APPENDICES:

A Systematic Review and Meta-analysis Survey of IDS/IPS Techniques for CAN and Vehicular Networks

Younis Abdo Mohammed Nasser Al Shojaa[1*], Khaled Al Soufy[2]

[1]Information Technology Department, Faculty of Engineering and Information Technology, Al-Qalam University, Ibb, Yemen.

[2]Electrical Engineering Department, Faculty of Engineering, Ibb University, Ibb, Yemen.

***Corresponding author:** Email younis.alshogaa@quni.edu.ye

APPENDIX A

REPRESENTATIVE MACHINE LEARNING (ML) STUDIES

TABLE II. REPRESENTATIVE MACHINE LEARNING (ML) STUDIES

Authors (Year)	Technique	Dataset	Strengths	Weaknesses	Result
Kalkan and Sahingoz [1]	ML IDS	Custom	Multi-model support	Complex deployment	95%
Alfardus and Rawat [2]	RF	Car-Hacking	Effective for known	Poor generalization	95%
			attacks		
Al-Janabi et al. [3]	SVM	KDD Cup	Performs well on	High false positives	90%
			unknown attacks		
Panigrahi et al. [4]	RF, SVM, etc.	NSL-KDD	RF achieves highest	Limited generalization	99%
			accuracy		
Micale et al. [5]	Context-aware	CAN	Context-based detection	Limited dataset size	>94%
	ML				
Alalwany and Mahgoub [6]	Delay ML	CAN	Novel delay-based	Simulated dataset	95%
			features		
Rajapaksha et al. [7]	Context-aware	J1939	Detects multiple attack	Simulated environment	>97%
	IDS		types		
Nagarajan et al. [8]	Robust ML	IoV	Secure and stable	Requires larger testing	>96%
Kumar and Das [9]	Supervised ML	CAV	Real-time performance	Limited unseen attack	97%
				coverage	
Ajibuwa et al. [10]	ML IDS	AVs	Detects AV-specific	Small dataset	95%
			threats		
Shahriar et al. [11]	CAN IDS	CAN	Practical design	Limited validation	93%
Anthony et al. [12]	Non-tree ML	AVs	Explores rare algorithms	Scalability concerns	94%
Alalwany and Mahgoub [13]	Ensemble ML	CAN	Boosts overall accuracy	Costly training phase	96%
Huang et al. [14]	Anomaly ML	Vehicle	Lightweight solution	Limited data diversity	95%
El-Gayar et al. [15]	Ensemble IDS	Vehicular	Collaborative	Complex deployment	96%
			decision-making		
Samir et al. [16]	ML IDS	CAN	Good accuracy	Restricted to CAN	95%
Ahmed et al. [17]	ML IDS	IoV	Resistant to DoS attacks	Limited evaluation	96%
Ahmad et al. [18]	ML IDS	CAV	Enhanced security	Generic evaluation	95%
			features		
Alemerien et al. [19]	Optimized ML	IoV	Optimized performance	Limited dataset	95%
Kousar et al. [20]	Lightweight ML	CAN	Fast execution	Limited testing	94%
Musa et al. [21]	ML IDS	IoAV	Handles class imbalance	Narrow scope	94%
Adu-Kyere et al. [22]	Custom IDS	Vehicle	Real-time performance	Scalability issues	93%
Abrar et al. [23]	GPS-IDS	GPS spoofing	Tailored GPS attack	Narrow focus	High
			detection		
Al-Kadri [24]	CAN-MIRGU	CAN	High detection rate	Limited to CAN	98.7%
Wasicek et al. [25]	Context-aware	CAN	High accuracy	Limited diversity	97%
	AI				
Ossen [26]	ASIC RF IDS	CAN	Real-time hardware	Hardware complexity	97%

APPENDIX B

REPRESENTATIVE DEEP LEARNING (DL) STUDIES

TABLE III. REPRESENTATIVE DEEP LEARNING (DL) STUDIES

Authors (Year)	Technique	Dataset	Strengths	Weaknesses	Result
Liu et al. [27]	RNN	Custom	Sequential modeling	Slow training	95%
Faker and Dogdu [28]	DL Ensemble	CICIDS2017	Robust to varied attacks	High computational cost	97%
			complex scenarios		
Kumar and Sharma [29]	CNN	NSL-KDD,	Learns hierarchical	High data requirements	99%
		CICIDS2017	features		
Raza et al. [30]	Federated CNN	CICIDS2017,	Privacy-preserving	Synchronization	99.1%
		TON_IoT	detection	overhead	
Longari et al. [31]	RNN-AE	Car-Hacking	Lightweight temporal	Slightly lower accuracy	98%
		CAN	modeling		
Altaie and Hoomod [32]	OR-CNN	NIDS V.10 2017	High accuracy, real-time	Dataset-dependent	99.9%
			capability	performance	
Shankar et al. [33]	1D-CNN +	CICIoT2022	Captures temporal	High computation cost	99.6%
	LSTM		features effectively		
Al-Aql and Al-Shammari [34]	Hybrid	Car-Hacking	Detects sequential	Very computationally	>97%
	RNN-LSTM	CAN	attacks	heavy	
Vibhute et al. [35]	LSTM (64 units)	CIC-IDS2017	Robust real-time	Limited dataset	97.6%
			detection	variation	
Alqubaysi et al. [36]	Federated DL	Car-Hacking	Preserves privacy across	Expensive computation	99.3%
			nodes		
Wu et al. [37]	Deep Transfer	NSL-KDD,	Reuses pretrained	Survey-based execution	>99%
	Learning	CICIDS	knowledge		
Kim and Song [38]	Embeddings +	Real CAN	Lightweight and efficient	Limited evaluation	98–99%
	DL			scope	
Bilot et al. [39]	GNN	Real CAN traces	Captures relational structure	Graph overhead	Outperformed
Hasan et al. [40]	CAN-GraphiT	CAN bus (7 attacks)	Graph + temporal feature learning	Complex preprocessing	98.45%
KS and Sujit [41]	CNN + BiLSTM + Attention	IoV/CAN	Captures deep temporal patterns	High computation cost	99%

APPENDIX C

REPRESENTATIVE HYBRID, COMPARATIVE, BENCHMARKING, AND OVERVIEW STUDIES

TABLE IV. Representative Hybrid, Comparative, Benchmarking, and Overview Studies

Authors (Year)	Technique	Dataset/Scope	Strengths	Weaknesses	Result
Dayyeh et al. [42]	DT, RF, SVM	Benchmark	High detection accuracy;	Hard to distinguish	99.48%
			proactive prevention	similar attacks	
Kocher and Kumar [43]	Hybrid RF + CNN	Benchmark	High accuracy via hybrid	High computational cost	≈99%
	+ LSTM		ML/DL		
Khraisat et al. [44]	Federated Learning	Survey	Privacy-preserving;	Sensitive to data	Survey
	IDS		decentralized operation	heterogeneity; overhead	
Nair [45]	ML + DL	Traffic/IDS data	Interpretable traffic	Requires feature	Effective
			prediction + IDS	engineering	
			detection		
Rani and Kaushal [46]	Supervised ML	Realistic datasets	Diverse attacks; realistic	Imbalanced datasets	>95%
			setting		
Najafli et al. [47]	Taxonomy / Survey	Review	Comprehensive taxonomy;	No new IDS model	Review
			hybrid-focused		
Sharmin et al. [48]	Benchmarking	Comparative	Structured benchmarking	No new IDS proposed	Framework
	Framework	framework	approach		
Islam and Ali [49]	ANFIS (Hybrid ML	Benchmark	Robust (ANN + fuzzy	Limited data coverage	99.6%
	+ Fuzzy)		logic)		
Ali et al. [50]	Comparative	Real-time	Real-time latency tested	Simulated environment	DL > ML
	ML/DL	evaluation			
Alsarhan et al. [51]	Hybrid ML	Custom	Comprehensive modeling	Complex implementation	92%
Note and Ali [52]	ML vs DL	Survey	Broad comparative view	High complexity	Survey
Rakine et al. [53]	IDS Survey	Survey	Broad overview of IDS	No experimental	Review
			techniques	validation	
Hnamte and Hussain [54]	Evaluation	Comparative study	Structured benchmarking	No new IDS model	Comparative
	Framework		method		
Yang et al. [55]	Hybrid Statistical +	Benchmark	Lightweight and accurate	Requires tuning	≈99%
	NN				

References

[1] Kalkan, S. C., & Sahingoz, O. K. (2020, July). In-vehicle intrusion detection system on controller area network with machine learning models. In *2020 11th international conference on computing, communication and networking technologies (ICCCNT)* (pp. 1-6). IEEE.

[2] Alfardus, A., & Rawat, D. B. (2021, December). Intrusion detection system for can bus in-vehicle network based on machine learning algorithms. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0944-0949). IEEE.

[3] Al-Janabi, M., Ismail, M. A., & Ali, A. H. (2021). Intrusion Detection Systems, Issues, Challenges, and Needs. *Int. J. Comput. Intell. Syst.*, *14*(1), 560-571.

[4] Panigrahi, R., Borah, S., Bhoi, A. K., Ijaz, M. F., Pramanik, M., Jhaveri, R. H., & Chowdhary, C. L. (2021). Performance assessment of supervised classifiers for designing intrusion detection systems: a comprehensive review and recommendations for future research. *Mathematics*, *9*(6), 690.

[5] Micale, D., Costantino, G., Matteucci, I., Fenzl, F., Rieke, R., & Patanè, G. (2022, December). Cahoot: a context-aware vehicular intrusion detection system. In *2022 IEEE international conference on trust, security and privacy in computing and communications (TrustCom)* (pp. 1211-1218). IEEE.

[6] Alalwany, E., & Mahgoub, I. (2022). Classification of normal and malicious traffic based on an ensemble of machine learning for a vehicle can-network. *Sensors*, *22*(23), 9195.

[7] Rajapaksha, S., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., Madzudzo, G., & Cheah, M. (2023). Ai-based intrusion detection systems for in-vehicle networks: A survey. *ACM Computing Surveys*, *55*(11), 1-40.

[8] Nagarajan, J., Mansourian, P., Shahid, M. A., Jaekel, A., Saini, I., Zhang, N., & Kneppers, M. (2023). Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. *Peer-to-Peer Networking and Applications*, *16*(5), 2153-2185.

[9] Kumar, A., & Das, T. K. (2023). CAVIDS: Real time intrusion detection system for connected autonomous vehicles using logical analysis of data. *Vehicular Communications*, *43*, 100652.

[10] Ajibuwa, O., Hamdaoui, B., & Yavuz, A. A. (2023). A survey on ai/ml-driven intrusion and misbehavior detection in networked autonomous systems: techniques, challenges and opportunities. *arXiv preprint arXiv:2305.05040*.

[11] Shahriar, M. H., Xiao, Y., Moriano, P., Lou, W., & Hou, Y. T. (2023). CANShield: Deep-learning-based intrusion detection framework for controller area networks at the signal level. *IEEE Internet of Things Journal*, *10*(24), 22111-22127.

[12] Anthony, C., Elgenaidi, W., & Rao, M. (2024). Intrusion detection system for autonomous vehicles using non-tree based machine learning algorithms. *Electronics*, *13*(5), 809.

[13] Alalwany, E., & Mahgoub, I. (2024). An effective ensemble learning-based real-time intrusion detection scheme for an in-vehicle network. *Electronics*, *13*(5), 919.

[14] Huang, W., Xu, H., Gong, Y., Liu, Z., Li, F., Lin, Z., & Hu, B. J. (2024). UltraADV: An Unsupervised Deep Learning Lightweight Framework for Anomaly Detection in V2X. *IEEE Internet of Things Journal*, *12*(9), 12735-12747.

[15] El-Gayar, M. M., Alrslani, F. A., & El-Sappagh, S. (2024). Smart collaborative intrusion detection system for securing vehicular networks using ensemble

machine learning model. *Information*, *15*(10), 583.

[16] Samir, S. B. H., Raissa, M., Touati, H., Hadded, M., & Ghazzai, H. (2024). Machine learning-based intrusion detection for securing in-vehicle can bus communication. *SN Computer Science*, *5*(8), 1082.

[17] Ahmed, N., Hassan, F., Aurangzeb, K., Magsi, A. H., & Alhussein, M. (2024). Advanced machine learning approach for DoS attack resilience in internet of vehicles security. *Heliyon*, *10*(8).

[18] Ahmad, U., Han, M., & Mahmood, S. (2024). Enhancing security in connected and autonomous vehicles: a pairing approach and machine learning integration. *Applied Sciences*, *14*(13), 5648.

[19] Alemerien, K., Al-Suhemat, S., & Almahadin, M. (2024). Towards optimized machine-learning-driven intrusion detection for Internet of Things applications. *International Journal of Information Technology*, *16*(8), 4981-4994.

[20] Kousar, A., Ahmed, S., Altamimi, A., & Khan, Z. A. (2024). A Novel Light-Weight Machine Learning Classifier for Intrusion Detection in Controller Area Network in Smart Cars. *Smart Cities*, *7*(6), 3289-3314.

[21] Musa, U. I., Musa, A. I., Galadima, Y. I., Kantunsung, R. O., Gupta, S., & Dua, S. (2024, May). Machine Learning-Based Cybersecurity Optimization in Internet of Things-Enabled Autonomous Vehicles. In *2024 1st International Conference on Innovative Engineering Sciences and Technological Research (ICIESTR)* (pp. 1-6). IEEE.

[22] Adu-Kyere, A., Nigussie, E., & Isoaho, J. (2024). Analyzing the effectiveness of IDS/IPS in real-time with a custom in-vehicle design. *Procedia Computer Science*, *238*, 175-183.

[23] Abrar, M. M., Youssef, A., Islam, R., Satam, S., Latibari, B. S., Hariri, S., ... &

Satam, P. (2024). GPS-IDS: An anomaly-based GPS spoofing attack detection framework for autonomous vehicles. *arXiv preprint arXiv:2405.08359*.

[24] AL-KADRI, M. O. (2024). CAN-MIRGU: a comprehensive CAN bus attack dataset from moving vehicles for intrusion detection system evaluation.

[25] Wasicek, A., Pesé, M. D., Weimerskirch, A., Burakova, Y., & Singh, K. (2017, June). Context-aware intrusion detection in automotive control systems. In *Proc. 5th ESCAR USA Conf* (pp. 21-22).

[26] Ossen, S. (2025). *Enabling Low-Latency High-Throughput Real-Time Stream Processing Using Smart Network Compute Elements* (Doctoral dissertation, Indiana University).

[27] Liu, H., Lang, B., Liu, M., & Yan, H. (2019). CNN and RNN based payload classification methods for attack detection. *Knowledge-Based Systems*, *163*, 332-341.

[28] Faker, O., & Dogdu, E. (2019, April). Intrusion detection using big data and deep learning techniques. In *Proceedings of the 2019 ACM Southeast conference* (pp. 86-93).

[29] Kumar, A., & Sharma, I. (2023, March). CNN-based approach for IoT intrusion attack detection. In *2023 International conference on sustainable computing and data communication systems (ICSCDS)* (pp. 492-496). IEEE.

[30] Raza, M., Saeed, M. J., Riaz, M. B., & Sattar, M. A. (2024). Federated learning for privacy-preserving intrusion detection in software-defined networks. *Ieee Access*, *12*, 69551-69567.

[31] Longari, S., Pozzoli, C. A., Nichelini, A., Carminati, M., & Zanero, S. (2023, June). Candito: Improving payload-based detection of attacks on controller area networks. In *International symposium on cyber security, cryptology, and machine learning* (pp. 135-150). Cham: Springer Nature Switzerland.

[32] Altaie, R. H., & Hoomod, H. K. (2024). An intrusion detection system using a hybrid lightweight deep learning algorithm. *Engineering, Technology & Applied Science Research*, *14*(5), 16740-16743.

[33] Shankar, T. S., Shamsudeen, K. V., & Ramadass, R. (2025). 1D-CNN-based Real-Time Network Intrusion Detection with Privacy-Preserving for IoT. *Journal of Wireless Networks and Communication Systems*.

[34] Al-Aql, N., & Al-Shammari, A. (2024). Hybrid rnn-lstm networks for enhanced intrusion detection in vehicle can systems. *Journal of Electrical Systems*, *20*(6s), 3019-3031.

[35] Vibhute, A. D., Khan, M., Kanade, A., Patil, C. H., Gaikwad, S. V., Patel, K. K., & Saini, J. R. (2024). An LSTM-based novel near-real-time multiclass network intrusion detection system for complex cloud environments. *Concurrency and Computation: Practice and Experience*, *36*(11), e8024.

[36] Alqubaysi, T., Asmari, A. F. A., Alanazi, F., Almutairi, A., & Armghan, A. (2025). Federated learning-based predictive traffic management using a contained privacy-preserving scheme for autonomous vehicles. *Sensors*, *25*(4), 1116.

[37] Wu, W., Joloudari, J., Jagatheesaperumal, S., Kandala, N. V. P. S., Gaftandzhieva, S., Hussain, S., ... & Doneva, R. (2024). Deep transfer learning techniques in intrusion detection system-Internet of vehicles: a state-of-the-art review. *Computers, Materials, & Continua*, *80*(2), 2785.

[38] Kim, H. R., & Song, H. M. (2024). Lightweight IDS Framework Using Word Embeddings for In-Vehicle Network Security. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *15*(2), 1-13.

[39] Bilot, T., El Madhoun, N., Al Agha, K., & Zouaoui, A. (2023). Graph neural networks for intrusion detection: A survey. *IEEe Access*, *11*, 49114-49139.

[40] Hasan, M. M., Ghose, S., & Roy, K. C. (2025). CAN-GraphiT: A Graph-Based IDS for CAN Networks using Transformer. *IEEE Access*.

[41] KS, R. R., & Sujit, B. B. (2025). Sequential-Attention Based Neural Architecture Integrating BiLSTM and Multi-Head Attention for Dynamic Anomaly Detection in IoT Environments. *International Journal of Intelligent Engineering & Systems*, *18*(8).

[42] Dayyeh, R., AlSawareah, W., Kasasbeh, B., Qaddoura, R., & Kamal, S. (2023, December). Comparative Analysis of Decision Trees, Random Forest, and k-Nearest Neighbors in Predictive Analytics for Orange Telecom's Customer Complaint Data. In *2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)* (pp. 1-6). IEEE.

[43] Kocher, G., & Kumar, G. (2022). A hybrid deep learning approach for effective intrusion detection systems using spatial-temporal features. *Adv. Eng. Sci.*, *54*(2), 1503-1519.

[44] Khraisat, A., Alazab, A., Singh, S., Jan, T., & Jr. Gomez, A. (2024). Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions. *ACM Computing Surveys*, *57*(1), 1-38.

[45] Nair, R. (2023). Unraveling the Decision-making Process Interpretable Deep Learning IDS for Transportation Network Security. Journal of Cybersecurity & Information Management, 12(2).

[46] Rani, D., & Kaushal, N. C. (2020, July). Supervised machine learning based network intrusion detection system for Internet of Things. In *2020 11th International conference on computing, communication and networking technologies (ICCCNT)* (pp. 1-7). IEEE.

[47] Najafli, S., Toroghi Haghighat, A., & Karasfi, B. (2024). Taxonomy of deep learning-based intrusion detection system approaches in fog computing: a

systematic review. *Knowledge and Information Systems*, *66*(11), 6527-6560.

[48] Sharmin, S., Mansor, H., Abdul Kadir, A. F., & Aziz, N. A. (2024). Benchmarking frameworks and comparative studies of Controller Area Network (CAN) intrusion detection systems: A review. *Journal of Computer Security*, *32*(5), 477-507.

[49] Islam, M. N., & Ali, M. H. (2026). ANFIS-Based Controller and Associated Cybersecurity Issues with Hybrid Energy Storage Used in EV-Connected Microgrid System. *Energies*, *19*(4), 1103.

[50] Ali, M. L., Thakur, K., Schmeelk, S., Debello, J., & Dragos, D. (2025). Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study. *Applied Sciences*, *15*(4), 1903.

[51] Alsarhan, A., Alauthman, M., Alshdaifat, E. A., Al-Ghuwairi, A. R., & Al-Dubai, A. (2023). Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 6113-6122.

[52] Note, J., & Ali, M. (2022). Comparative analysis of intrusion detection system using machine learning and deep learning algorithms. *Annals of Emerging Technologies in Computing (AETiC)*, *6*(3), 19-36.

[53] Rakine, I., Oukaira, A., El Guemmat, K., Atouf, I., Ouahabi, S., Talea, M., & Bouragba, T. (2025). Comprehensive Review of Intrusion Detection Techniques: ML and DL in Different Networks. *IEEE Access*.

[54] Hnamte, V., & Hussain, J. (2023). Dependable intrusion detection system using deep convolutional neural network: A novel framework and performance evaluation approach. *Telematics and Informatics Reports*, *11*, 100077.

[55] Yang, Y. M., Chang, K. C., & Luo, J. N. (2025). Hybrid neural network-based

intrusion detection system: Leveraging lightgbm and mobilenetv2 for iot security. *Symmetry*, *17*(3), 314.