Hydro Guard-Ids AI Driven Anomaly Detection for Critical Water Infrastructure

G. Naveen Kumar[1], Kommera Shivani[2], Madaram Pranitha[2], Lode Navadeep[2], Gunivenaka Sai Teja[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering (Data science)

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India

ABSTRACT

The increasing complexity of modern water distribution systems and the growing risk of cyber-physical attacks have created a strong need for intelligent monitoring and prediction mechanisms. The traditional water monitoring system relies on manual observation and threshold-based techniques, which are inefficient in detecting anomalies and predicting system behavior accurately. These systems lack automation, real-time analysis, and the ability to handle large-scale sensor data, leading to delayed responses and potential failures. The major problem addressed in this project is the accurate detection of abnormal conditions and prediction of critical system parameters in water distribution networks using data-driven approaches. The traditional system fails to capture complex relationships among sensor readings such as tank levels, flow rates, pump status, and pressure variations. This highlights the need for an advanced system capable of performing One Classification and Four Regression Tree (1CA4RT) efficiently. To address these challenges, the system implements Restricted Boltzmann Machine (RBM) with Logistic Regression (LR) for classification and Ridge Regressor (RR) for regression, along with Adaptive Boosting (AB) and Natural Gradient Boosting (NGB) as baseline models. A hybrid model, Variational Quantum Probabilistic Tree Ensemble (VQPTE), integrating Variational Quantum Neural Network (VQNN), Probabilistic Output Representation Transformation (PORT), and Random Forest (RF), is proposed. The system classifies normal and attack conditions and predicts parameters such as average tank level, pump status, flow rate, and pressure. The VQPTE model achieves 97.35% accuracy and high R^2 scores (0.9758, 0.9913, 0.9954, 0.9826), enabling accurate, reliable, and real-time monitoring.

Keywords: Water Distribution Systems, Cyber-Physical Attacks, One Classification and Four Regression Tree (1CA4RT), Variational Quantum Probabilistic Tree Ensemble (VQPTE).

1. INTRODUCTION

Water reservoirs are susceptible to various types of attacks that can jeopardize water quality, disrupt service, and pose risks to public health and safety. The following text presents real-world examples of attacks on water reservoirs, highlighting their consequences and the lessons learned. In 1993, Milwaukee, Wisconsin, experienced a major outbreak of Cryptosporidium, a waterborne parasite, due to inadequate filtration and disinfection practices. The contamination affected the city's water reservoir and led to over 400,000 cases of illness and 69 deaths. This incident highlighted the need for improved water treatment and surveillance systems to prevent and respond to waterborne disease outbreaks [1]. In May 2000, contaminated groundwater infiltrated the municipal water supply system in Walkerton, Ontario, Canada, leading to a widespread outbreak of Escherichia coli infections. The contamination was traced back to a cattle farm near one of the wells supplying the reservoir. The incident resulted from a combination of inadequate water treatment processes, flawed monitoring, and an improper response to the detected contamination [2]. During the Iraq war in 2003, several incidents of deliberate sabotage targeted water reservoirs and treatment facilities. The attackers aimed to disrupt water supply, degrade infrastructure, and create chaos. These acts

of sabotage resulted in severe water shortages and compromised sanitation services in various regions of Iraq [3].

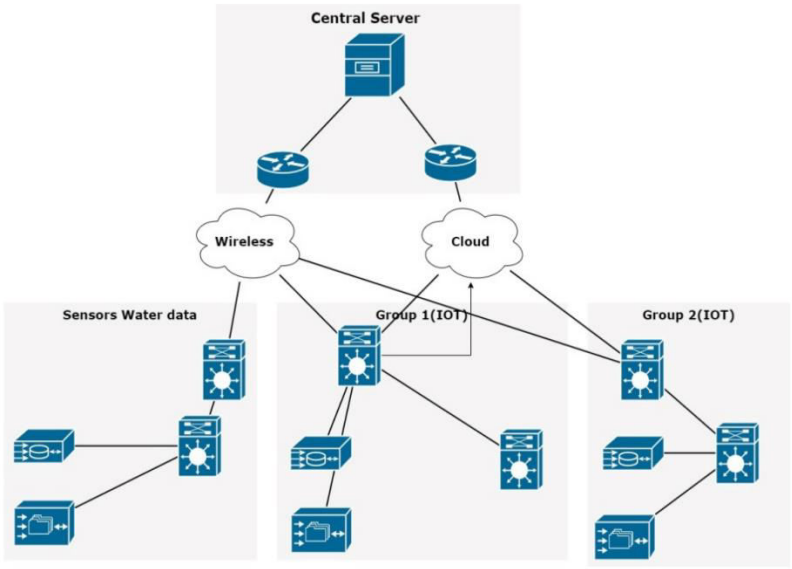


Fig 1: Smart water monitoring and IOT network

Back in 2013, an individual hacker managed to gain remote access to the Supervisory Control and Data Acquisition (SCADA) system that controlled the Bowman Avenue Dam located in Rye Brook, New York. Despite the fact that the attack had no operational consequences as the dam was offline at the time, it sparked concerns regarding the susceptibility of vital water infrastructure to cyber–physical attacks [4]. In 2014, two individuals attempted to poison the drinking water supply at the Lake Forest Reservoir in California. The attackers, with access to the reservoir site, poured a harmful substance into the water. However, their actions were detected before the contaminated water entered the distribution system. This incident emphasized the importance of rigorous security protocols, surveillance systems, and prompt incident response [5]. In 2019, a group of individuals attempted to poison a water reservoir in regional Victoria, Australia. They released a hazardous substance into the reservoir, targeting a specific community. The plot was detected early, and swift action prevented the contamination from reaching the water supply, underscoring the importance of robust monitoring systems and rapid response protocols [6]. In 2023, an attack on the Nova Kachovka Dam, located in the southern territory of Ukraine, currently occupied by Russia, was recorded. It is one of the biggest industrial and ecological disasters in Europe for decades. It is still impossible to say whether the dam collapsed because it was deliberately targeted or if the breach could have been caused by structural failure [7].

2. LITERATURE SURVEY

2.1 Industrial Control Systems and PLC-Based Anomaly Detection

Anomaly detection in industrial control systems (ICS) has gained significant attention due to increasing cybersecurity threats. Fujita et al. [8] developed a system toolset using open-source OpenPLC by extracting information from programmable logic controller (PLC) programs. Their work highlighted limitations in conventional classification-based approaches for sensor anomaly detection, emphasizing that continuous sensor data requires regression-based techniques to effectively handle complex attack patterns.

Wei Y, Law AW-K et al. [9] proposed a Combined Anomaly Detection Framework (CADF) for securing digital twins of water treatment systems. Their framework utilized a PLC-based whitelist mechanism to detect actuator anomalies, while employing natural gradient boosting (NGB) and probabilistic deep learning techniques to detect sensor-based attacks, demonstrating a comprehensive and robust security approach.

2.2 Data-Driven and Statistical Approaches for Infrastructure Monitoring

Data-driven anomaly detection methods have been widely applied in infrastructure systems, particularly for water management. Rousso et al. [10] conducted a systematic review focusing on pressure-based data for leak detection and localization, highlighting the growing adoption of anomaly detection techniques in water distribution networks.

Tashman and Gorder et al. [13] introduced a two-level anomaly detection system for monitoring remote water hand-pumps. Their approach involved modeling normal water usage behavior using approximate variational Bayesian inference to derive probabilistic distributions, enabling proactive maintenance through early fault detection.

Foster et al. [14] provided critical insights into the real-world implications of system failures, reporting that approximately 33% of water points in Ethiopia were non-functional. Their findings emphasized the importance of reliable anomaly detection systems to prevent service disruptions and associated public health risks.

2.3 Machine Learning and Deep Learning-Based Techniques

Machine learning and deep learning approaches have significantly advanced anomaly detection capabilities. Jones et al. [11] proposed an SVM-like approach that models system behavior using Signal Temporal Logic (STL), providing interpretable descriptions of normal behavior. However, the method is limited when system behaviors cannot be concisely expressed using STL.

Goh et al. [12] developed an unsupervised deep learning approach using stacked Long Short-Term Memory (LSTM) networks to detect anomalies in the Secure Water Treatment (SWaT) dataset. While effective, their evaluation was limited to a single subsystem and a subset of attack scenarios.

Zhu et al. [16] introduced a hybrid model combining LSTM and Generative Adversarial Networks (GAN), leveraging LSTM's strength in temporal modeling and GAN's capability for feature extraction and data distribution modeling. Their approach utilized generator residuals and discriminator loss to identify anomalies, achieving high detection performance.

2.4 One-Class and Boundary-Based Anomaly Detection Methods

In scenarios where abnormal data is scarce, one-class learning techniques have been widely adopted. Scholkopf et al. [15] proposed the one-class Support Vector Machine (OC-SVM), which identifies anomalies by learning a boundary around normal data points. Similarly, Tax and Duin introduced Support Vector Data Description (SVDD), which encloses normal data within a hypersphere to detect deviations.

These methods have proven effective in various applications; however, their performance may be limited when dealing with highly dynamic or high-dimensional data, necessitating more advanced hybrid and deep learning approaches.

3. PROPOSED SYSTEM

The proposed methodology defines a structured and data-driven framework for securing water distribution systems and predicting operational parameters to ensure infrastructural integrity. The research follows a comprehensive analytical pipeline that begins with sensor-based data ingestion and advances through rigorous preprocessing, feature transformation, hybrid learning, and multi-output prediction stages. The overall architecture of the proposed framework provides a robust defense mechanism by integrating deep representation learning with ensemble-based decision-making. By utilizing a hybrid VQPTE approach, the methodology enables the effective detection of cyber-physical threats and the accurate estimation of system states even in the presence of noisy or inconsistent real-time data. The framework is designed to handle the complexities of industrial control systems, ensuring high reliability through comparative evaluation against multiple baseline models. The system supports both real-time individual feature testing and batch-level dataset analysis, making it a versatile tool for modern water utility management as shown in Fig. 3.

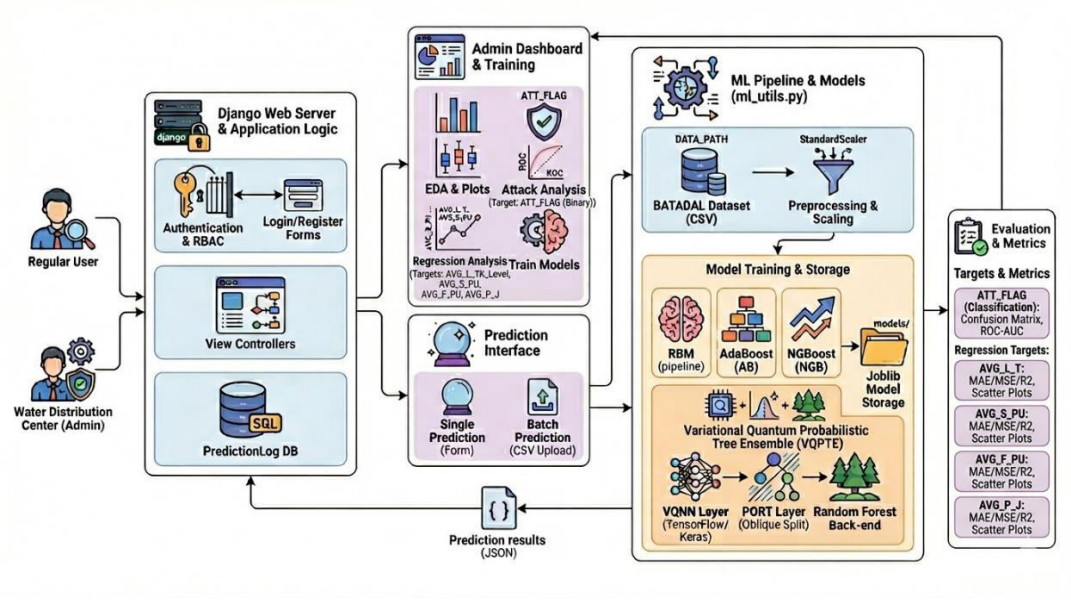


Fig. 3: Proposed system architecture

User Interface (Admin/User Interaction)

- Users interact with the system through a web-based graphical interface supporting both Water Distribution Center (Admin) and General User roles.
- Admin users are granted elevated privileges to upload datasets, perform preprocessing, conduct EDA, train models, and analyze system performance.
- General users can provide individual feature values or upload datasets to obtain real-time classification and regression predictions.
- All user-initiated actions are transmitted to the backend for processing, model inference, and result generation.

Raw Dataset Input

- Consists of comprehensive water distribution system data featuring sensor-based numerical and binary attributes.

- Includes vital system parameters such as tank water levels, pump flow rates, pump status, valve status, and junction pressures.
- Accounts for potential inconsistencies, noise, or variations inherent in real-time physical system behavior.
- Serves as the foundational input layer for both anomaly detection (security) and parameter prediction (operational) tasks.

Data Preprocessing Module

- Handles automated data cleaning by addressing inconsistencies and preparing structured inputs for the pipeline.
- Encodes categorical outputs, such as the ATT_FLAG, into numerical formats to ensure model compatibility.
- Applies feature scaling using standardization techniques to normalize numerical values across different sensor types.
- Produces a clean, normalized, and high-quality dataset suitable for training advanced machine learning models.

Feature Engineering and Representation

- Organizes raw sensor data into meaningful groups such as tank levels, flow rates, and pressure values.
- Constructs derived features, including average tank levels and pump statuses, to capture system-wide behavior.
- Ensures precise alignment and representation of features for both classification-based security tasks and regression-based estimation.
- Prepares optimized feature vectors that serve as the primary input for the learning models.

Data Splitting and Preparation

- Divides the processed dataset into distinct training and testing subsets to facilitate supervised learning.
- Maintains consistency in data distribution through controlled random splitting to prevent training bias.
- Ensures an unbiased evaluation of model performance by testing the system on previously unseen data.
- Prepares structured, multi-dimensional inputs specifically tailored for 1CA4RT

Baseline Machine Learning Models

- Implements established models, including RBM-based architectures, AdaBoost (AB), and Natural Gradient Boosting (NGB).
- Each baseline model independently learns patterns and relationships from the training data to provide a performance benchmark.

- Generates predictions for anomaly detection (classification) and system parameter estimation (regression).
- Enables a comparative analysis of model performance to validate the superiority of the proposed hybrid approach.

Hybrid Model (VQPTE)

- Utilizes VQNN for advanced feature extraction and the learning of latent representations from complex sensor data.
- Applies PORT-based transformations to structure extracted features for optimized tree-based learning.
- Integrates Random Forest using 1CA4RT-based principles to perform the final predictive decision-making.
- Enhances overall predictive performance by combining deep representation learning with the stability of ensemble methods.

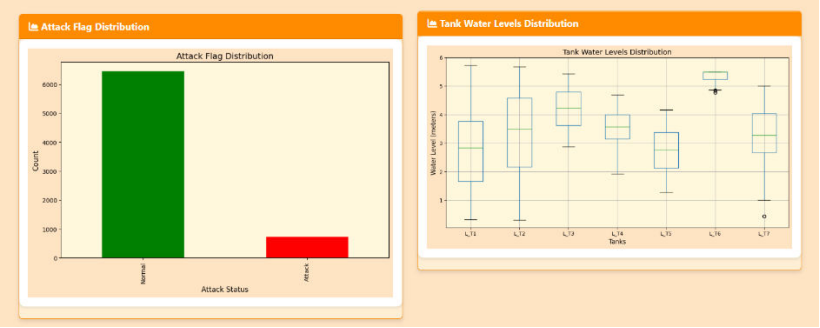
Prediction Output and Analysis

- Produces classification results, categorizing system states as Normal or Attack for real-time anomaly detection.
- Generates regression outputs for critical parameters, including AVG_L_T, AVG_S_PU, AVG_F_PU, and AVG_P_J.
- Supports flexible processing modes, allowing for single-input point predictions or batch processing from uploaded files.
- Displays all results through the user interface with intuitive visualizations for easy interpretation by operators.

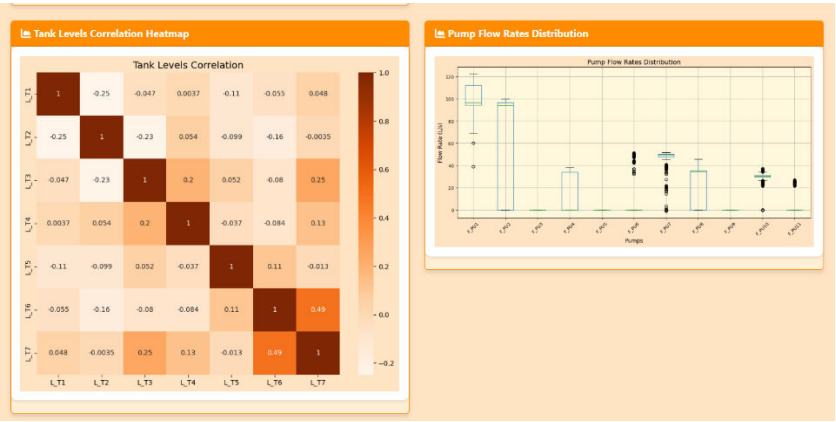
4. RESULTS DESCRIPTION

Fig. 5 (a) illustrates the attack flag distribution in the water distribution system, depicting the frequency of normal (0) and attack (1) conditions present in the dataset. It highlights the proportion between class labels 0 and 1, indicating class imbalance. The figure shows that normal instances (0) significantly dominate over attack instances (1). This imbalance reflects real-world anomaly detection scenarios where attack events are rare. The visualization provides a clear understanding of the target variable ATT_FLAG (0 = Normal, 1 = Attack).

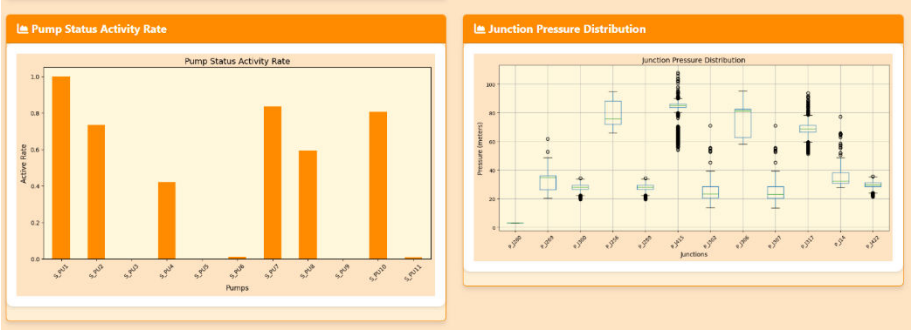
Fig. 5 (b) depicts the distribution of tank water levels for tanks L_T1, L_T2, L_T3, L_T4, L_T5, L_T6, and L_T7. It illustrates the variation in water levels measured in meters across seven tanks. The figure highlights differences in median values, interquartile ranges, and presence of outliers among the tanks. It enables comparison of tank behavior under different conditions. This analysis helps identify irregular fluctuations in tanks such as L_T3 and L_T6.



(a)



(b)



(c)

Fig. 5: EDA of water distribution system under attack and normal conditions:(a) Attack distribution, (b) tank level distribution, (c) tank correlation heatmap

Fig. 5 (c) illustrates the correlation heatmap of tank levels including L_T1, L_T2, L_T3, L_T4, L_T5, L_T6, and L_T7. It represents correlation coefficient values ranging from -1 to +1 between tank pairs. The figure highlights both positive and negative relationships among variables. It identifies moderate correlations such as between L_T6 and L_T7 (around 0.49). This analysis helps in understanding interdependencies among tanks. It also supports feature selection for model training.

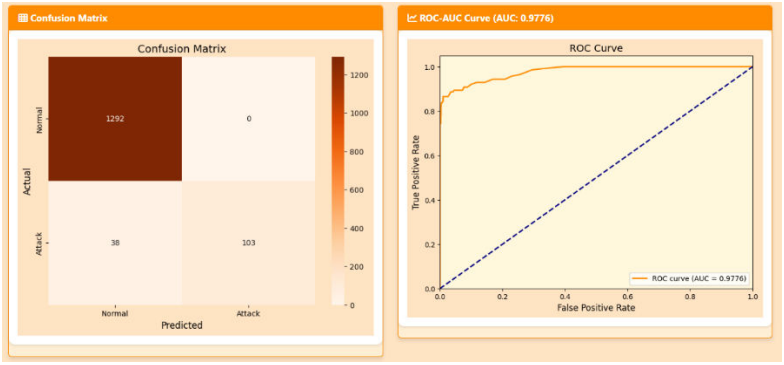


Fig. 6: Confusion Matrix & ROC curve obtained for Attack Type of VQPTE Models

Fig. 6 depicts the confusion matrix and ROC curve for the proposed VQPTE model in attack detection. The confusion matrix shows 1292 correctly classified normal instances, 0 false positives, 38 false negatives, and 103 correctly identified attack instances. This indicates significant improvement in detecting attack samples compared to other models. The ROC curve achieves a high AUC value of 0.9776, reflecting excellent classification performance. The figure demonstrates that the VQPTE model provides superior accuracy and strong discriminative power for anomaly detection.

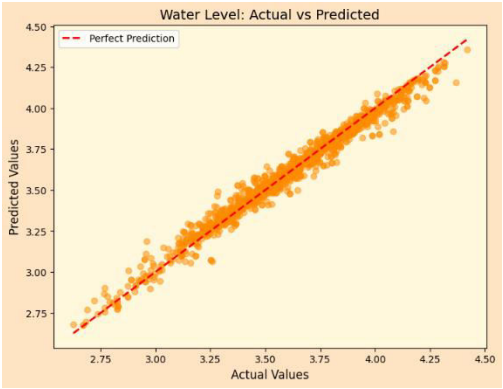


Fig. 7: Scatter plots obtained for water level of VQPTE models

Fig. 7 depicts the scatter plot of actual versus predicted water levels for the proposed VQPTE model. It shows a strong alignment of data points closely along the perfect prediction line. The predicted values match the actual values with minimal deviation across the entire range of approximately 2.7 to 4.5 meters. The tight clustering indicates very low prediction error and high model precision. This figure demonstrates that the VQPTE model achieves superior regression performance compared to other models.

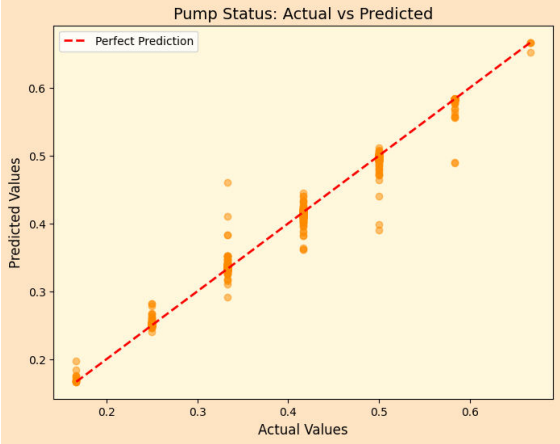


Fig. 8: Scatter plots obtained for pump status of VQPTE models

Fig. 8 depicts the scatter plot of actual versus predicted pump status values for the proposed VQPTE model. It shows a strong alignment of points closely along the perfect prediction line. The predicted values match the actual values with minimal deviation across the full range. The tight clustering indicates reduced prediction error and high precision. This figure demonstrates that the VQPTE model achieves superior performance in pump status prediction.

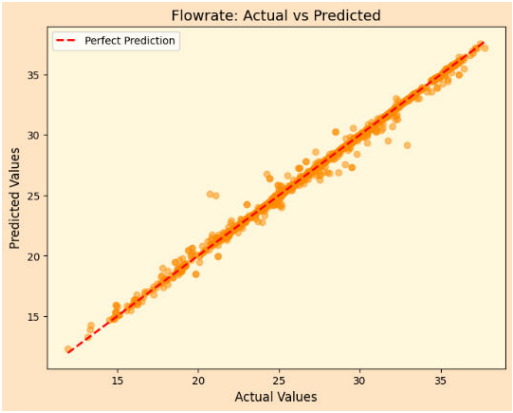


Fig. 9: Scatter plots obtained for flow rate of VQPTE models

Fig. 9 depicts the scatter plot of actual versus predicted flow rate values for the proposed VQPTE model. It shows a very tight clustering of points along the perfect prediction line. The predicted values closely match actual values across the entire range from approximately 12 to 38 L/s. Minimal deviation indicates very low prediction error and high model precision. This figure demonstrates that the VQPTE model achieves superior regression performance for flow rate prediction.

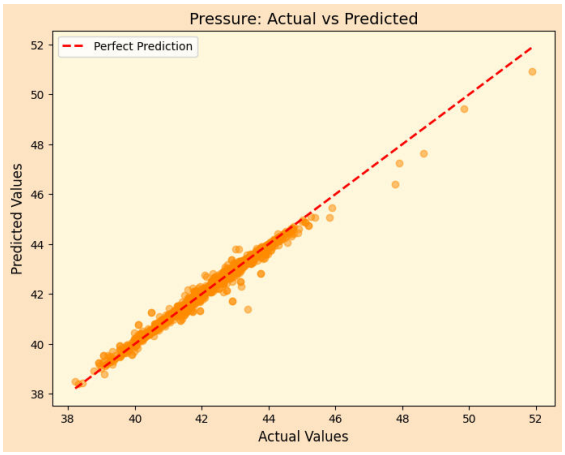


Fig. 10: Scatter plots obtained for pressure of VQPTE models

Fig. 10 depicts the scatter plot of actual versus predicted pressure values for the proposed VQPTE model. It shows a very tight clustering of points closely aligned with the perfect prediction line. The predicted values match actual values with minimal deviation across the entire range from approximately 38 to 52 meters. The strong linear alignment indicates very low prediction error and high precision. This figure demonstrates that the VQPTE model achieves superior regression performance for pressure prediction.

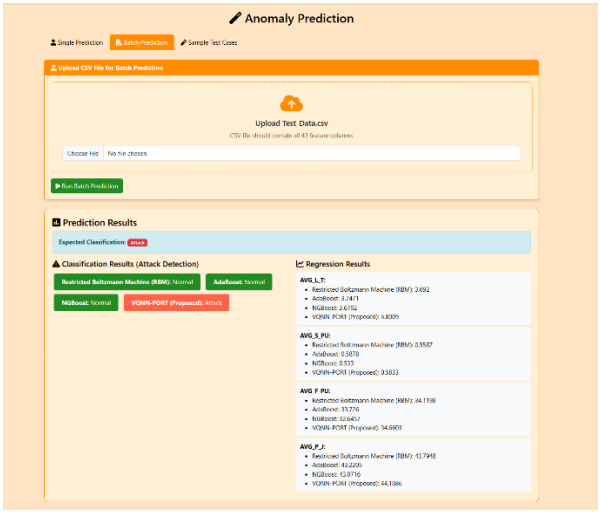


Fig. 11: Prediction interface for user interface

Fig. 11 illustrates the prediction interface of the Hydro Guard IDS system designed for anomaly detection and parameter estimation. It depicts the batch prediction functionality where users upload a test dataset containing multiple feature columns. The interface presents classification results indicating attack detection outcomes for models such as RBM, AB, NGB, and the proposed VQPTE model. It also displays regression outputs including predicted values for parameters such as average tank level (AVG_L_T), pump status (AVG_S_PU), flow rate (AVG_F_PU), and junction pressure (AVG_P_J). The figure highlights the integration of classification and regression modules within a unified user interface for real-time decision support.

COMPARATIVE ANALYSIS

Table 1 presents the classification performance of different models for the ATT_FLAG target variable. The VQNN-PORT model achieves the highest accuracy of 97.35%, precision of 97.42%, recall of 97.35%, and F1-score of 97.16%, along with a ROC-AUC of 0.9776. In comparison, AB achieves 93.09% accuracy and 0.8305 ROC-AUC, while NGB achieves 92.88% accuracy and 0.8866 ROC-AUC. RBM shows lower performance with 90.09% accuracy and a ROC-AUC of 0.6206. The results clearly indicate that the proposed model significantly outperforms the existing models. As shown in Table 3, VQNN-PORT provides the most accurate classification results.

Table 1 ATT_FLAG – Model Performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC
RBM	90.09	81.28	90.09	85.46	0.6206
AB	93.09	93.27	93.09	91.46	0.8305
NGB	92.88	93.40	92.88	91.00	0.8866
VQNN-PORT	97.35	97.42	97.35	97.16	0.9776

Table 2 illustrates the regression performance for predicting AVG_L_T. The VQNN-PORT model achieves the lowest MAE of 0.0333, MSE of 0.0023, RMSE of 0.0475, and the highest R^2 score of 0.9758. AdaBoost performs well with an R^2 score of 0.8788 but has higher errors compared to the proposed model. NGB shows moderate performance with an R^2 score of 0.5764, while RBM performs poorly with an R^2 score of 0.3485. The error values for RBM are significantly higher than other models. As observed in Table 4, VQNN-PORT provides superior prediction accuracy for AVG_L_T.

Table 2 AVG_L_T – Model Performance

Model	MAE	MSE	RMSE	R^2 Score
RBM	0.1968	0.0608	0.2466	0.3485
AB	0.0864	0.0113	0.1064	0.8788
NGB	0.1591	0.0396	0.1989	0.5764
VQNN-PORT	0.0333	0.0023	0.0475	0.9758

Table 3 shows the regression performance for the AVG_S_PU target variable. The VQNN-PORT model achieves an MAE of 0.0026, MSE of 0.0001, RMSE of 0.0091, and an R^2 score of 0.9913, indicating near-perfect performance. AdaBoost achieves an R^2 score of 0.9218, while RBM and NGB achieve 0.8520 and

0.8218 respectively. The error values for VQNN-PORT are significantly lower compared to all other models. This demonstrates the model's strong capability in predicting pump status. As presented in Table 5, VQNN-PORT outperforms all models for AVG_S_PU prediction.

Table 3 AVG_S_PU – Model Performance

Model	MAE	MSE	RMSE	R^2 Score
RBM	0.0272	0.0014	0.0376	0.8520
AB	0.0217	0.0007	0.0273	0.9218
NGB	0.0325	0.0017	0.0412	0.8218
VQNN-PORT	0.0026	0.0001	0.0091	0.9913

Table 4 presents the regression performance for the AVG_F_PU target variable. The VQNN-PORT model achieves an MAE of 0.1440, MSE of 0.1275, RMSE of 0.3571, and an R^2 score of 0.9954. AdaBoost achieves an R^2 score of 0.9359, while RBM and NGB achieve 0.8180 and 0.8067 respectively. RBM and NGB show significantly higher error values, such as RMSE values of 2.2499 and 2.3189. The results indicate that the proposed model handles flow prediction more effectively. As shown in Table 6, VQNN-PORT provides the best performance for AVG_F_PU.

Table 4 AVG_F_PU – Model Performance

Model	MAE	MSE	RMSE	R^2 Score
RBM	1.5837	5.0621	2.2499	0.8180
AB	1.0978	1.7826	1.3351	0.9359
NGB	1.8327	5.3771	2.3189	0.8067
VQNN-PORT	0.1440	0.1275	0.3571	0.9954

Table 5 illustrates the regression performance for the AVG_P_J target variable. The VQNN-PORT model achieves an MAE of 0.1015, MSE of 0.0305, RMSE of 0.1746, and an R^2 score of 0.9826. AdaBoost achieves an R^2 score of 0.8603, while NGB and RBM achieve 0.6423 and 0.5468 respectively. The error values for RBM are significantly higher, with an RMSE of 0.8909. The results show that the proposed model provides highly accurate pressure predictions. As observed in Table 7, VQNN-PORT consistently outperforms existing models.

Table 5 AVG_P_J – Model Performance

Model	MAE	MSE	RMSE	R^2 Score
RBM	0.6531	0.7937	0.8909	0.5468
AB	0.4011	0.2447	0.4947	0.8603
NGB	0.6034	0.6265	0.7915	0.6423
VQNN-PORT	0.1015	0.0305	0.1746	0.9826

5. Conclusion

The intelligent water distribution monitoring system was successfully designed and implemented using a combination of Django and machine learning techniques. The system integrates multiple existing models including RBM, AdaBoost, and NGB along with the proposed VQNN-PORT model for both classification and regression tasks. Experimental results demonstrate significant performance improvements achieved by the proposed model. For the ATT_FLAG classification task, VQNN-PORT achieved an accuracy of 97.35%, outperforming RBM (90.09%), AdaBoost (93.09%), and NGB (92.88%), along with a high ROC-AUC of 0.9776 indicating strong classification capability. In regression tasks, the proposed model consistently achieved superior performance across all target variables. For AVG_L_T, it achieved an R^2 score of 0.9758 compared to 0.8788 (AdaBoost) and 0.3485 (RBM). For AVG_S_ PU, it achieved an R^2 score of 0.9913, significantly higher than other models. For AVG_F_PU, the model achieved an R^2 score of 0.9954 with very low error values, and for AVG_P_J, it achieved an R^2 score of 0.9826, outperforming all existing models. These results confirm that the proposed VQNN-PORT model provides improved accuracy, reduced error, and better generalization capability. Overall, the system enables reliable anomaly detection and accurate prediction of water distribution parameters, making it suitable for real-time monitoring applications.

REFERENCES

[1] Mac Kenzie, W.R.; Hoxie, N.J.; Proctor, M.E.; Gradus, M.S.; Blair, K.A.; Peterson, D.E.; Kazmierczak, J.J.; Addiss, D.G.; Fox, K.R.; Rose, J.B. A massive outbreak in Milwaukee of Cryptosporidium infection transmitted through the public water supply. N. Engl. J. Med. 1994, 331, 161–167.

[2] Hrudey, S.E.; Hrudey, E.J. Safe Drinking Water: Lessons from Recent Outbreaks in Affluent Nations; IWA Publishing: London, UK, 2004.

[3] Al-Ansari, N.; Al-Hadithi, M.; Knutsson, S. Terrorism and Security of Water Supplies: The Threat of Water Terrorism. J. Water Resour. Protect. 2013, 5, 449–461.

[4] U.S. Department of Justice. Bowman Avenue Dam: A Case Study in the Complexity of Responding to Cyber-Physical Attacks. 2016.

[5] Smarsh, D.J. Water Utility Incident Response Planning: Ensuring Effective Emergency Response to Contamination Events. In Proceedings of the American Water Works Association (AWWA) Water Quality Technology Conference, New Orleans, LA, USA, 16–20 November 2014.

[6] The Age. Terrorism Plot to Poison Water Supply: Inside the Ringwood Conspiracy. 2019.

[7] CNN. Here are the Key Theories on What Caused Ukraine's Catastrophic Dam Collapse. 2023.

[8] Fujita, S.; Hata, K.; Mochizuki, A.; Sawada, K.; Shin, S.; Hosokawa, S. OpenPLC based control system testbed for PLC whitelisting system. Artif. Life Robot. 2021, 26, 149–154.

[9] Wei Y, Law AW-K, Yang C, Tang D. Combined Anomaly Detection Framework for Digital Twins of Water Treatment Facilities. Water. 2022; 14(7):1001. https://doi.org/10.3390/w14071001

[10] B.Z. Rousso et al.Smart water networks: a systematic review of applications using high-frequency pressure and acoustic sensors in real water distribution systemsJ. Clean. Prod.(2023)

[11] A. Jones, Z. Kong, and C. Belta, Anomaly detection in cyber-physical systems: A formal methods approach, in Proc. of the IEEE Conf. on Decision and Control (CDC), 2018, pp. 848–853.

[12] Y. Harada, Y. Yamagata, O. Mizuno, and E.-H. Choi, Log-based anomaly detection of CPS using a statistical method, in Proc. of the IEEE Int. Workshop on Enterprise & Service-Driven Computing for Cyber-Physical Systems (IWESEP), 2017, pp. 1–6.

[13] Tashman, Z.; Gorder, C.; Parthasarathy, S.; Nasr-Azadani, M.M.; Webre, R. Anomaly Detection System for Water Networks in Northern Ethiopia Using Bayesian Inference. Sustainability 2020, 12, 2897. https://doi.org/10.3390/su12072897

[14] Foster, T.; Furey, S.; Banks, B.; Willetts, J. Functionality of handpump water supplies: A review of data from sub-Saharan Africa and the Asia-Pacific region. Int. J. Water Resour. Dev. 2019, 1–15.

[15] Scholkopf, B.; Smola, A.J.; Bach, F. Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond; MIT Press: Cambridge, MA, USA, 2022.