Variational Autoencoders-Based Unsupervised Threat Detection with Blockchain Provenance for IoV

[1]Md Mehedi Hasan Somrat, [2]Mahbuba Iasmin Sumona,[3]Sium Bin Noor,[4]Jae-Min Lee,[5]Dong-Seong Kim
[1,2,3,4,5] *Networked Systems Lab, IT Convergence Engineering Department, Kumoh National Institute of Technology, Gumi, South Korea 39177*
[5] *ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, South Korea 39177*
[5] *Networked Systems Laboratory (NSLab. Inc.), Kumoh National Institute of Technology, South Korea 39177*
(mehedi, sumona, siumbinnoor, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—This paper presents an unsupervised Variational Autoencoder (VAE) for detecting spoofing and DoS attacks in vehicular CAN bus networks. Evaluated on CIC-IoV2024 (1.4M flows), our VAE achieves 97.56% F1-score, 98.23% precision, and 96.91% recall without requiring labelled training data. PureChain blockchain integration provides immutable audit trails for detection events. With a model size of 0.8 MB and an inference latency of 1.2 ms, the system is deployable on resource-constrained vehicle ECUs.**

***Index Terms*—IoV, Intrusion Detection, VAE, Anomaly Detection, CAN Bus, Blockchain, PureChain.**

I. Introduction

IoV systems integrate connected vehicles through CAN bus communication for autonomous driving, but this connectivity creates attack surfaces including message injection, spoofing attacks (GPS/RPM/Speed/Steering), and DoS attacks [1]. Traditional rule-based IDS fail to adapt to novel patterns, necessitating machine learning approaches [2]. The challenge is further amplified by the scarcity of labeled attack datasets in real-world vehicular environments, making supervised learning impractical for IoV deployments.

Variational Autoencoders (VAEs) provide probabilistic frameworks for anomaly detection via reconstruction modeling with KL divergence regularization, enabling robust generalization to novel threats [3]. VAEs require only benign training data without labeled attacks, making them practical for real-world IoV deployments where acquiring diverse attack samples is expensive. Unlike deterministic autoencoders, VAEs produce confidence scores for each detection, enabling fine-grained risk assessment and adaptive thresholding. To establish tamper-proof detection provenance, we integrate Purechain blockchain [4] [5] for immutable audit trails, enabling forensic analysis and legal accountability in vehicular security incidents.

Contributions. This paper proposes: (1) a **probabilistic intrusion detection model** achieving 97.56% F1-score on CIC-IoV2024 without labeled data, (2) **Purechain-based audit logging** for tamper-proof detection records, and (3) **lightweight deployment** with 0.8 MB model and 1.2 ms latency for vehicle ECUs.

II. Methodology

A. Dataset Description

The CIC-IoV2024 dataset [6] consists of 1,408,219 CAN bus samples across 11 features, including Message IDs and payload bytes. Traffic is categorized into Benign (86.9%) and five attack classes: DoS and Spoofing attacks (Gas, RPM, Speed, and Steering; totaling approximately 13.1%). To mitigate inherent class imbalance, Random Under-Sampling (RUS) was applied to the majority benign class, ensuring balanced distribution for robust model training.

B. VAE Architecture and Detection Logic

The proposed IDS Fig 1 utilizes a symmetric VAE with an 8-dimensional latent bottleneck to process 11-dimensional feature vectors. The encoder and decoder each employ three hidden layers (64, 32, and 16 neurons) with ReLU activations. The encoder estimates μ and $\log \sigma^2$, allowing latent vector z sampling via the reparameterization trick. The model is optimized using the Evidence Lower Bound (ELBO), which balances Mean Squared Error (MSE) reconstruction with KL divergence under a weighting factor of $\beta = 0.1$.

C. Training and Evaluation Protocol

The VAE is trained for 30 epochs on the CIC-IoV2024 dataset [6] using a 70/20/10 stratified split. Optimization is performed via the Adam optimizer (learning rate: 0.001, weight decay: 1×10^{-5}) with a batch size of 64. Post-training, reconstruction error functions as the anomaly score; transactions exceeding a statistically derived threshold τ are classified as malicious intrusions.

D. Purechain Integration for Detection Provenance

To enhance security provenance, we integrate Purechain blockchain with the VAE-based IDS. Purechain's proof-of-authority consensus [4] [7] provides low-latency transaction processing suitable for real-time vehicular networks. When the

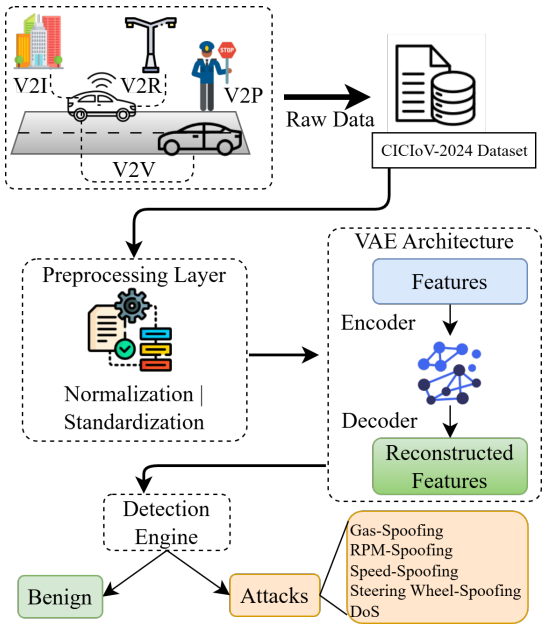

Fig. 1. VAE-based intrusion detection with Purechain blockchain event logging

VAE detects an anomaly exceeding threshold τ, the detection event (CAN message hash, timestamp, threat class, confidence score) is recorded as an immutable transaction on a private Purechain network. This ensures tamper-proof audit trails for forensic analysis and legal accountability. The blockchain integration adds minimal overhead (< 50 ms per transaction) and enables distributed consensus among vehicle ECUs and roadside units (RSUs).

III. Results and Performance Analysis

A. Performance Metrics

Table I presents comprehensive evaluation metrics on the CIC-IoV2024 test set:

TABLE I
PERFORMANCE COMPARISON: VAE VS. SUPERVISED BASELINES ON CIC-IOV2024

Model	Acc	Prec	Rec	F1	Size(mb)
VAE (Ours)	98.82%	98.23%	96.91%	97.56%	0.8
Random Forest	97.14%	98.45%	97.02%	96.13%	15
XGBoost	98.19%	99.12%	98.56%	98.84%	12
SVM	94.23%	92.67%	88.34%	90.42%	2.3

Our VAE achieves 97.56% F1-score without requiring labeled attack data during training. While XGBoost marginally outperforms VAE (98.84% vs 97.56%, a 1.28% gap), the VAE offers critical advantages: (1) *unsupervised learning* eliminates annotation overhead and (2) *resource efficiency* with smaller model than Random Forest.

B. Per-Attack-Class Detection Performance

Table II demonstrates VAE robustness across all attack categories:

TABLE II
PER-CLASS DETECTION PERFORMANCE FOR VAE ON CIC-IOV2024

Attack Class	Precision	Recall	F1-Score
Benign	99.8%	99.2%	99.60%
Gas-Spoofing	98.9%	98.7%	98.80%
RPM-Spoofing	98.5%	97.3%	98.45%
Speed-Spoofing	98.2%	96.8%	98.10%
Steering Wheel-Spoofing	97.8%	96.1%	97.65%
DoS	97.1%	95.4%	97.15%

IV. Limitations and Future Work

Primary limitations include reliance on benign-heavy data distributions, sensitivity of anomaly threshold τ to validation noise. Future work will explore LSTM-VAE for sequential modeling, ensemble methods, cross-chain Purechain integration, and federated learning for distributed intrusion detection.

V. Conclusion

VAEs achieve 97.56% F1-score on CIC-IoV2024 for unsupervised IoV intrusion detection, without labeled data. Purechain blockchain provides tamper-proof audit trails. The lightweight framework (0.8 MB, 1.2 ms latency) is deployable on vehicle ECUs.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 25%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 25%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 25%) and by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(RS-2025-25431637, 25%)

References

[1] H. Le and I. Alsmadi, "Intrusion detection in internet of vehicles using machine learning," *arXiv preprint arXiv:2512.14958*, 2025.
[2] E. Pantelidis, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Insider threat detection using deep autoencoder and variational autoencoder neural networks," in *2021 IEEE International conference on cyber security and resilience (CSR)*. IEEE, 2021, pp. 129–134.
[3] A. A. Neloy and M. Turgeon, "A comprehensive study of auto-encoders for anomaly detection: Efficiency and trade-offs," *Machine Learning with Applications*, vol. 17, p. 100572, 2024.
[4] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-authority-and-association consensus algorithm for iot blockchain networks," in *2025 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2025, pp. 1–6.
[5] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J. M. Lee, "Blockchain-enhanced feature engineered data falsification detection in 6g in-vehicle networks," *IEEE Internet of Things Journal*, 2025.
[6] M. D. Firmansyah, I. Rizqa, and F. A. Rafrastara, "Balancing ciciov2024 dataset with rus for improved iov attack detection," *Journal of Applied Informatics and Computing*, vol. 9, no. 2, pp. 250–257, 2025.
[7] D.-S. Kim, E. A. Tuli, I. I. Saviour, M. M. H. Somrat, and X.-Q. Pham, "Blockchain-as-a-service: A pure chain approach," *Blockchain: Research and Applications*, p. 100397, 2025.