AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY UNDER SECTION 3 OF UGC ACT, 1956

MYSURU CAMPUS

Dissertation Phase II- 18CA497

DETECTION AND PREVENTION OF DOS AND FUZZY CAN BUS ATTACKS ON AUTONOMOUS CAR USING QUANTUM MACHINE LEARNING

Meghana R, Sowmyashree Sakrepatna Ramesha
PG Student Department of Computer Science, School of Computing, Amrita Vishwa Vidyapeetham, Mysuru.

Supervisor:
Dr. Adwitiya Mukhopadhyay
Vice Chairperson, Department of Computer Science, School of Computing, Amrita Vishwa Vidyapeetham, Mysuru.

ABSTRACT

In this study, we introduce an advanced cybersecurity framework for both detection and prevention of Denial-of-Service DoS and Fuzzy attacks on the CAN bus of autonomous vehicles, leveraging Quantum Machine Learning for enhanced threat detection and using a honeypot-based intrusion prevention system for real-time mitigation.

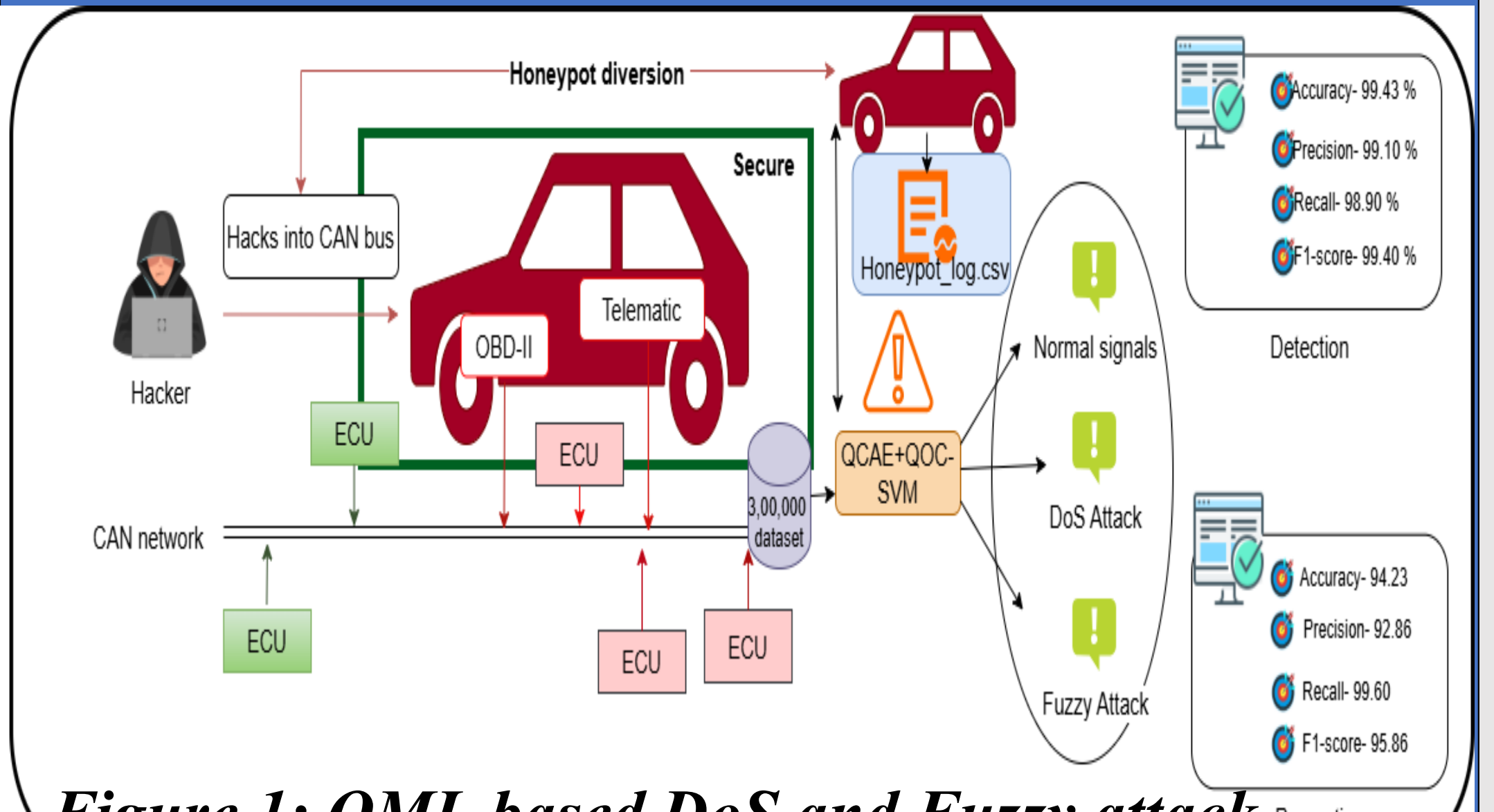


Figure 1: QML based DoS and Fuzzy attack detection and prevention

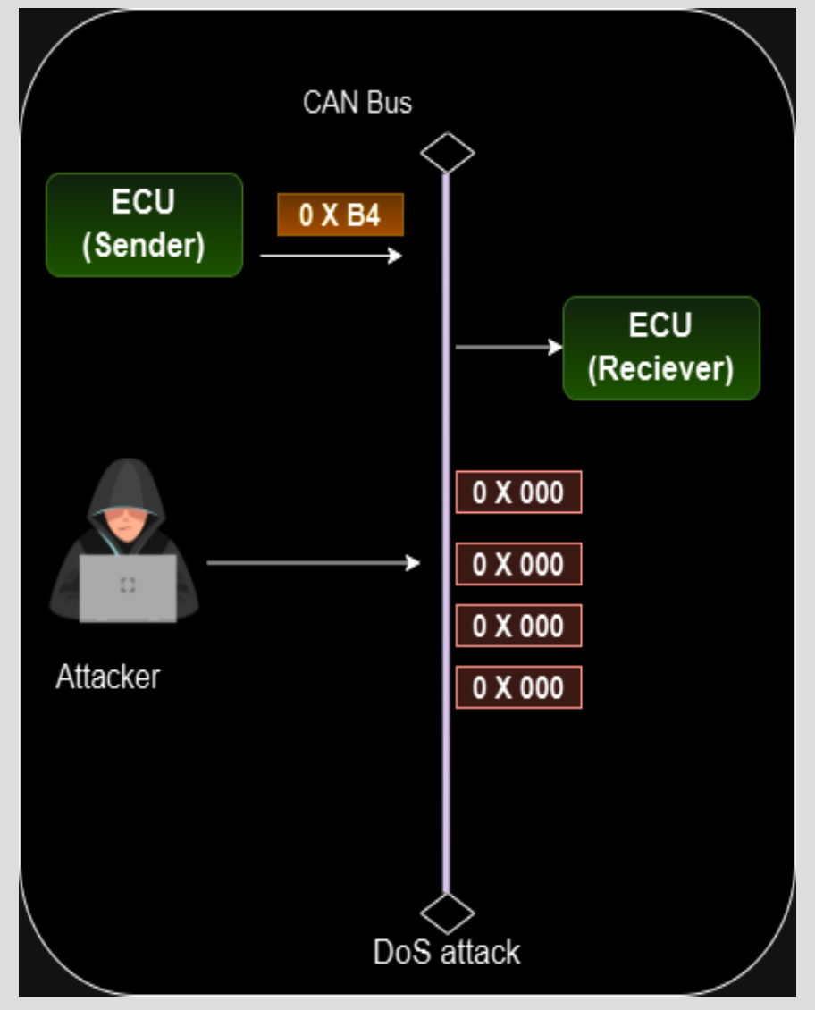
INTRODUCTION

OBJECTIVES

- Develop a QML model to detect DoS and fuzzy attacks on the CAN bus.
- Use quantum autoencoders and SVMs for traffic classification.
- Compare model performance with ML, DL, and QML baselines.
- Build a real-time honeypot system for attack prevention.
- Test system scalability, speed, and real-time efficiency.

COMPARISION OF DOS VS FUZZY ATTACKS

Figure 2: DoS attack scenario



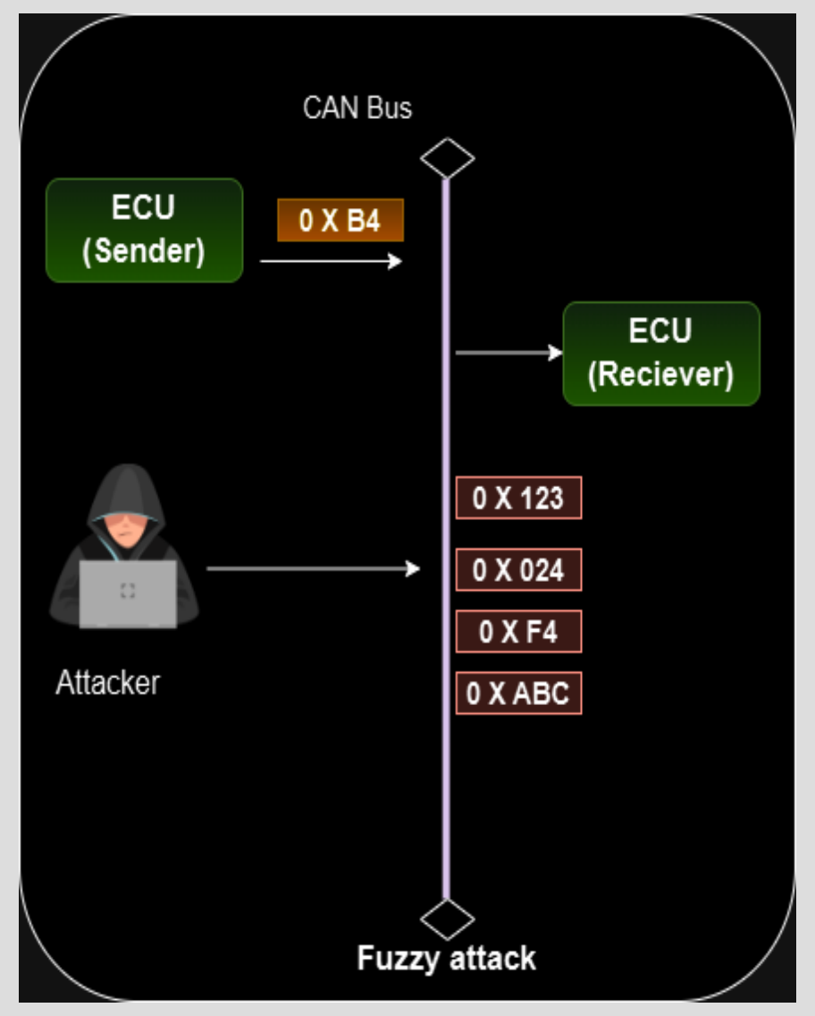


Figure 2: Fuzzy attack scenario

PROPOSED MODEL FOR DETECTION

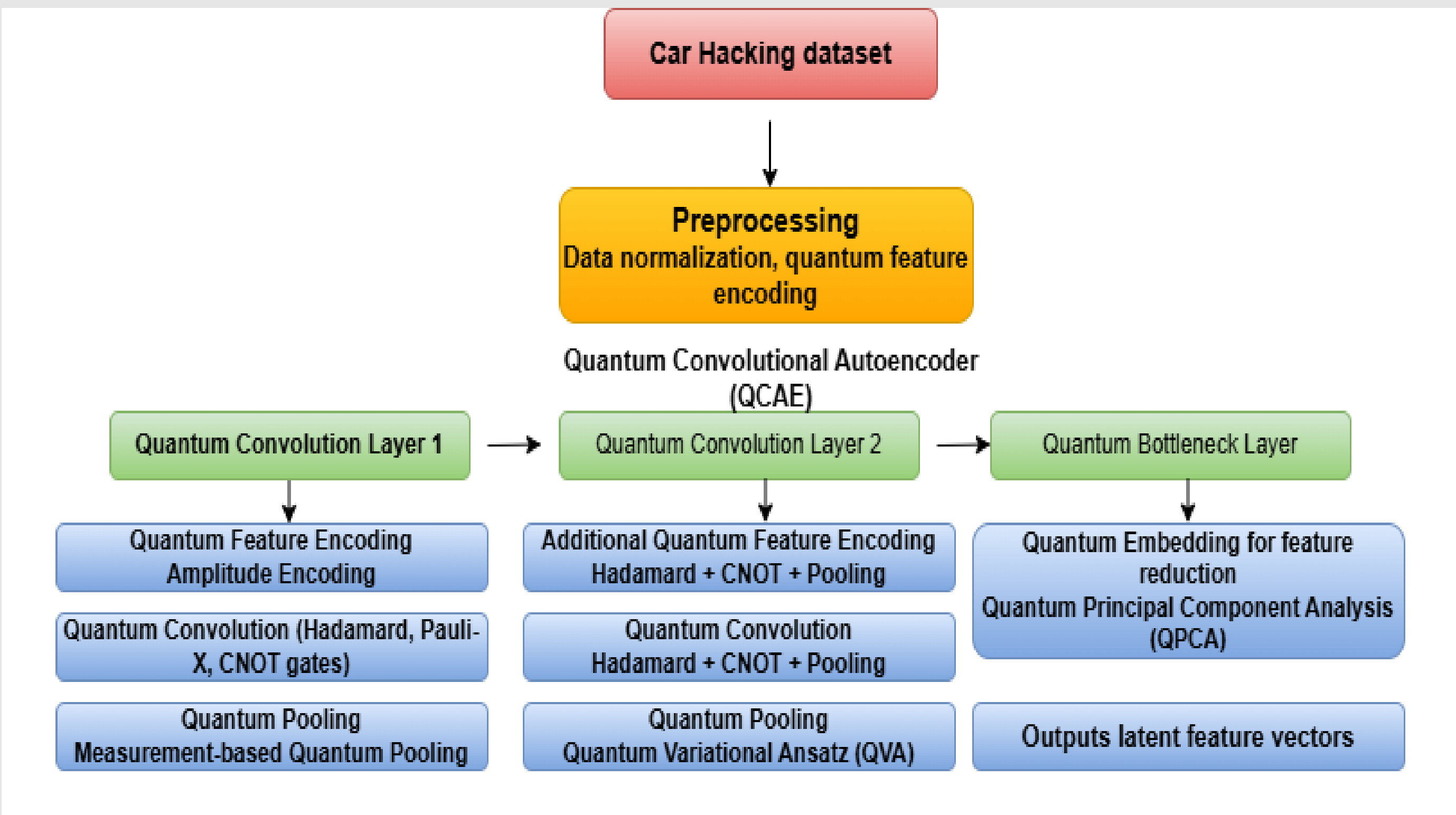

Car Hacking dataset
Preprocessing
Data normalization, quantum feature encoding
Quantum Convolutional Autoencoder (QCAE)
Quantum Convolution Layer 1
Quantum Convolution Layer 2
Quantum Bottleneck Layer
Quantum Feature Encoding
Amplitude Encoding
Quantum Convolution (Hadamard, Pauli-X, CNOT gates)
Quantum Pooling
Measurement-based Quantum Pooling
Additional Quantum Feature Encoding
Hadamard + CNOT + Pooling
Quantum Convolution
Hadamard + CNOT + Pooling
Quantum Pooling
Quantum Variational Ansatz (QVA)
Quantum Embedding for feature reduction
Quantum Principal Component Analysis (QPCA)
Outputs latent feature vectors

Figure 2: Quantum Convolutional Autoencoder (QCAE)

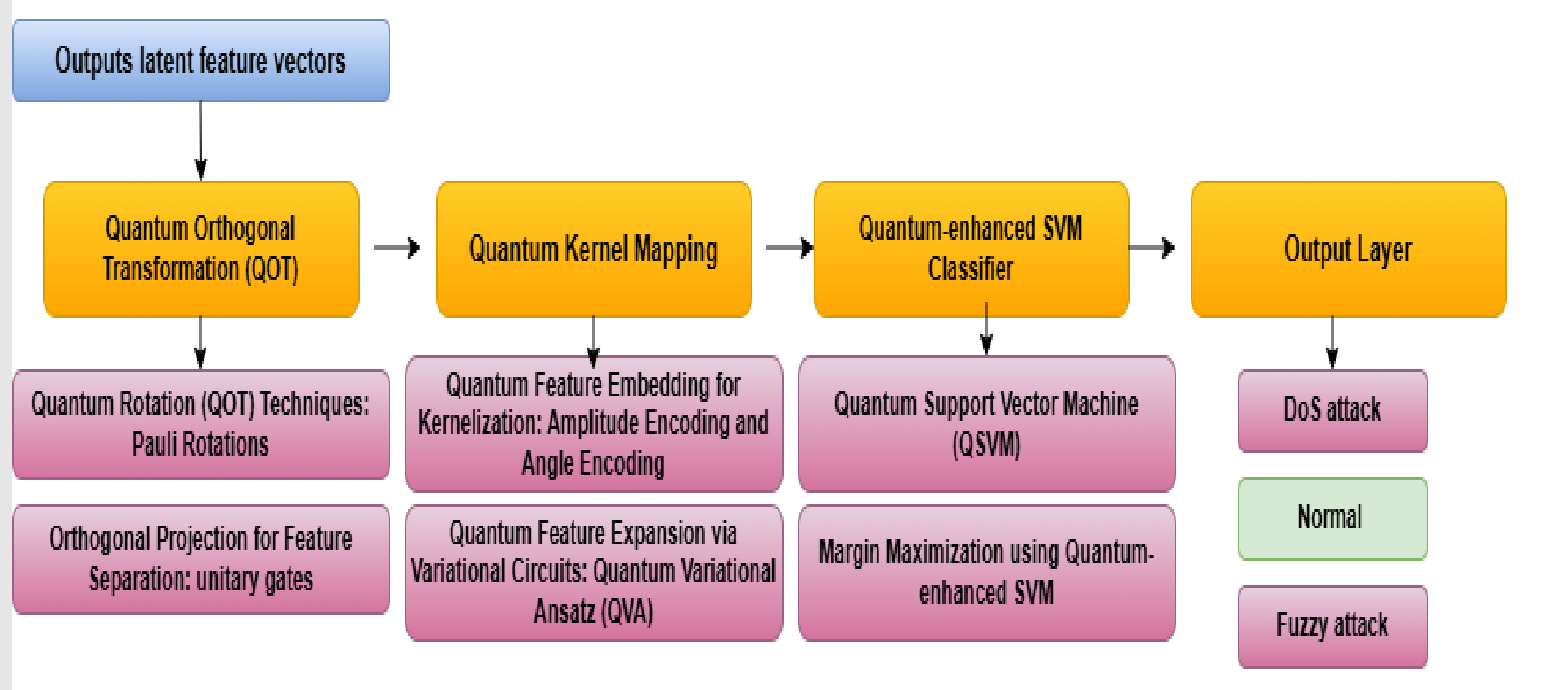

Outputs latent feature vectors
Quantum Orthogonal Transformation (QOT)
Quantum Kernel Mapping
Quantum-enhanced SVM Classifier
Output Layer
Quantum Rotation (QOT) Techniques: Pauli Rotations
Orthogonal Projection for Feature Separation: unitary gates
Quantum Feature Embedding for Kernelization: Amplitude Encoding and Angle Encoding
Quantum Feature Expansion via Variational Circuits: Quantum Variational Ansatz (QVA)
Quantum Support Vector Machine (QSVM)
Margin Maximization using Quantum-enhanced SVM
DoS attack
Normal
Fuzzy attack

Figure 3: Quantum Orthogonal Classifier with SVM (QOC-SVM)

PROPOSED MODEL FOR PRVENTION

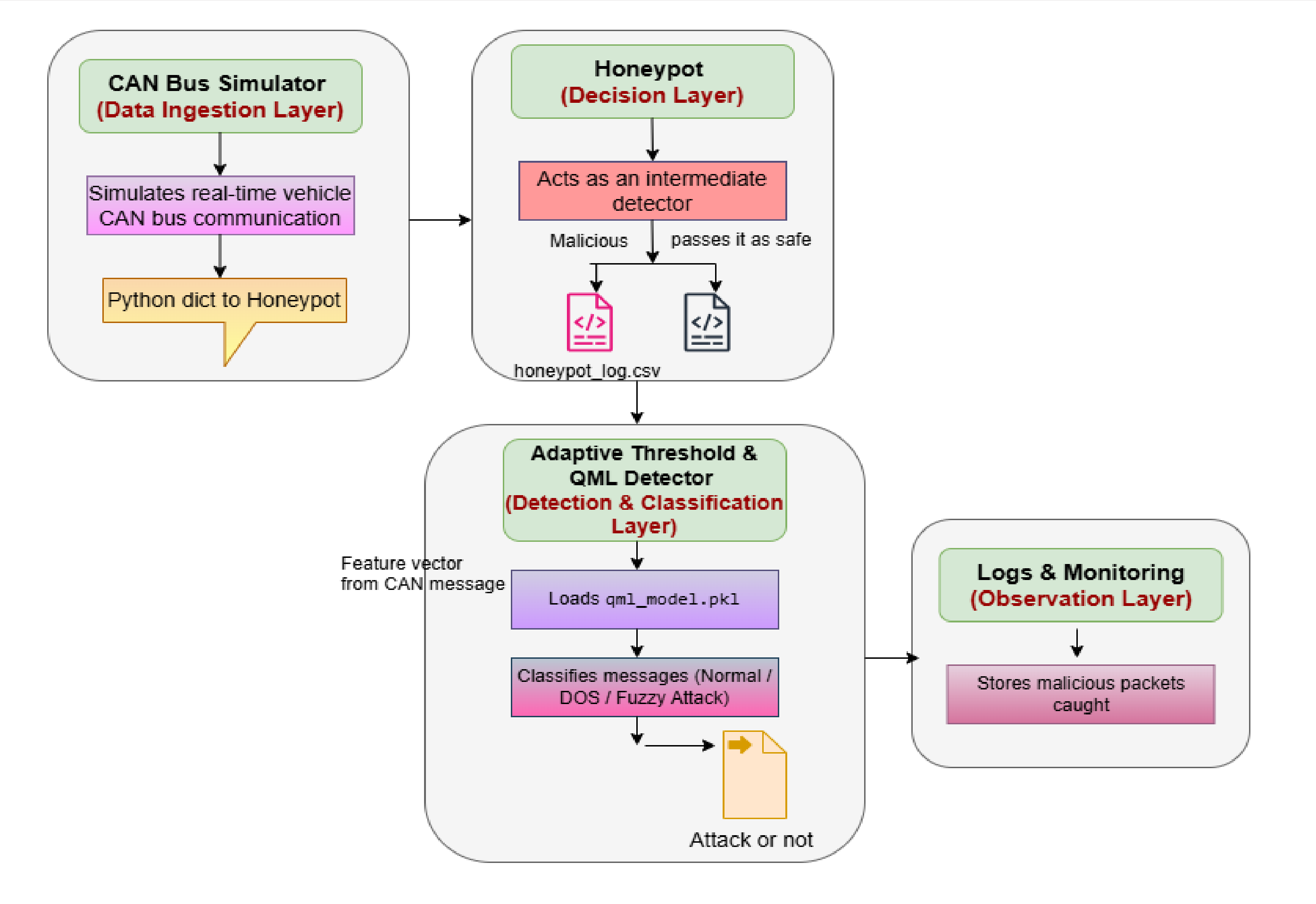

CAN Bus Simulator
(Data Ingestion Layer)
Simulates real-time vehicle CAN bus communication
Python dict to Honeypot
Honeypot
(Decision Layer)
Acts as an intermediate detector
Malicious
passes it as safe
honeypot_log.csv
Adaptive Threshold & QML Detector
(Detection & Classification Layer)
Feature vector from CAN message
Loads qml_model.pkl
Classifies messages (Normal / DOS / Fuzzy Attack)
Attack or not
Logs & Monitoring
(Observation Layer)
Stores malicious packets caught

Figure 4:QML based Honeypot prevention model

EXPERIMENTAL RESULTS

Models	Accuracy (%)	Precision	Recall	F1-score	No. of Batches: Batch Size
Machine Learning					
SVM	84.31	0.89	0.84	0.84	6000:40
RF	88.95	0.89	0.89	0.89	6153:39
KNN	94.05	0.94	0.94	0.94	-
Naive Bayes	94.31	0.94	0.94	0.94	-
XGB	91.00	0.91	0.91	0.91	-
Deep Learning					
CNN	94.50	0.9453	0.9457	0.9445	7500:32
MLP	93.80	0.92	0.926	0.929	6154:39
FNN	95.00	0.9510	0.950	0.9530	7500:32
Models	Accuracy (%)	Precision	Recall	F1-score	No. of Batches: Batch Size
QML					
QAE	97.30	0.97	0.93	0.972	4897:49
VQC	91.05	0.92	0.91	0.91	2891:83
QSVM	97.80	0.978	0.96	0.965	6000:40
QKNN	82.61	0.88	0.83	0.82	13333:18
Hybrid QML					
QAE+QRF	93.26	0.9298	0.9278	0.9328	4363:55
QAE+QKNN	94.98	0.9470	0.9450	0.9500	4897:49
QCAE+QOC-SVM	99.43	0.991	0.989	0.994	7741:31

Table 1. Experimental Results of detection

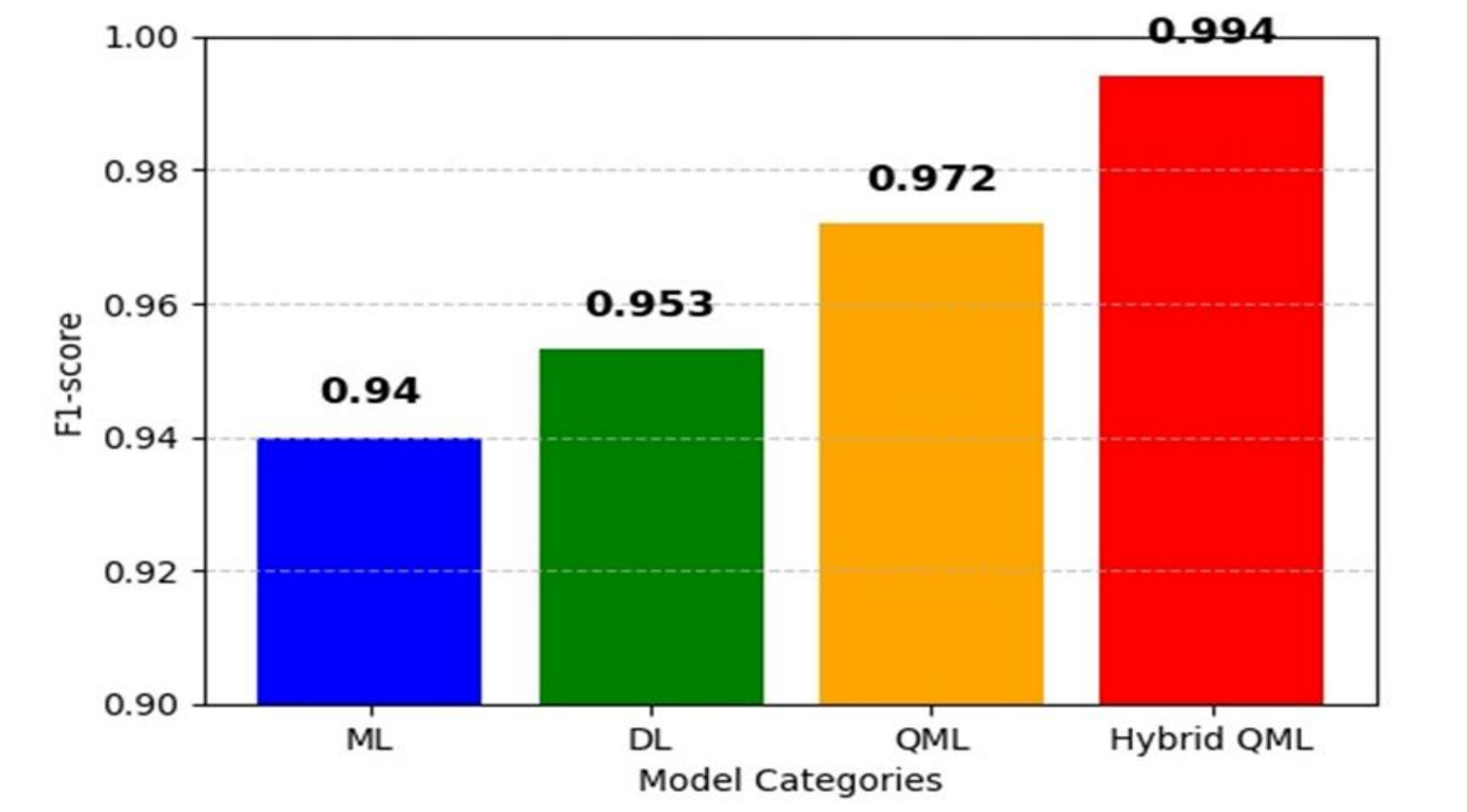


Figure 4. F1 Score

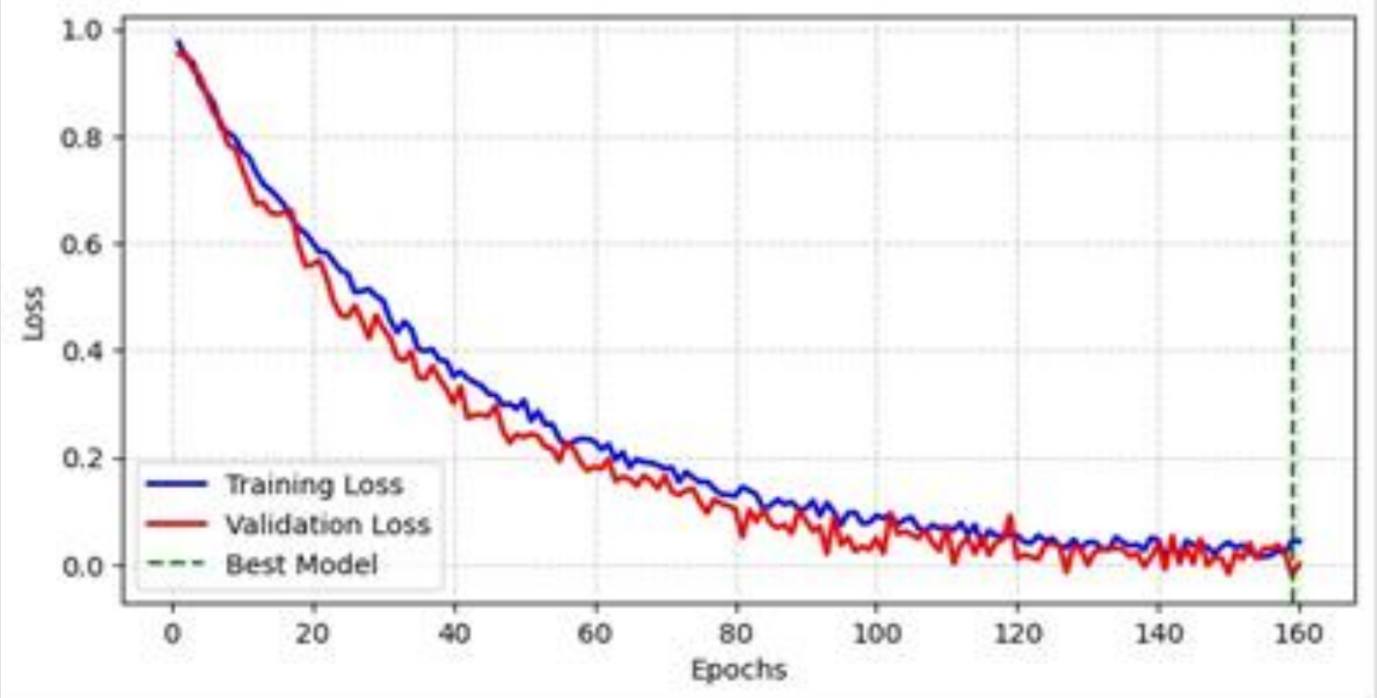


Figure 5. Learning curve

Model	Threshold Dos: Fuzzy: Normal	Accuracy (%)	Precision	Recall	F1 score
QCAE +QOC-SVM	0.4: 0.3: 0.7	80	68.72	89.60	80.94
QCAE +QOC-SVM	0.5: 0.5: 0.5	86	72.34	88.56	89.996
QCAE +QOC-SVM	0.6: 0.6: 0.8	94.29	92.86	99.06	95.86

Table 1. Experimental Results of Prevention

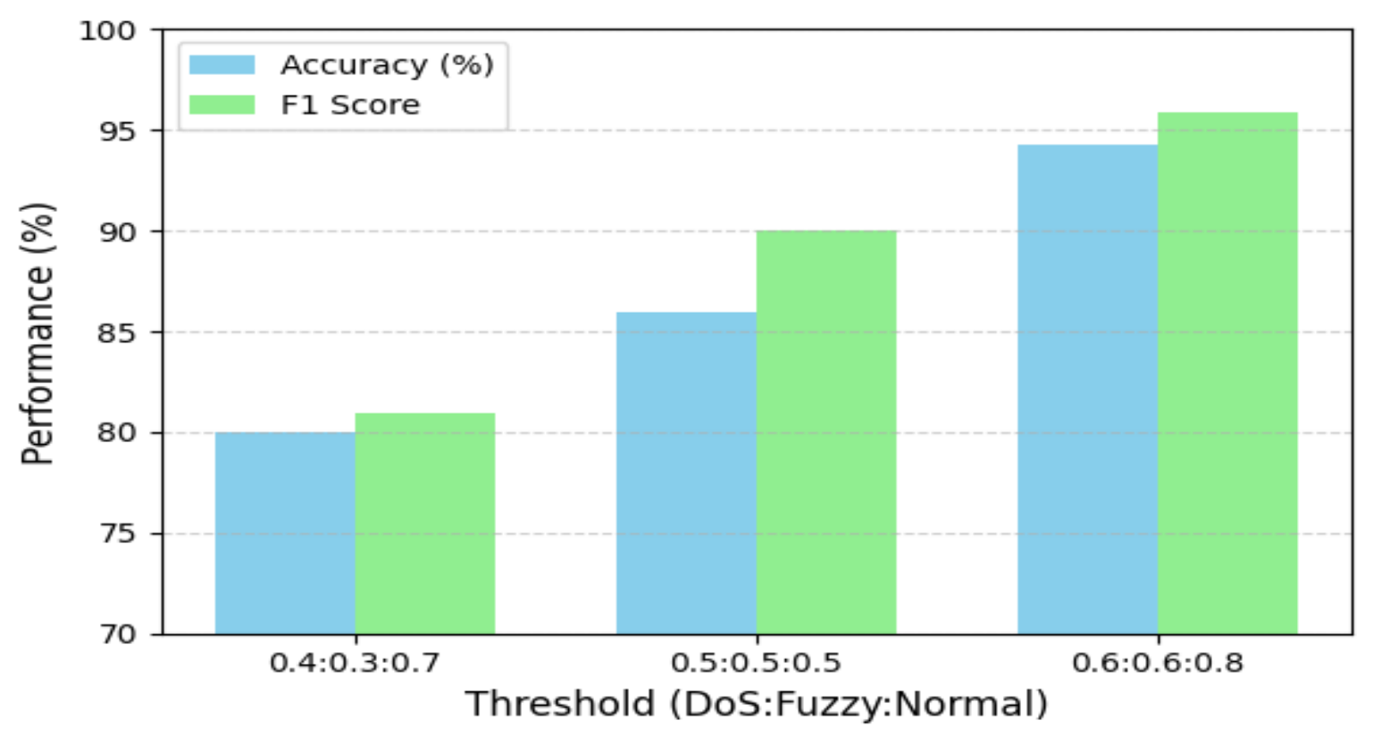


Figure 6. Accuracy & F1 score vs Threshold

CONCLUSION

This research proposes an integrated detection and prevention framework to secure autonomous vehicles against Denial of Service (DoS) and Fuzzy Attacks on the CAN bus using Quantum Machine Learning (QML).

🧠 **The detection system uses:**

- Quantum Convolutional Autoencoder (QCAE) for feature extraction.
- Quantum Orthogonal Classifier with SVM (QOC-SVM) for message classification.

📊 The QCAE+QOC-SVM hybrid model effectively distinguishes Normal, DoS, and Fuzzy signals, achieving:

- F1-Score: 99.43%
- On a dataset of over 300,000 CAN messages (public + simulator-generated).

🔍 The model demonstrates robustness and flexibility, requiring minimal supervision and adapting well to complex traffic patterns.

🛡 The prevention system is integrated into a honeypot setup:

Malicious messages are detected in real-time.

- Redirected to logging mechanisms, preventing them from affecting the vehicle's control system.

📈 The prevention layer achieved:

- Accuracy: 94.29%
- F1-Score: 95.86%
- Proving it to be highly reliable and responsive in mitigating real-time threats.

CONFERENCE AND PUBLICATION

1. QCAE-QOC-SVM: A Hybrid Quantum Machine Learning Model for DoS and Fuzzy Attack Detection on Autonomous Vehicle CAN Bus.- MethodsX jornal- Submitted.

2. Autonomous Vulnerabilities: An In-Depth Review of Cyber Attacks Targeting Self-Driving Cars and Sustainable Development Goals – ***yet to submit.***

3. A Smart Honeypot-Based Intrusion Prevention Framework for Securing In-Vehicle Networks Against DoS and Fuzzy Threats **– yet to submit**.

REFERENCES

1. U. Ahmad, M. Han, and S. Mahmood. Enhancing security in connected and autonomous vehicles: A pairing approach and machine learning integration. Applied Sciences, 14(13):5648, June 2024.

2. Oleg Illiashenko, Vyacheslav Kharchenko, Ievgen Babeshko, Herman Fesenko, and Felicita Di Giandomenico. Security-informed safety analysis of autonomous transport systems considering ai-powered cyberattacks and protection. Entropy, 25(8):1123, July 2023.

3. Sana Aurangzeb. Cybersecurity for autonomous vehicles against malware attacks in smart-cities. Unpublished.

4. Bifta Sama Bari, Kumar Yelamarthi, and Sheikh Ghafoor. Intrusion detection in vehicle controller area network (can) bus using machine learning: A comparative performance study. Sensors, 23(7):3610, March 2023.

5. O. Y. Al-Jarrah, K. El Haloui, M. Dianati, and C. Maple. A novel detection approach of unknown cyber-attacks for intra-vehicle networks using recurrence plots and neural networks. IEEE Open Journal of Vehicular Technology, 4:271– 280, 2023.

6. Tudor Andreica, Adrian Musuroi, Alfred Anistoroaei, Camil Jichici, and Bogdan Groza. Blockchain integration for in-vehicle can bus intrusion detection systems with iso/sae 21434 compliant reporting. Scientific Reports, 14(1):8169, April 2024.