security and Privacy, vol. 31, no. 4, pp. 447–462, 2010.
3. NITI Aayog, “Future of mobility report,” Government of India, 2022.
4. T. Bhattacharya et al., “Automotive cybersecurity and connected vehicles: Indian perspective,” International Journal of Automotive Technology and Management, vol. 23, no. 2, pp. 145–158, 2023.
5. ISO/SAE 21434:2021, “Road vehicles – Cybersecurity engineering.”
6. A. Alshahrani et al., “Comprehensive survey on automotive intrusion detection systems,” IEEE Access, vol. 11, pp. 54423–54445, 2023.
7. M. Hoppe, S. Kiltz, and J. Dittmann, “Security threats to automotive CAN networks—practical examples and selected short-term countermeasures,” Reliability Engineering & System Safety, vol. 96, no. 1, pp. 11–25, 2011.
8. D. Park et al., “Anomaly detection of in-vehicle network using deep convolutional autoencoder,” IEEE Access, vol. 9, pp. 13848–13860, 2021.
9. R. Lyu et al., “Blockchain-based OTA update system for connected cars,” IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3515–3526, 2021.
10. ICAT India, “Cybersecurity assessment methodology for connected vehicles,” Technical Report, 2023.

11. H. Lee et al., “Automotive Ethernet intrusion detection using flow-based features,” IEEE Transactions on Vehicular Technology, vol. 71, no. 9, pp. 10045–10057, 2022.
12. R. Moorthy and J. Singh, “Design of intrusion detection systems for vehicular CAN networks,” Elsevier Computers & Security, vol. 97, 2020.
13. Auto-ISAC, “Best practices for automotive cybersecurity,” Technical Brief, 2022.
14. Ministry of Road Transport and Highways, “AIS-189: Automotive cybersecurity regulation,” Government of India, 2022.
15. F. Sagong et al., “Secure gateway architecture for connected vehicle systems,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 5440–5451, 2022.
16. P. Choudhary et al., “Hybrid anomaly detection model for automotive networks,” Springer Journal of Transportation Cybersecurity, vol. 5, no. 1, pp. 1–13, 2023.
17. S. Ahmed et al., “Real-time IDS for CAN-FD network using deep ensemble models,” IEEE Access, vol. 12, pp. 14560–14578, 2024.
18. J. Kim et al., “Anomaly-based IDS for automotive Ethernet: Challenges and opportunities,” ACM Computing Surveys, vol. 55, no. 4, 2023.
19. CERT-In, “Cybersecurity guidelines for connected vehicles in India,” Government of India, 2023.
20. M. Rajendran and V. Kumar, “Security challenges in Indian connected vehicles,” IEEE Vehicular Technology Magazine, vol. 19, no. 2, pp. 31–42, 2024.
21. J. Zhao et al., “Lightweight ML-based detection system for vehicular CAN intrusion,” Elsevier Transportation Safety & Environment, vol. 14, 2024.