REFERENCES

[1] N. Singh, T. Mishra, and R. Banerjee, "Projection of Private Vehicle Stock in India up to 2050," *Transportation Research Procedia*, vol. 48, pp. 3380–3389, 2020, doi: 10.1016/j.trpro.2020.08.116.

[2] W. Ahmed, W. Di, and D. Mukathe, "Blockchain-Assisted Privacy-Preserving and Context-Aware Trust Management Framework for Secure Communications in VANETs," *Sensors*, vol. 23, no. 12, Jun. 2023, doi: 10.3390/s23125766.

[3] J. Kamel *et al.*, "VeReMi Extension: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, IEEE, 2020, pp. 1–6. doi: 10.1109/ICC40277.2020.9149132ï.

[4] M. L. Bouchouia *et al.*, "A Survey on Misbehavior Detection for Connected and Autonomous Vehicles," *Vehicular Communications*, no. 41, 2023, [Online]. Available: https://www.elsevier.com/open-access/userlicense/1.0/

[5] J. Kamel, M. Raashid Ansari, J. Petit, A. Kaiser, I. Ben Jemaa, and P. Urien, "Simulation Framework for Misbehavior Detection in Vehicular Networks," *IEEE Trans Veh Technol*, vol. 69, no. 6, p. 1, 2020, doi: 10.1109/TVT.2020.2984878ï.

[6] M. Muhammad and G. A. Safdar, "5G-based V2V broadcast communications: A security perspective," *Array*, vol. 11, p. 100084, Sep. 2021, doi: 10.1016/j.array.2021.100084.

[7] M. A. Amanullah, S. W. Loke, M. Baruwal Chhetri, and R. Doss, "A Taxonomy and Analysis of Misbehaviour Detection in Cooperative Intelligent Transport Systems: A Systematic Review," Aug. 28, 2023, *Association for Computing Machinery*. doi: 10.1145/3596598.

[8] D. E. Laouiti, M. Ayaida, N. Messai, S. Najeh, L. Najjar, and F. Chaabane, "Sybil Attack Detection in VANETs using an AdaBoost Classifier," in *2022 International Wireless Communications and Mobile Computing, IWCMC 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 217–222. doi: 10.1109/IWCMC55113.2022.9824974.

[9] S. A. Almalki, "An Online Polymorphic Attack Detection Model for Cooperative Intelligent Transportation Systems," University of Idaho, 2022.

[10] P. Sharma and H. Liu, "A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles," *IEEE Internet Things J*, vol. 8, no. 6, pp. 4991–4999, Mar. 2021, doi: 10.1109/JIOT.2020.3035035.

[11] I. Mahmoudi, J. Kamel, I. Ben-Jemaa, A. Kaiser, and P. Urien, "Towards a Reliable Machine Learning Based Global Misbehavior Detection in C-ITS: Model Evaluation Approach," in *Vehicular Ad-hoc Networks for Smart Cities: Third International Workshop*, Springer, 2020, pp. 73–86. [Online]. Available: https://hal.science/hal-02353893

[12] K. Sharshembiev, S. M. Yoo, and E. Elmahdi, "Protocol misbehavior detection framework using machine learning classification in vehicular Ad Hoc networks," *Wireless Networks*, vol. 27, no. 3, pp. 2103–2118, Apr. 2021, doi: 10.1007/s11276-021-02565-7.

[13] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks," *IEEE Trans Veh Technol*, vol. 69, no. 8, pp. 8871–8885, Aug. 2020, doi: 10.1109/TVT.2020.2996620.

[14] T. Nandy, R. Md Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," Feb. 01, 2024, *King Saud bin Abdulaziz University*. doi: 10.1016/j.jksuci.2024.101945.

[15] J. Zhang, B. Gong, M. Waqas, S. Tu, and S. Chen, "Many-Objective Optimization Based Intrusion Detection for in-Vehicle Network Security," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 15051–15065, Dec. 2023, doi: 10.1109/TITS.2023.3296002.

[16] A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, Jun. 2021, doi: 10.1007/s11831-020-09496-0.

[17] F. H. Kumbhar and S. Y. Shin, "Novel Vehicular Compatibility-Based Ad Hoc Message Routing Scheme in the Internet of Vehicles Using Machine Learning," *IEEE Internet Things J*, vol. 9, no. 4, pp. 2817–2828, Feb. 2022, doi: 10.1109/JIOT.2021.3093545.

[18] Y. Wang, N. Masoud, and A. Khojandi, "Real-Time Sensor Anomaly Detection and Recovery in Connected Automated Vehicle Sensors," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1411–1421, Mar. 2021, doi: 10.1109/TITS.2020.2970295.

[19] A. C. Dhar, A. Roy, M. A. H. Akhand, and M. A. S. Kamal, "CascadMLIDS: A Cascaded Machine Learning Framework for Intrusion Detection System in VANET," *Electronics (Switzerland)*, vol. 12, no. 18, Sep. 2023, doi: 10.3390/electronics12183779.

[20] B. Manale and M. Tomader, "A Survey of Intrusion Detection Algorithm in VANET," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Mar. 2020. doi: 10.1145/3386723.3387830.

[21] S. Amaouche *et al.*, "FSCB-IDS: Feature Selection and Minority Class Balancing for Attacks Detection in VANETs," *MDPI*, vol. 13, no. 13, Jul. 2023, doi: 10.3390/app13137488.

[22] W. F. Kamil and I. J. Mohammed, “Deep learning model for intrusion detection system utilizing convolution neural network,” *De Gruyter*, vol. 13, no. 1, Jan. 2023, doi: 10.1515/eng-2022-0403.

[23] Y. Xiao *et al.*, “A review of object detection based on deep learning,” *Multimed Tools Appl*, vol. 79, no. 33–34, pp. 23729–23791, Sep. 2020, doi: 10.1007/s11042-020-08976-6.

[24] A. H. Farea, O. H. Alhazmi, and K. Kucuk, “Advanced Optimized Anomaly Detection System for IoT Cyberattacks Using Artificial Intelligence,” *Computers, Materials and Continua*, vol. 78, no. 2, pp. 1525–1545, 2024, doi: 10.32604/cmc.2023.045794.

[25] A. Tuan Hoang *et al.*, “A review on application of artificial neural network (ANN) for performance and emission characteristics of diesel engine fueled with biodiesel-based fuels,” *Sustainable Energy Technologies and Assessments*, vol. 47, Oct. 2021, doi: 10.1016/j.seta.2021.101416.

[26] G. O. Anyanwu, C. I. Nwakanma, J. H. Kim, J. M. Lee, and D. S. Kim, “Misbehavior Detection in Connected Vehicles using BurST-ADMA Dataset,” in *International Conference on ICT Convergence*, IEEE Computer Society, 2022, pp. 874–878. doi: 10.1109/ICTC55196.2022.9952947.

[27] H. A. Idris, K. Ueda, B. Mokhtar, and S. A. Elsagheer Mohamed, “Machine Learning Based Misbehavior Detection System for False Data Injection Attack in Internet of Vehicles Using Neighbor Public Transport Vehicle Approach,” *International Journal of Computer Networks and Applications*, vol. 11, no. 2, pp. 159–176, Mar. 2024, doi: 10.22247/ijcna/2024/224442.

[28] B. G. Marcot and A. M. Hanea, “What is an optimal value of k in k-fold cross-validation in discrete Bayesian network analysis?,” *Comput Stat*, vol. 36, no. 3, pp. 2009–2031, Sep. 2021, doi: 10.1007/s00180-020-00999-9.

[29] M. Lee and T. Atkison, "VANET applications: Past, present, and future," *Vehicular Communications*, vol. 28, Apr. 2021, doi: 10.1016/j.vehcom.2020.100310.

[30] S. Ullah, W. Boulila, A. Koubaa, and J. Ahmad, "MAGRU-IDS: A Multi-Head Attention-Based Gated Recurrent Unit for Intrusion Detection in IIoT Networks," *IEEE Access*, vol. 11, pp. 114590–114601, 2023, doi: 10.1109/ACCESS.2023.3324657.

[31] Y. Al Sawafi, A. Touzene, and R. Hedjam, "Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, Apr. 2023, doi: 10.3390/jsan12020021.

[32] D. Kilichev, D. Turimov, and W. Kim, "Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models," *Mathematics*, vol. 12, no. 4, Feb. 2024, doi: 10.3390/math12040571.

[33] S. N. Kugali and S. Kadadevar, "Vehicular ADHOC Network (VANET):-A Brief Knowledge," *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 6, 2020, [Online]. Available: www.ijert.org

[34] S. Saudagar and R. Ranawat, "Attack Classification and Detection for Misbehaving Vehicles using ML/DL," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, pp. 491–496, 2023, doi: 10.17762/ijritcc.v11i8s.7230.

[35] Motor Industry Software Reliability Association (MISRA), "MISRA Compliance:2020," Feb. 2020. [Online]. Available: www.misra.org.uk

[36] Automotive Open System Architecture (AUTOSAR), "Specification of Cryptography," Nov. 2023.

[37] L. Deng, G. Xie, H. Liu, Y. Han, R. Li, and K. Li, "A Survey of Real-Time Ethernet Modeling and Design Methodologies: From AVB to TSN," Mar. 01, 2023, *Association for Computing Machinery*. doi: 10.1145/3487330.

[38] I. W. Damaj, J. K. Yousafzai, and H. T. Mouftah, "Future Trends in Connected and Autonomous Vehicles: Enabling Communications and Processing Technologies," *IEEE Access*, vol. 10, pp. 42334–42345, 2022, doi: 10.1109/ACCESS.2022.3168320.

[39] G. Karopoulos, G. Kambourakis, E. Chatzoglou, J. L. Hernández-Ramos, and V. Kouliaridis, "Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and a Meta-Taxonomy," *Electronics (Switzerland)*, vol. 11, no. 7, Apr. 2022, doi: 10.3390/electronics11071072.

[40] F. A. Butt, J. N. Chattha, J. Ahmad, M. U. Zia, M. Rizwan, and I. H. Naqvi, "On the Integration of Enabling Wireless Technologies and Sensor Fusion for Next-Generation Connected and Autonomous Vehicles," *IEEE Access*, vol. 10, pp. 14643–14668, 2022, doi: 10.1109/ACCESS.2022.3145972.

[41] R. S. Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, "In-Vehicle Communication Cyber Security: Challenges and Solutions," Sep. 01, 2022, *MDPI*. doi: 10.3390/s22176679.

[42] E. Moradi-Pari, D. Tian, M. Bahramgiri, S. Rajab, and S. Bai, "DSRC Versus LTE-V2X: Empirical Performance Analysis of Direct Vehicular Communication Technologies," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 5, pp. 4889–4903, May 2023, doi: 10.1109/TITS.2023.3247339.

[43] IEEE Vehicular Technology Society, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-Networking," IEEE, 2020.

[44] "MK5 RSU," 2024.

[45] "WaveBee Road AV1023A V2X Roadside Unit (RSU)," USA, USA, Jul. 2024.

[46] "Kapsch RIS-9260 V2X Roadside ITS Station," USA, Jun. 2020.

[47] "Roadside Unit 2X High performance edge-computing for best V2X experience," Munich, 2023.

[48] C. Bormann, M. Ersue, A. Keranen, and C. Gomez, "Terminology for Constrained-Node Networks," Internet Engineering Task Force (IETF). Accessed: Sep. 18, 2024. [Online]. Available: https://www.ietf.org/archive/id/draft-bormann-lwig-7228bis-08.html#name-classes-of-constrained-devi

[49] X. Xu, Y. Wang, and P. Wang, "Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks," 2022, *Hindawi Limited*. doi: 10.1155/2022/4725805.

[50] B. Hammi, Y. M. Idir, S. Zeadally, R. Khatoun, and J. Nebhen, "Is it Really Easy to Detect Sybil Attacks in C-ITS Environments: A Position Paper," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 18273–18287, Oct. 2022, doi: 10.1109/TITS.2022.3165513.

[51] R. Rahal, A. Amara Korba, and N. Ghoualmi-Zine, "Towards the Development of Realistic DoS Dataset for Intelligent Transportation Systems," *Wirel Pers Commun*, vol. 115, no. 2, pp. 1415–1444, Nov. 2020, doi: 10.1007/s11277-020-07635-1.

[52] G. B. Santhi and D. Sheela, "Reliability refinement in VANET with hybrid jamming attacks using novel index based voting algorithm," *Peer Peer Netw Appl*, vol. 13, no. 6, pp. 2145–2154, Nov. 2020, doi: 10.1007/s12083-019-00828-x.

[53] A. Youness and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," in *10th annual computing and communication workshop and conference (CCWC)*, IEEE, 2020, pp. 1110–1115.

[54] F. Pascale, E. A. Adinolfi, S. Coppola, and E. Santonicola, “Cybersecurity in automotive: An intrusion detection system in connected vehicles,” *Electronics (Basel)*, vol. 10, no. 15, Aug. 2021, doi: 10.3390/electronics10151765.

[55] A. A. Noura, R. A. Alolaqi, and R. Y. Alhumaidan, “Proposed Solutions to Detect and Prevent DoS Attacks on VANETs System,” in *3rd international conference on computer applications & information security (ICCAIS)*, Riyadh: IEEE, Mar. 2020, pp. 1–6.

[56] J. Alsamiri and K. Alsubhi, “Federated Learning for Intrusion Detection Systems in Internet of Vehicles: A General Taxonomy, Applications, and Future Directions,” *Future Internet*, vol. 15, no. 12, pp. 1–53, Dec. 2023, doi: 10.3390/fi15120403.

[57] E. Vieira, J. Almeida, J. Ferreira, and P. C. Bartolomeu, “Enabling Seamless Data Security, Consensus, and Trading in Vehicular Networks,” *IEEE Transactions on Intelligent Vehicles*, 2024, doi: 10.1109/TIV.2024.3388247.

[58] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, “MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles,” *IEEE Internet Things J*, vol. 7, no. 4, pp. 3310–3322, Apr. 2020, doi: 10.1109/JIOT.2020.2967568.

[59] H. K. Maji and M. Wang, “Black-box use of one-way functions is useless for optimal fair coin-tossing,” in *Annual International Cryptology Conference*, Springer, 2020, pp. 593–617. doi: 10.1007/978-3-030-56880-1_21.

[60] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity challenges in vehicular communications,” Jun. 01, 2020, *Elsevier Inc.* doi: 10.1016/j.vehcom.2019.100214.

[61] A. Kumar *et al.*, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocess Microsyst*, vol. 80, Feb. 2021, doi: 10.1016/j.micpro.2020.103352.

[62] A. Sangwan, G. Jambheshwar, A. Sangwan, and R. P. Singh, "A Classiication of Misbehavior Detection Schemes for VANETs: A Survey," *Wirel Pers Commun*, no. 129.1, pp. 285–322, 2023, doi: 10.21203/rs.3.rs-831966/v1.

[63] A. Chowdhury, G. Karmakar, J. Kamruzzaman, and S. Islam, "Trustworthiness of Self-Driving Vehicles for Intelligent Transportation Systems in Industry Applications," *IEEE Trans Industr Inform*, vol. 17, no. 2, pp. 961–970, Feb. 2021, doi: 10.1109/TII.2020.2987431.

[64] R. P. Nayak *et al.*, "TFMD-SDVN: a trust framework for misbehavior detection in the edge of software-defined vehicular network," *Journal of Supercomputing*, vol. 78, no. 6, pp. 7948–7981, Apr. 2022, doi: 10.1007/s11227-021-04227-z.

[65] A. Boualouache, R. Soua, and T. Engel, "SDN-based Misbehavior Detection System for Vehicular Networks," in *IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, IEEE, Jul. 2020, p. 1.

[66] K. Gu, X. Y. Dong, and W. J. Jia, "Malicious Node Detection Scheme Based on Correlation of Data and Network Topology in Fog Computing-Based VANETs," *IEEE Transactions on Cloud Computing*, vol. 10, no. 2, pp. 1215–1232, 2022, doi: 10.1109/TCC.2020.2985050.

[67] S. Sultan, Q. Javaid, A. J. Malik, F. Al-Turjman, and M. Attique, "Collaborative-trust approach toward malicious node detection in vehicular ad hoc networks," *Environ Dev Sustain*, vol. 24, no. 6, pp. 7532–7550, Jun. 2022, doi: 10.1007/s10668-021-01632-5.

[68] A. Sangwan, A. Sangwan, and R. P. Singh, "A Classification of Misbehavior Detection Schemes for VANETs: A Survey," *Wirel Pers Commun*, vol. 129, no. 1, pp. 285–322, Mar. 2023, doi: 10.1007/s11277-022-10098-1.

[69] A. Boualouache and T. Engel, "A Survey on Machine Learning-Based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 2, pp. 1128–1172, 2023, doi: 10.1109/COMST.2023.3236448.

[70] F. Haidar, M. Makassikis, M. Sall, H. Bakhti, A. Kaiser, and B. Lonc, "Experimentation and Assessment of Pseudonym Certificate Management and Misbehavior Detection in C-ITS," *IEEE Open Journal of Intelligent Transportation Systems*, vol. 2, pp. 128–139, 2021, doi: 10.1109/OJITS.2021.3085366.

[71] F. Hawlader, A. Boualouache, S. Faye, and T. Engel, "Intelligent Misbehavior Detection System for Detecting False Position Attacks in Vehicular Networks," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, IEEE, 2021, pp. 1–6.

[72] H. Y. Hsu, N. H. Cheng, and C. W. Tsai, "A Deep Learning-Based Integrated Algorithm for Misbehavior Detection System in VANETs," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2021, pp. 53–58. doi: 10.1145/3491396.3506509.

[73] Y. Liu, H. Xue, W. Zhuang, F. Wang, L. Xu, and G. Yin, "CT2-MDS: Cooperative trust-aware tolerant misbehaviour detection system for connected and automated vehicles," *IET Intelligent Transport Systems*, vol. 16, no. 2, pp. 218–231, Feb. 2022, doi: 10.1049/itr2.12139.

[74] A. Goyal, A. Bhatia, A. Yadav, and D. K. Sharma, "Misbehavior Detection in Cooperative Intelligent Transportation Systems using Temporal Fusion

Transformer," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jan. 2023, pp. 431–437. doi: 10.1145/3571306.3571448.

[75] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior Detection for Position Falsification Attacks in VANETs Using Machine Learning," *IEEE Access*, vol. 10, pp. 1893–1904, 2022, doi: 10.1109/ACCESS.2021.3136706.

[76] A. R. Abdulla and N. G. M. Jameel, "A Review on IoT Intrusion Detection Systems Using Supervised Machine Learning: Techniques, Datasets, and Algorithms," *UHD Journal of Science and Technology*, vol. 7, no. 1, pp. 53–65, Mar. 2023, doi: 10.21928/uhdjst.v7n1y2023.pp53-65.

[77] E. Ashraf, N. F. F. Areed, H. Salem, E. H. Abdelhady, and A. Farouk, "IoT Based Intrusion Detection Systems from The Perspective of Machine and Deep Learning: A Survey and Comparative Study," 2022.

[78] M. K. Dahouda and I. Joe, "A Deep-Learned Embedding Technique for Categorical Features Encoding," *IEEE Access*, vol. 9, pp. 114381–114391, 2021, doi: 10.1109/ACCESS.2021.3104357.

[79] P. Li, X. Rao, J. Blase, Y. Zhang, X. Chu, and C. Zhang, "CleanML: A Study for Evaluating the Impact of Data Cleaning on ML Classification Tasks," in *IEEE 37th International Conference on Data Engineering (ICDE)*, IEEE, Apr. 2021. [Online]. Available: http://arxiv.org/abs/1904.09483

[80] M. Naveed *et al.*, "A Deep Learning-Based Framework for Feature Extraction and Classification of Intrusion Detection in Networks," *Wirel Commun Mob Comput*, vol. 2022, 2022, doi: 10.1155/2022/2215852.

[81] H. Wang and Y. Li, "Overview of DDoS Attack Detection in Software-Defined Networks," *IEEE Access*, vol. 12, pp. 38351–38381, 2024, doi: 10.1109/ACCESS.2024.3375395.

[82] I. Baturynska and K. Martinsen, “Prediction of geometry deviations in additive manufactured parts: comparison of linear regression with machine learning algorithms,” *J Intell Manuf*, vol. 32, no. 1, pp. 179–200, Jan. 2021, doi: 10.1007/s10845-020-01567-0.

[83] M. T. Nguyen and K. Kim, “Genetic convolutional neural network for intrusion detection systems,” *Future Generation Computer Systems*, vol. 113, pp. 418–427, Dec. 2020, doi: 10.1016/j.future.2020.07.042.

[84] Y. Guo, Z. Mustafaoglu, and D. Koundal, “Spam Detection Using Bidirectional Transformers and Machine Learning Classifier Algorithms,” *Journal of Computational and Cognitive Engineering*, vol. 2, no. 1, pp. 5–9, Feb. 2023, doi: 10.47852/bonviewJCCE2202192.

[85] R. W. Van Der Heijden, T. Lukaseder, and F. Kargl, “VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs,” in *Security and Privacy in Communication Networks: 14th International Conference*, Singapore: Springer International Publishing, Aug. 2018, pp. 318–337.

[86] G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D. S. Kim, “Falsification Detection System for IoV Using Randomized Search Optimization Ensemble Algorithm,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, pp. 4158–4172, Apr. 2023, doi: 10.1109/TITS.2022.3233536.

[87] A. H. Magsi, A. Ghulam, S. Memon, K. Javeed, M. Alhussein, and I. Rida, “A Machine Learning-Based Attack Detection and Prevention System in Vehicular Named Data Networking,” *Computers, Materials and Continua*, vol. 77, pp. 1445–1465, 2023, doi: 10.32604/cmc.2023.040290.

[88] T. Alladi, V. Kohli, V. Chamola, and F. R. Yu, “A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent

transportation systems," *Digital Communications and Networks*, vol. 9, no. 5, pp. 1113–1122, Oct. 2023, doi: 10.1016/j.dcan.2022.06.018.

[89] S. F. Ahmed *et al.*, "Deep learning modelling techniques: current progress, applications, advantages, and challenges," *Artif Intell Rev*, vol. 56, no. 11, pp. 13521–13617, Nov. 2023, doi: 10.1007/s10462-023-10466-8.

[90] M. A. Amanullah, M. B. Chhetri, S. W. Loke, and R. Doss, "BurST-ADMA: Towards an Australian Dataset for Misbehaviour Detection in the Internet of Vehicles," *IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, 2022.

[91] H. A. Idris *et al.*, "Explaining Machine Learning Based Speed Anomaly Detection System Using eXplainable Artificial Intelligence," *13th International Conference on Information Systems and Advanced Technologies*, pp. 64–76, 2024, doi: 10.1007/978-3-031-60594-9_8.

[92] H. A. Idris, K. Ueda, B. Mokhtar, and S. A. Elsagheer Mohamed, "Novel Intelligent BSM Falsification Attack Detection System Using Trusted Neighbor Vehicle Approach in IoV," *International Journal of Computing*, vol. 23, no. 1, pp. 116–125, 2024, doi: 10.47839/ijc.23.1.3443.