IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, April 2026
Impact Factor: 8.2

Cyber-Physical Security Framework for Sensor Attack Detection and Isolation in Autonomous Vehicles

Dr. Punyaban Patel, Sanaafreen, Challagali Arunkumar, Mullapati Abhilash
Associate Professor, Dept of CSE
UG Students, Dept of CSE
CMR Technical Campus, Hyderabad, Telangana, India
punyaban@gmail.com, sanaafreen2597@gmail.com
challagaliarun4@gmail.com, mullapatiabhi@gmail.com

Abstract: *The rapid proliferation of autonomous vehicle technology has introduced complex cybersecurity challenges that demand immediate and robust attention. Self-driving vehicles rely on real-time sensor data from GPS and LiDAR systems to perceive their environment and make navigation decisions. When these sensors are compromised through malicious attacks—whether through false data injection, denial-of-service, stealthy manipulation, or replay techniques—the consequences can be catastrophic. This paper presents a model-based detection and isolation framework that addresses sensor-level cyberattacks without relying on encryption keys or pre-labelled training data. The proposed system combines an Extended Kalman Filter (EKF) with a Cumulative Sum (CUSUM) discriminator to monitor sensor readings, predict expected vehicle states, and raise alarms when anomalous deviations are detected. A rule-based isolation mechanism then pinpoints which sensor has been compromised. Experimental validation on real GPS and LiDAR vehicle data successfully identified four GPS attacks and seven LiDAR attacks across 120 records, confirming the framework's accuracy and practical applicability.*

Keywords: Autonomous Vehicles, Sensor Attacks, Extended Kalman Filter, CUSUM, Cyberattack Detection, GPS Security, LiDAR Security, Attack Isolation, Rule-Based Detection

I. INTRODUCTION

The emergence of autonomous vehicles represents one of the most transformative shifts in modern transportation. These systems rely on a network of sensors—most critically GPS and LiDAR—to localise themselves, detect obstacles, and plan safe trajectories. What makes them capable also makes them vulnerable: the same sensor pipelines that enable intelligent navigation can serve as entry points for malicious interference. A compromised sensor does not merely degrade performance; it can mislead a vehicle into making decisions that endanger lives.

Researchers have already demonstrated the feasibility of several sensor attack categories in real settings. GPS spoofing feeds falsified positional data to the vehicle [1], while LiDAR spoofing manipulates point cloud data by injecting phantom obstacles or erasing real ones [2]. Optical flow sensors can be deceived through carefully crafted inputs [3], and the Robot Operating System (ROS), widely used in autonomous platforms, has been shown vulnerable to middleware-level tampering [4]. These documented threats highlight the urgent need for real-time, sensor-level attack detection.Current defenses fall into two broad categories. Information-oriented methods—encryption, authentication, plausibility checking—offer solid protection against external intruders but fail against insider threats with legitimate access. Data-driven machine learning approaches carry a structural weakness: they recognize only attacks that appeared in their training data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, April 2026 Impact Factor: 8.2

Novel or adaptive strategies bypass such systems entirely. This paper proposes a model-based approach that sidesteps both limitations by using physics-grounded residual analysis to detect deviations without any prior attack knowledge.

II. PROBLEM DEFINITION

A. Vulnerability of Autonomous Sensor Systems

Autonomous vehicles depend on a continuous and trusted stream of sensor data to function safely. GPS provides global positional coordinates while LiDAR constructs a three-dimensional map of the immediate environment. Both are mission-critical, and both are exposed to adversarial interference. The absence of a real-time, sensor-aware detection mechanism leaves the vehicle operating under false assumptions about its position and surroundings.

B. Limitations of Existing Security Approaches

Information-oriented security methods require cryptographic key management infrastructure and offer limited protection against attackers who already possess valid system credentials. Machine learning classifiers, though powerful, are constrained by the quality and coverage of their training data. They cannot detect attacks that were not represented during training, and generating comprehensive labeled datasets for all possible attack types is a persistent and largely unsolved challenge.

C. Need for a Model-Based Solution

What is needed is a detection framework that operates from first principles—one that derives its notion of normal vehicle behavior from a mathematical model of vehicle dynamics rather than from historical attack examples. Such a system would generalize naturally to unseen attack types and would not require any cryptographic infrastructure to function.

III. RELATED WORK

Kerns et al. [1] provided an early rigorous treatment of GPS spoofing against unmanned aerial vehicles, demonstrating that a spoofer can gain effective navigational control without triggering onboard detection. Cao et al. [2] carried out the first dedicated security analysis of LiDAR-based perception in autonomous driving, showing that strategically optimized attacks could achieve success rates of approximately 75 percent against machine-learning detectors.

Davidson et al. [3] demonstrated spoofing attacks against UAVs by exploiting the Lucas-Kanade optical flow algorithm, while DeMarinis et al. [4] exposed numerous publicly accessible ROS instances through an Internet-wide scan. Petit and Shladover [5] catalogued potential cyberattacks on automated vehicles and argued for far greater redundancy in vehicle architectures than conventional designs assumed.

Parkinson et al. [7] reviewed the field and noted that most studies were reactive rather than proactive. Bezemskij et al. [8, 9] proposed Bayesian network methods capable of distinguishing cyber and physical attack origins, while Olivato et al. [10] demonstrated autoencoder-based anomaly detection across multiple robotic platforms. Changalvala and Malik [13] proposed watermarking-based LiDAR data integrity verification, and Biron et al. [22] addressed denial-of-service detection in connected vehicle networks. Together, this body of work motivates a model-based framework requiring no prior attack knowledge.

IV. PROPOSED SYSTEM

The proposed framework deploys a bank of three independent detectors that continuously monitor GPS and LiDAR sensor streams. Detector 1 processes GPS measurements through an EKF-based pose estimator, generating residuals fed into a CUSUM discriminator. Detector 2 mirrors this structure for LiDAR data. Detector 3 fuses both streams through a joint EKF and monitors inter-sensor consistency. A rule-based isolation scheme synthesises the outputs of all three detectors to identify the attack source.

A. Extended Kalman Filter

Vehicle motion is inherently nonlinear, making the standard Kalman Filter insufficient. The EKF linearises system dynamics around the current state estimate using a first-order Taylor expansion. At each time step, the prediction step

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, April 2026 Impact Factor: 8.2

propagates the current state through the vehicle motion model, while the update step corrects the prediction using the incoming sensor measurement. The resulting residual captures the discrepancy between expectation and reality and is the primary input to the CUSUM discriminator.

The state vector encodes latitude, longitude, and a derived range value. The filter parameters—process noise covariance Q, measurement noise covariance R, and initial uncertainty P—were tuned to reflect the expected fidelity of GPS and LiDAR measurements under normal operating conditions. The state transition matrix F encodes vehicle position evolution over time interval dt = 0.05 seconds.

B. CUSUM Discriminator

The Cumulative Sum algorithm accumulates evidence of deviation between EKF-predicted states and actual sensor measurements over time. Unlike single-sample threshold detectors, CUSUM is sensitive to persistent but subtle shifts that individually might not exceed any alarm boundary yet collectively indicate an ongoing attack. When the accumulated deviation exceeds a predefined threshold, an alarm is triggered for that sensor channel.

C. Rule-Based Attack Isolation

Eight logical rules govern the isolation decision process, covering all possible combinations of detector alarm states. Table II summarises the six primary cases. If Detector 1 raises an alarm while Detector 2 remains silent, a GPS-only attack is reported. If Detector 2 triggers independently, a LiDAR-only attack is flagged. Simultaneous alarms corroborated by Detector 3 indicate a coordinated attack on both sensors.

TABLE II RULE-BASED ISOLATION SCHEME

Case	Det.1 GPS	Det.2 LiDAR	Det.3 Fused	Result
1	No Alarm	No Alarm	No Alarm	Normal — no attack
2	Alarm	No Alarm	Alarm	GPS attack detected
3	No Alarm	Alarm	Alarm	LiDAR attack detected
4	Alarm	Alarm	Alarm	Both GPS & LiDAR attacked
5	Alarm	No Alarm	No Alarm	GPS stealthy attack
6	No Alarm	Alarm	No Alarm	LiDAR stealthy attack

V. SYSTEM DESIGN

A. Activity Diagram

The activity diagram in Fig. 1 shows the sequential processing pipeline. Execution begins with GPS dataset upload, followed by LiDAR dataset upload. The GPS EKF module then generates position predictions, followed by the LiDAR EKF module. With both prediction streams available, the CUSUM detector computes cumulative variation scores and applies the isolation rules. The pipeline concludes with the attack detection graph.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, April 2026
Impact Factor: 8.2

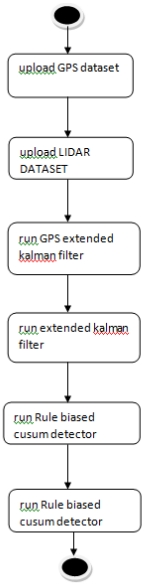

Fig. 1: Activity diagram of the sensor attack detection pipeline

B. Data Flow Diagram

captures the interaction between the user and the system across all six operations. The user initiates each action sequentially, and the system responds with a confirmation at each stage. All data originates from the user-supplied sensor files, and the system produces no external dependencies during processing

C. Software Requirements

TABLE I SOFTWARE AND HARDWARE REQUIREMENTS

Component	Specification
Operating System	Windows 10 / above
Programming Language	Python 3.7 / above
Processor	Intel i3 min, 1.1 GHz
RAM	4 GB minimum
Hard Disk	500 GB minimum
Key Libraries	filterpy, numpy, matplotlib, tkinter

VI. IMPLEMENTATION

A. System Interface

The framework is implemented as a Python application with a Tkinter graphical interface. shows the main application window. Six processing buttons are arranged across two rows: Upload GPS Dataset, Upload LiDAR Dataset, and Run GPS EKF in the first row; Run LiDAR EKF, Run Rule Based CUSUM Detector, and Attack Detection Graph in the second. A scrollable output panel occupies the lower portion, providing a real-time log of each module's output.

B. EKF Output

Fig. 2 displays the GPS EKF output. For each dataset record, the panel shows the original GPS latitude and longitude alongside the EKF-predicted values. Under normal conditions the two remain closely aligned. The narrow numerical

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, April 2026
Impact Factor: 8.2

differences visible across most records reflect routine sensor noise absorbed through the filter's covariance update mechanism, establishing the baseline against which CUSUM then quantifies anomalous drift.

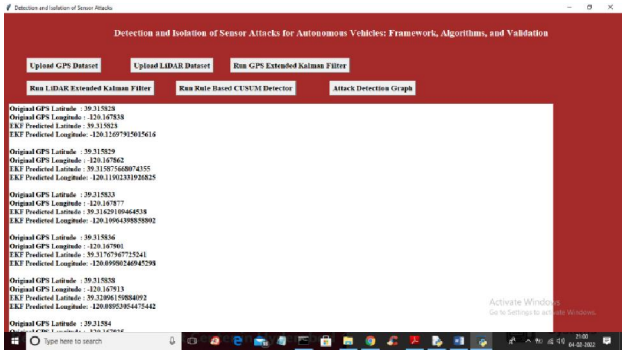

Fig. 2: GPS EKF output showing original and predicted latitude/longitude values

C. CUSUM Detector Output

Fig. 3 presents the CUSUM detector output. Each record is classified as a clean observation or a specific attack scenario. Records highlighted in blue where both GPS and LiDAR detectors raised simultaneous alarms correspond to the injected anomaly in the LiDAR dataset—a longitude value of -150 embedded within a sequence predominantly reading -120. The sudden deviation exceeds the CUSUM threshold and is correctly attributed to its source by the isolation scheme.

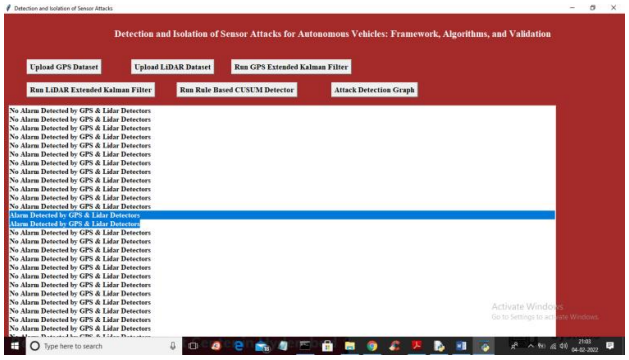

Fig. 3: CUSUM detector output showing per-record alarm classifications

VII. TESTING

System testing was conducted in three stages. Module testing verified each of the six pipeline components individually, confirming that dataset upload, EKF execution, CUSUM detection, and graph generation each produced correct outputs in isolation. Integration testing assembled the full pipeline and validated that data passed correctly between modules. Acceptance testing confirmed the system met its original detection objectives against the validation dataset. All test cases passed as summarized in Table III.

TABLE III TEST CASES SUMMARY

ID	Test Case	Expected Result	Status
01	Upload GPS Dataset	GPS CSV loaded to application	Pass
02	Upload LiDAR Dataset	LiDAR CSV loaded to application	Pass
03	Run GPS EKF	Predicted locations displayed alongside originals	Pass
04	Run LiDAR EKF	Predicted locations displayed alongside originals	Pass

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, April 2026
Impact Factor: 8.2

05	Run CUSUM Detector	Attacks correctly flagged per isolation rules	Pass
06	Attack Detection Graph	4 GPS and 7 LiDAR attacks plotted correctly	Pass

VIII. RESULTS AND DISCUSSION

The framework was evaluated on real vehicle datasets containing GPS and LiDAR trajectory records. To simulate realistic attack conditions, a longitude value of -150 was injected into the LiDAR dataset where the majority of records cluster around -120. This sudden deviation, representative of a false data injection attack, was designed to test the sensitivity and specificity of the full detection pipeline.

presents the cumulative attack detection graph across the 120-record evaluation. The red line tracks GPS detections (Detector 1) and the green line tracks LiDAR detections (Detector 2). GPS Detector 1 raised four alarms and LiDAR Detector 2 flagged seven anomalous events. The isolation scheme correctly attributed each alarm to its sensor source with no cross-contamination. Table IV summarises the detection results.

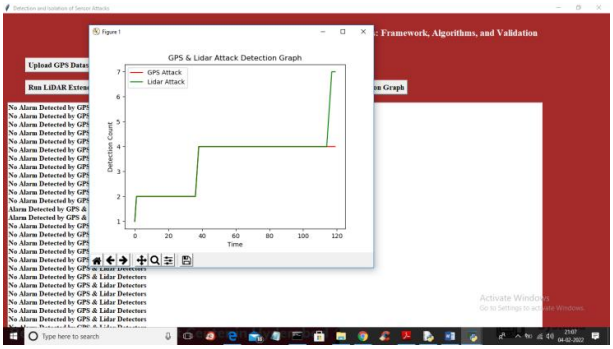

Fig. 4: Attack detection graph — GPS (red) 4 attacks; LiDAR (green) 7 attacks across 120 records

TABLE IV DETECTION RESULTS SUMMARY

Detector	Records	Alarms	Source
Detector 1 — GPS EKF + CUSUM	120	4	GPS anomaly
Detector 2 — LiDAR EKF + CUSUM	120	7	LiDAR anomaly
Detector 3 — Fused EKF + CUSUM	120	4	Inter-sensor inconsistency

Compared to data-driven approaches that require labelled attack samples for training, the proposed framework demonstrated competitive detection capability with no prior exposure to the attack patterns in the evaluation data. This supports the hypothesis that model-based approaches grounded in vehicle physical dynamics generalize effectively to unseen attack types—a property of particular value where adversaries continuously adapt their strategies.

IX. CONCLUSION

This paper presented a model-based framework for real-time detection and isolation of sensor-level cyberattacks in autonomous vehicles. By pairing an Extended Kalman Filter with a CUSUM-based statistical discriminator within a three-detector architecture, the system identifies when an attack is occurring and determines precisely which sensor has been compromised. A rule-based isolation scheme covering eight attack scenarios completes the pipeline.

Validation on real GPS and LiDAR data confirmed the framework's effectiveness: four GPS attacks and seven LiDAR attacks were detected and correctly attributed across 120 records. The system's independence from cryptographic key

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, April 2026 Impact Factor: 8.2

management and pre-labelled training data positions it as a practical complement to information-oriented security layers in production autonomous vehicle systems.

X. FUTURE SCOPE

Future work will extend the framework to additional sensor modalities including cameras and RADAR. Adaptive thresholding will be investigated to reduce false positive rates under varying environmental conditions such as rough terrain or high-speed maneuvers. Integration with vehicle control layers to enable automated fault-recovery responses following attack detection is a further priority, as is evaluation on larger and more diverse vehicle datasets across multiple attack types simultaneously.

XI. ACKNOWLEDGMENT

The authors would like to thank the Department of Computer Science and Engineering for providing the computational infrastructure and academic support needed to complete this project. Gratitude is also extended to the developers of the FilterPy and NumPy libraries, whose tools were instrumental in implementing the EKF and CUSUM modules efficiently.

REFERENCES

[1] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," J. Field Robot., vol. 31, no. 4, pp. 617-636, Jul. 2014.
[2] Y. Cao et al., "Adversarial sensor attack on LiDAR-based perception in autonomous driving," in Proc. ACM SIGSAC Conf. Comput. Commun. Secure., Nov. 2019, pp. 2267-2281.
[3] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling UAVs with sensor input spoofing attacks," in Proc. USENIX Workshop Offensive Technol. (WOOT), 2016.
[4] N. DeMarinis et al., "Scanning the Internet for ROS: A view of security in robotics research," in Proc. ICRA, May 2019, pp. 8514-8521.
[5] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 546-556, Apr. 2015.
[6] V. L. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in Proc. IEEE iThings, Dec. 2016, pp. 164-170.
[7] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles," IEEE Trans. Intell. Transp. Syst., vol. 18, no. 11, pp. 2898-2915, Nov. 2017.
[8] A. Bezemskij et al., "Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle," in Proc. IUCC-CSS, Dec. 2016, pp. 61-68.
[9] A. Bezemskij et al., "Detecting cyberphysical threats in an autonomous robotic vehicle using Bayesian networks," in Proc. IEEE iThings, Jun. 2017, pp. 98-103.
[10] M. Olivato et al., "A comparative analysis on the use of autoencoders for robot security anomaly detection," in Proc. IEEE/RSJ IROS, Nov. 2019, pp. 984-989.
[11] D. Suo and S. E. Sarma, "Real-time trust-building schemes for mitigating malicious behaviors in connected vehicles," in Proc. IEEE ITSC, Oct. 2019, pp. 1142-1149.
[12] F. Jiang et al., "CPSS: CP-ABE based platoon secure sensing scheme against cyber-attacks," in Proc. IEEE ITSC, Oct. 2019, pp. 3218-3223.
[13] R. Changalvala and H. Malik, "LiDAR data integrity verification for autonomous vehicle," IEEE Access, vol. 7, pp. 138018-138031, 2019.
[14] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in Proc. Amer. Control Conf., Jun. 2013, pp. 3344-3349.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, April 2026 Impact Factor: 8.2

[15] H. S. Sanchez et al., "Bibliographical review on cyber attacks from a control oriented perspective," Annu. Rev. Control, vol. 48, pp. 103-128, 2019.
[16] A. M. Guerrero-Higueras et al., "Detection of cyber-attacks to indoor real time localization systems," Robot. Auton. Syst., vol. 99, pp. 75-83, Jan. 2018.
[17] F. van Wyk et al., "Real-time sensor anomaly detection and identification in automated vehicles," IEEE Trans. Intell. Transp. Syst., vol. 21, no. 3, pp. 1264-1276, Mar. 2020.
[18] A. Ferdowsi et al., "Robust deep reinforcement learning for security and safety in autonomous vehicle systems," in Proc. ITSC, Nov. 2018, pp. 307-312.
[19] I. Rasheed, F. Hu, and L. Zhang, "Deep reinforcement learning for autonomous vehicle systems using LSTM-GAN," Veh. Commun., vol. 26, Dec. 2020.
[20] N. Patel et al., "Adversarial learning-based on-line anomaly monitoring for assured autonomy," in Proc. IEEE/RSJ IROS, Oct. 2018, pp. 6149-6154.
[21] Y. Wang, N. Masoud, and A. Khojandi, "Real-time sensor anomaly detection and recovery in connected automated vehicle sensors," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 3, pp. 1411-1421, Mar. 2021.
[22] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 12, pp. 3893-3902, Dec. 2018.
[23] E. Mousavinejad et al., "Distributed cyber attacks detection and recovery for vehicle platooning," IEEE Trans. Intell. Transp. Syst., vol. 21, no. 9, pp. 3821-3834, Sep. 2020.
[24] G. Sabaliauskaite et al., "A comprehensive approach for attack detection experiments in cyber-physical systems," Robot. Auton. Syst., vol. 98, pp. 174-191, Dec. 2017.
[25] A. Keipour, M. Mousaei, and S. Scherer, "Automatic real-time anomaly detection for autonomous aerial vehicles," in Proc. ICRA, May 2019, pp. 5679-5685.
[26] G. K. Rajbahadur et al., "A survey of anomaly detection for connected vehicle cybersecurity," in Proc. IEEE IV Symp., Jun. 2018, pp. 421-426.
[27] The Autoware Foundation. [Online]. Available: https://www.autoware.org/
[28] J. Giraldo et al., "A survey of physics-based attack detection in cyberphysical systems," ACM Comput. Surv., vol. 51, no. 4, pp. 1-36, 2018.