

Autoencoder-based anomaly detection in water cyber-physical systems

Sara Tahiri, Mouad Choukhairi, Youssef Fakhri, Amnai Mohamed

Computer Science Research Laboratory (LaRI), Department of Computer Science, Faculty of Sciences, Ibn Tofail University, Kenitra, Morocco

Article Info

Article history:

Received Jun 9, 2025

Revised Jul 24, 2026

Accepted Aug 12, 2026

Keywords:

Autoencoder

Big data analytics

Cyber-physical system

Internet of things

Machine learning

Secure water treatment

Water distribution systems

ABSTRACT

Cyber-physical systems (CPS) are at the core of enabling services in the critical infrastructures, such as a smart water network, hence the need for effective anomaly detection to ensure operational safety and security. In this paper proposes deep water anomaly detection (DeepWAD), a big data-based multiple purpose anomaly detection tool that leverages deep learning, supports big data, and internet of things (IoT) data collection and analysis. In a unified processing pipeline, it estimates and contrasts three kinds of autoencoders, viz adversarial autoencoder (AAE), variational autoencoder (VAE), and classical autoencoder (CAE). These models are then applied to a practical water treatment system, namely the secure water treatment (SWaT) dataset. Using reconstruction errors, DeepWAD analyzes time-series data generated by IoT sensors in order to discover anomalies including, for example, equipment malfunctions, sensor errors, and cyber threats. The framework also demonstrates the performance of various architectures in terms of data complexity, training consistency, and reconstruction accuracy. Due to its generality, DeepWAD can also be applied in other CPS domains such as the energy grid or industrial control systems. It serves as a decision-support tool to select the most appropriate anomaly detection model depending on system constraints and detection requirements.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Sara Tahiri

Computer Science Research Laboratory, Department of Computer Science, Faculty of Sciences

Ibn Tofail University

Kenitra, Morocco

Email: sara.tahiri@uit.ac.ma

1. INTRODUCTION

Recently, for the operation of essential infrastructures such as water treatment and distribution networks, cyber-physical systems (CPS) have been taking increasingly significant roles [1]–[4]. The networks of such systems are becoming more and more tightly integrated, and sensors-based monitoring, real-time data acquisition, and automatic control play a very important role [5], [6]. But this added complexity and interconnections also bring about new challenges, such as security, reliability, and anomaly detection [7], [8].

Modern water systems incorporate internet of things (IoT) technologies to monitor various parameters such as water flow, pressure, chemical concentration, and operational status [9]. These IoT-enabled infrastructures generate large volumes of time-series data that require scalable and intelligent processing to detect abnormal behavior [10], [11]. Anomalies may arise from system faults, sensor malfunctions, or intentional cyberattacks [12]. Undetected, such anomalies can lead to significant operational disruptions, water quality degradation, or security breaches [13], [14]. In dynamic and data-rich situations, traditional anomaly detection

techniques that rely on rule-based systems or basic statistical thresholds frequently fail. In contrast, deep learning approaches, particularly those based on autoencoder (AE) architectures, offer a promising solution [15], [16]. These models are capable of learning complex patterns from normal operating data and identifying deviations without requiring labeled anomaly data [17].

Detecting anomalies in CPS has emerged as a vital research focus due to the growing dependence on automated and interconnected systems, such as those used in water treatment, energy distribution, and industrial control mechanisms. Historically, anomaly detection has depended on rule-based techniques, thresholding, and statistical methods [18], [19]. Although these strategies provide ease of use, they frequently fall short in terms of flexibility and scalability necessary for contemporary CPS, particularly when managing high-dimensional, real-time sensor data. With the introduction of IoT technologies in CPS, the amount and diversity of data collected have surged, necessitating the development of intelligent, data-driven approaches [20], [21]. Machine learning methods, especially deep learning models, have garnered interest for their capacity to capture intricate nonlinear patterns in time-series data without the need for labeled anomaly examples [22].

AE have been commonly utilized in this domain, particularly for unsupervised anomaly detection. Adversarial autoencoder (AAE) is a neural network designed to recreate its input. When trained on data representative of normal operations, it aims to reduce reconstruction errors for expected behaviors [23], [24]. Consequently, high reconstruction errors from new inputs could signify anomalies. Classical autoencoder (CAE) have demonstrated encouraging performance in industrial settings, including manufacturing systems, smart buildings, and supervisory control and data acquisition (SCADA) networks. To enhance generalization and resilience, variational autoencoder (VAE) brings a probabilistic latent space into the equation [21]. VAEs are better equipped to manage uncertainty and demonstrate greater robustness to data variations, which is especially advantageous in the dynamic environments of CPS. AAE builds on the CAE concept by adding a generative adversarial component that helps to regularize the latent space [22]. This aids the model in learning more organized representations, potentially increasing the distinction between normal and abnormal patterns. Techniques based on AAEs have been implemented in network intrusion detection and industrial quality control, yielding promising outcomes. The secure water treatment (SWaT) dataset is widely recognized as a standard benchmark for assessing anomaly detection techniques in CPS. It replicates a water treatment procedure and features labeled attack scenarios, making it particularly suitable for verifying unsupervised models [22], [23]. Previous studies employing the SWaT dataset have concentrated on specific model types, yet few have provided systematic evaluations across various AE architectures within a unified experimental framework. This study aims to fill that void by performing a comparative analysis of CAE, VAE, and AAE models within the framework of IoT-enabled CPS, utilizing consistent evaluation metrics and processing protocols to evaluate their relative efficacy in identifying anomalies [25].

In this context, this study propose deep water anomaly detection (DeepWAD), a modular and comparative framework for unsupervised anomaly detection. DeepWAD integrates real-time IoT data acquisition, big data preprocessing, and deep learning through three types of AE models: CAE, VAE, and AAE. Rather than combining the outputs of these models, DeepWAD evaluates them independently to identify the most suitable architecture for CPS anomaly detection based on detection accuracy, robustness, and training efficiency. Using the SWaT dataset, the framework is verified, a widely used benchmark that simulates real-world operations of a water treatment plant. By applying and comparing the three models within a consistent processing pipeline, DeepWAD contributes valuable insights for practitioners seeking to enhance anomaly detection capabilities in CPS environments.

The rest of the paper is organized as follows. Section 1 provides the introduction and related works by reviewing the most recent literature on the use of AEs for CPS anomaly detection. Section 2 provides a detailed presentation of the methodology, where the system architecture, CAE, VAE, and AAE models are employed, and the data processing pipeline is presented. Section 3 describes results and discussion, canvassing model performance in terms of reconstruction loss, anomaly scoring, and receiver operating characteristic (ROC) curves. Finally, section 4 concludes the study, summarizing key findings and identifying directions for future research and real-world deployment of the DeepWAD framework.

2. METHOD

This section outlines the method used for identifying anomalies in a smart water treatment system by employing deep learning techniques and data from IoT sensors. The suggested framework, named

DeepWAD, as shown in Figure 1 consists of four main components: i) gathering data from the SWaT system, ii) data preprocessing and feature transformation, iii) training three different AE models (CAE, VAE, and AAE), and iv) evaluation and detection through reconstruction error analysis.

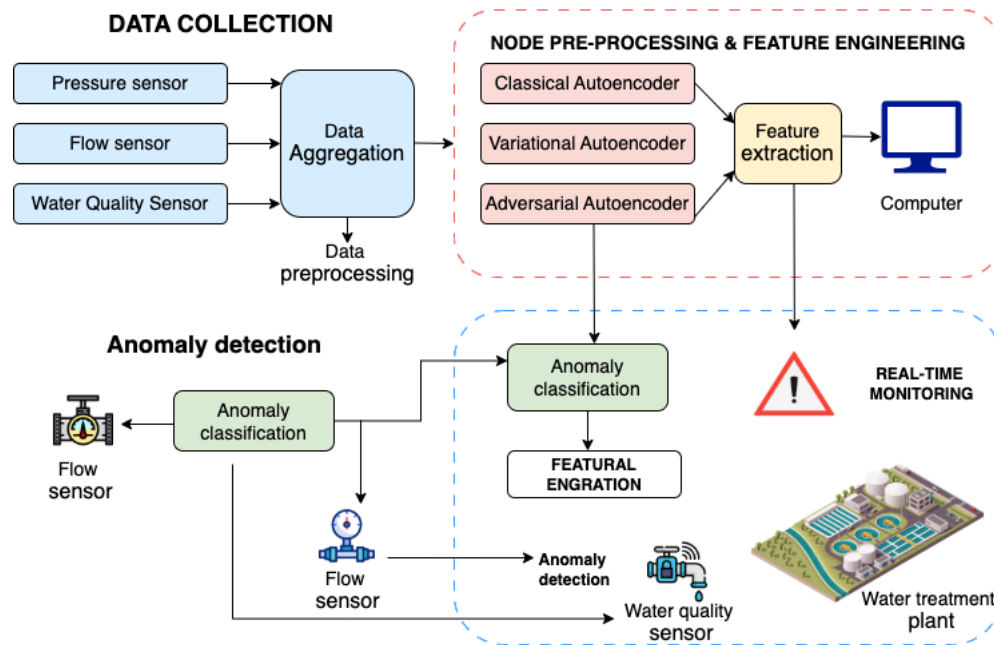


Figure 1. DeepWAD framework

Each phase is designed to replicate a realistic industrial setting where training is conducted exclusively on normal operational data. The DeepWAD framework facilitates comprehensive anomaly detection within a CPS environment that utilizes IoT technology. It comprises several components: data gathering layer, where real-time sensor data is collected from the SWaT system, monitoring factors like flow rates, tank levels, pump operations, and chemical concentrations; data processing layer, where incoming data is cleaned, normalized, and segmented into time windows using a sliding window technique, preserving temporal patterns for sequence modeling; model layer, where each of the three AEs (CAE, VAE, and AAE) is trained independently on the processed data. This modular design allows DeepWAD to evaluate the performance of each architecture individually, and the detection layer, where anomalies are detected by evaluating the reconstruction error during testing. Thresholds are used to flag abnormal windows, enabling real-time anomaly identification in the smart water treatment context.

The SWaT dataset, which contains 11 days of time-series data from sensors and actuators in a simulated water treatment plant, is used as the foundation for training and testing. The first 7 days contain only normal behavior and are used for training, while the remaining 4 days include multiple types of attack scenarios and serve as the test set. To prepare the data for input to the deep learning models, the following preprocessing steps are applied as summarized in Table 1.

Table 1. Data preprocessing steps applied to the SWaT dataset

Step	Description
Data cleaning	Remove missing values and corrupted sensor readings
Feature normalization	Apply min-max scaling to bring all features to a [0, 1] range
Time windowing	Segment the continuous time-series into overlapping windows (e.g., 100 steps)
Label assignment	Labels (normal/attack) are added only for evaluation, not for training

Each AE models (CAE, VAE, and AAE) is trained independently using only the normal part of the SWaT dataset. The models are optimized using the Adam optimizer over 25 epochs, with mean squared error

(MSE) as the primary reconstruction loss. The training process aims to minimize this reconstruction loss for normal sequences. During inference, each time series segment is passed through the trained model. Anomaly scores are computed based on reconstruction error, and a threshold is applied to classify the segment as normal or anomalous. The complete procedure is outlined in Algorithm 1.

Algorithm 1: Training and inference procedure for anomaly detection

Require: Normal training data X_{train} , test data X_{test} , window size w

Ensure: Anomaly score vector S

1: **Preprocessing:**

2: Normalize features in X_{train} and X_{test}

3: Segment X_{train} into windows of size w

4: **Model training:**

5: **for** epoch = 1 to N **do**

6: Feed training windows into the AE

7: Compute reconstruction loss $L = \|x - \hat{x}\|^2$

8: Backpropagate and update weights

9: **end for**

10: **Anomaly detection:**

11: Segment X_{test} into windows

12: **for** each test window x **do**

13: Reconstruct $\hat{x}$ using trained model

14: Compute anomaly score $s = \|x - \hat{x}\|^2$

15: Append s to S

16: **end for**

17: **return** S

Each AE model's performance is evaluated using a number of quantitative metrics. The model's capacity to differentiate between normal and anomalous windows is measured by the area under the curve (AUC), which is the most significant. The classification performance is further assessed using precision, recall, and F1-score following the application of a decision threshold. To determine the ideal threshold that optimizes the F1-score, a grid search is performed on the validation set. This threshold is then applied to the anomaly scores of the test data for final classification. The threshold-based classification process is outlined in Algorithm 2.

Algorithm 2: Threshold-based anomaly classification

Require: Anomaly score vector S , Ground truth labels Y , Threshold search space T

Ensure: Classification labels $\hat{Y}$, Optimal threshold t^*

1: Initialize best F1-score $F1^* = 0$

2: **for** each threshold t in T **do**

3: Assign predicted label $\hat{y}_i = 1$ if $s_i > t$, else 0

4: Compute precision, recall, F1-score

5: **if** F1-score $> F1^*$ **then**

6: Update $F1^* \leftarrow$ F1-score

7: Update $t^* \leftarrow t$

8: **end if**

9: **end for**

10: **Final Classification:**

11: **for** each s_i in S **do**

12: $\hat{y}_i = 1$ if $s_i > t^*$, else 0

13: **end for**

14: **return** $\hat{Y}, t^*$

3. RESULTS AND DISCUSSION

This section presents the experimental results obtained from applying the proposed DeepWAD framework to the SWaT dataset for anomaly detection. The evaluation focuses on three AEs-based CAE, VAE, and AAE which are assessed based on their training dynamics, reconstruction accuracy, anomaly scoring behavior, and classification effectiveness. Each model was trained exclusively on normal operational data for 25 epochs, and their training and validation loss curves were analyzed to understand convergence patterns and stability. Figure 2 presents the training and validation loss curves of the three evaluated architectures. As shown in Figure 2(a), the CAE achieved rapid and stable convergence with minimal signs of overfitting, indicating

efficient learning of normal patterns. The VAE as shown in Figure 2(b), due to its stochastic latent representation, exhibited moderate variability during training, while the AAE as shown in Figure 2(c) encountered instability stemming from adversarial interactions between its encoder and discriminator components.

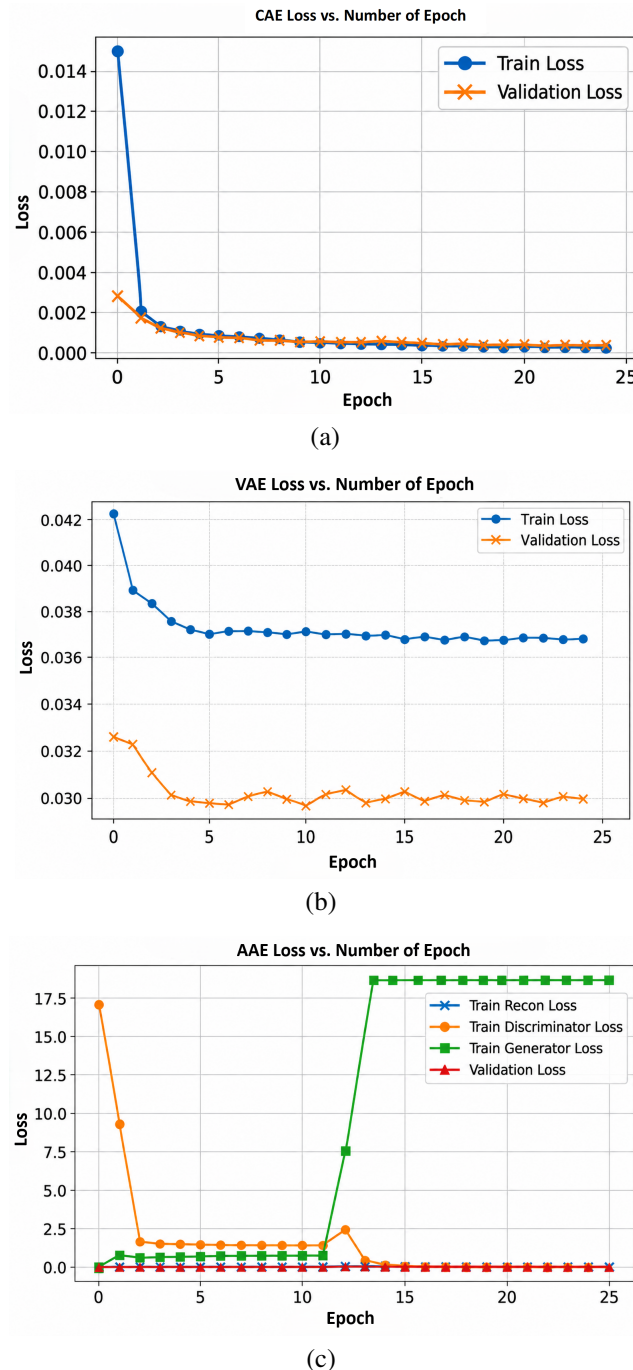


Figure 2. Training and validation loss curves for: (a) CAE, (b) VAE, and (c) AAE

To further evaluate model performance, anomaly scores were computed using the mean squared reconstruction error across the test dataset. Figure 3 illustrates the distribution of these scores, revealing that CAE provided a clear separation between normal and anomalous samples, with tightly clustered normal scores and a broader spread for attack data. The VAE benefited from its latent variability, producing a smoother and

more distinguishable distribution, whereas the AAE generated noisier and less distinct score patterns. Figure 3 presents the anomaly-score distributions obtained from the reconstruction errors. Figure 3(a) corresponds to the CAE model, Figure 3(b) corresponds to the VAE model, and Figure 3(c) correspond to the AAE model.

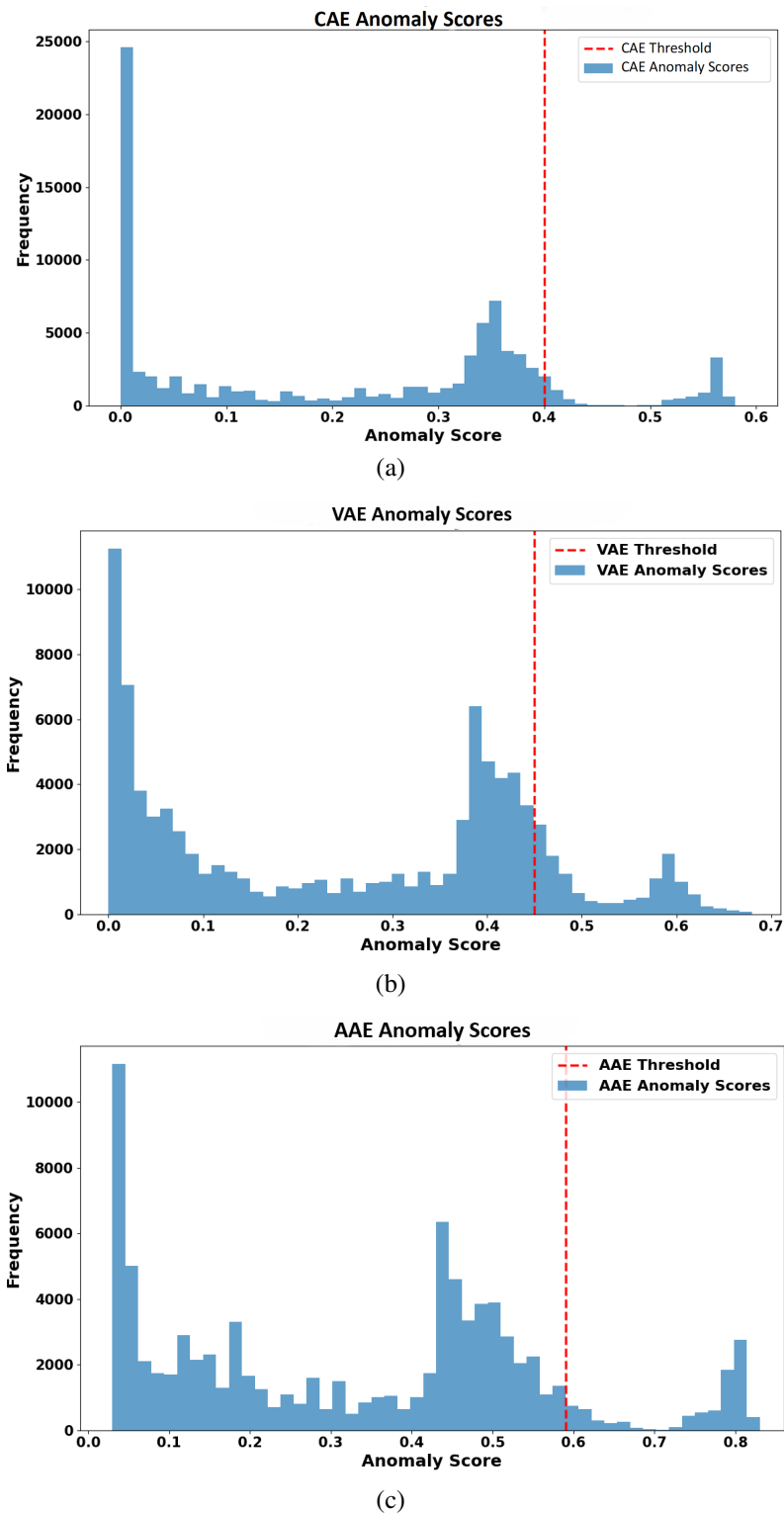


Figure 3. Anomaly score distributions based on reconstruction error for: (a) CAE, (b) VAE, and (c) AAE

Lastly, the models' classification capabilities were assessed through ROC curves and their corresponding AUC values, as depicted in Figure 4 and summarized in Table 2. These metrics quantitatively reflect each model's ability to discriminate between normal and anomalous data, providing a comprehensive comparison of their detection effectiveness within the DeepWAD framework. ROC curves used to assess performance of the anomaly detection for each AE architecture of the three models are illustrated in Figure 4.

Specifically, Figure 4(a) corresponds to the CAE, Figure 4 (b) to the VAE, and Figure 4(c) to the AAE. These curves enable a direct visual comparison of the trade-off between true positive rate and false positive rate across the different architectures. Such comparison facilitates the assessment of relative anomaly detection performance among the three models.

Table 2. AUC scores for each AE model evaluated within the DeepWAD framework

Model	AUC score
CAE	0.787
VAE	0.791
AAE	0.782

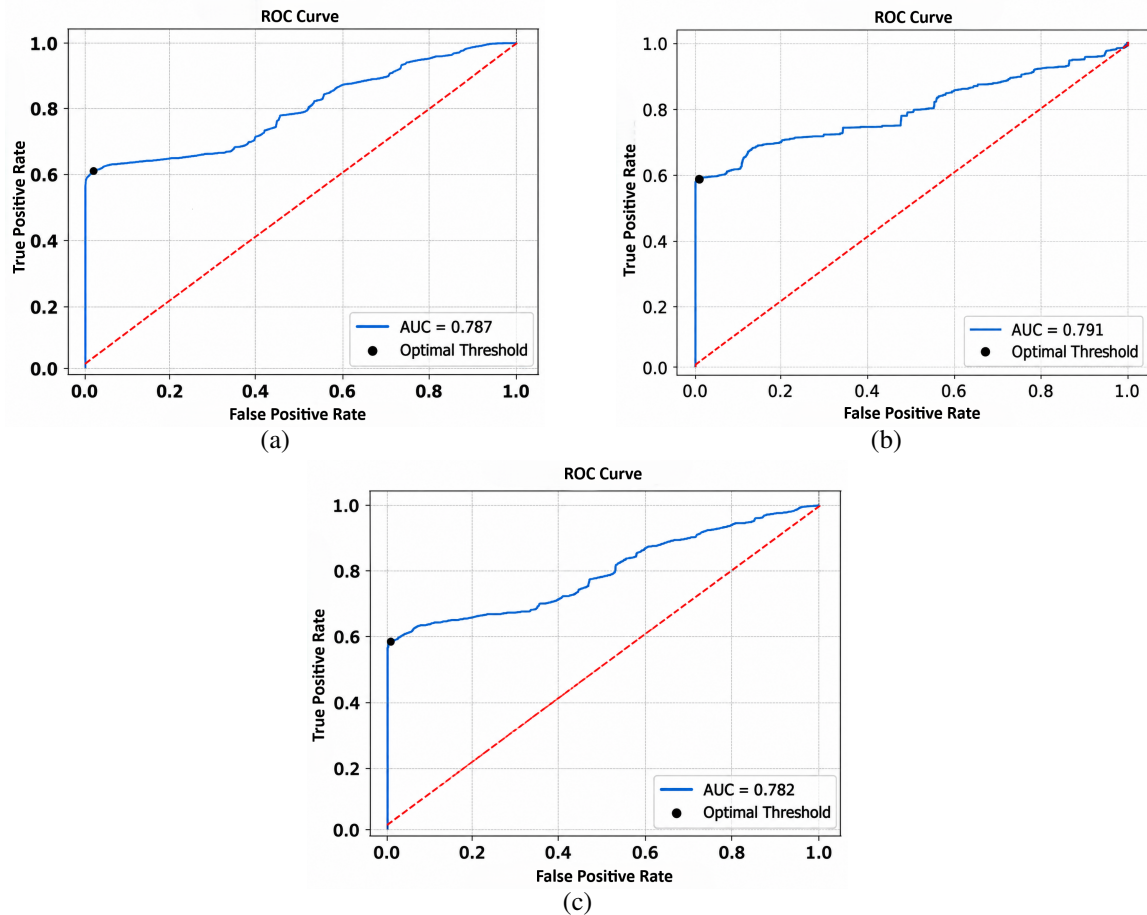


Figure 4. ROC curves illustrating anomaly detection performance for: (a) CAE, (b) VAE, and (c) AAE

Table 3 summarizes the key characteristics and observations for each AE model based on performance, stability, and suitability. The obtained results are consistent with previous studies on reconstruction-based anomaly detection in CPS. Similar to the findings reported by Malhotra *et al.* [16] and Fährmann *et al.* [22], AE-based models demonstrate strong capability in learning normal operational behavior without requiring labeled attack data. The proposed DeepWAD framework achieves competitive AUC scores while maintaining a computationally efficient architecture, making it suitable for real-time CPS deployment.

Table 3. Comparative summary of AE models used in the DeepWAD framework

Criteria	CAE	VAE	AAE
Training stability	High	Moderate	Low (adversarial dynamics)
Convergence speed	Fast	Moderate	Slower
Detection accuracy (AUC)	0.787	0.791	0.782
Generalization	Moderate	High	High
Robustness to noise	Moderate	High	Variable
Interpretability	Easy	Medium	Low
Computational cost	Low	Medium	High
Best use case	Real-time, resource-constrained environments	Complex, dynamic systems	Structured anomaly detection, feature-rich data

4. CONCLUSION

This work introduced a deep learning approach, DeepWAD, for anomaly detection in cyber-physical infrastructure systems in the water treatment domain. Three AEs (CAE, VAE, and AAE) are applied on time series sensor data for operational anomaly detection. The framework was evaluated on the SWaT dataset, and results indicated that all considered models can accurately detect anomalies, and VAE achieves a good trade-off between detection and robustness. While the CAE showed its robust convergence and efficiency, VAE achieved the best effectiveness in anomaly discrimination via its probabilistic property, and AAE had to be carefully tuned. The core detection engine was chosen to be the VAE model. DeepWAD is also modular, and other variants of AE can be used, depending on specific requirements. This work will address real-time deployment, be it latency and scalability optimization, or hybrid models/attention augmentation, as future work to further refine the detection accuracy.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Sara Tahiri	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓			✓
Mouad Choukhairi	✓	✓			✓	✓		✓		✓				
Youssef Fakhri		✓		✓	✓		✓			✓		✓	✓	
Amnai Mohamed					✓					✓		✓	✓	

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal Analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project Administration

Fu : Funding Acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The SWaT dataset analyzed in this study is provided by iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design (SUTD) at <https://www.sutd.edu.sg/itrust/itrust-labs/datasets/dataset-characteristics/swat/>. Access is subject to iTrust's terms of usage. Researchers may request access at <https://www.sutd.edu.sg/itrust/request-for-datasets/>.

REFERENCES

- [1] A. Jones, Z. Kong, and C. Belta, "Anomaly detection in cyber-physical systems: a formal methods approach," in *53rd IEEE Conference on Decision and Control*, Dec. 2014, pp. 848–853, doi: 10.1109/CDC.2014.7039487.
- [2] D. Abshari and M. Sridhar, "A survey of anomaly detection in cyber-physical systems," Feb. 2026, *arXiv:2502.13256v1*.
- [3] A. A. Cook, G. Misirli, and Z. Fan, "Anomaly detection for IoT time-series data: a survey," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6481–6494, Jul. 2020, doi: 10.1109/JIOT.2019.2958185.
- [4] Q. Xu, S. Ali, and T. Yue, "Digital twin-based anomaly detection in cyber-physical systems," in *2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST)*, Apr. 2021, pp. 205–216, doi: 10.1109/ICST49551.2021.00031.
- [5] R. Geetha and T. Thilagam, "A review on the effectiveness of machine learning and deep learning algorithms for cyber security," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 2861–2879, Jun. 2021, doi: 10.1007/s11831-020-09478-2.
- [6] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, "Deep learning for anomaly detection: a review," *ACM Computing Surveys*, vol. 54, no. 2, pp. 1–38, Mar. 2022, doi: 10.1145/3439950.
- [7] B. Sharma, L. Sharma, and C. Lal, "Anomaly detection techniques using deep learning in IoT: a survey," in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, Dec. 2019, pp. 146–149, doi: 10.1109/ICCIKE47802.2019.9004362.
- [8] R. Kabore, A. Kouassi, R. N'goran, O. Asseu, Y. Kermarrec, and P. Lenca, "Review of anomaly detection systems in industrial control systems using deep feature learning approach," *Engineering*, vol. 13, no. 1, pp. 30–44, 2021, doi: 10.4236/eng.2021.131003.
- [9] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: a survey," *Internet of Things*, vol. 19, Aug. 2022, doi: 10.1016/j.iot.2022.100568.
- [10] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: progress and opportunities," *ACM Computing Surveys*, vol. 54, no. 5, pp. 1–36, Jun. 2022, doi: 10.1145/3453155.
- [11] S. Zia, N. Bibi, S. Alhazmi, N. Muhammad, and A. Alhazmi, "Enhanced anomaly detection in IoT through transformer-based adversarial perturbations model," *Electronics*, vol. 14, no. 6, Mar. 2025, doi: 10.3390/electronics14061094.
- [12] G. Koutroulis, B. Mutlu, and R. Kern, "A causality-inspired approach for anomaly detection in a water treatment system," *Sensors*, vol. 23, no. 1, Dec. 2022, doi: 10.3390/s23010257.
- [13] Z. Dong, K. Liu, D. Han, Y. Cao, and Y. Xia, "Reconstruction-based multi-scale anomaly detection for cyber-physical systems," in *2022 4th International Conference on Industrial Artificial Intelligence (IAI)*, Aug. 2022, pp. 1–6, doi: 10.1109/IAI55780.2022.9976844.
- [14] M. Catillo, A. Pecchia, and U. Villano, "CPS-GUARD: intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders," *Computers & Security*, vol. 129, Jun. 2023, doi: 10.1016/j.cose.2023.103210.
- [15] M. R. G. Raman, W. Dong, and A. Mathur, "Deep autoencoders as anomaly detectors: method and case study in a distributed water treatment plant," *Computers & Security*, vol. 99, Dec. 2020, doi: 10.1016/j.cose.2020.102055.
- [16] P. Malhotra, A. Ramakrishnan, G. Anand, L. Vig, P. Agarwal, and G. Shroff, "LSTM-based encoder-decoder for multi-sensor anomaly detection," in *ICML 2016 Anomaly Detection Workshop*, 2016.
- [17] R. Alguliyev, L. Sukhostat, and A. Mammadov, "Anomaly detection in cyber-physical systems based on BiGRU-VAE," in *2022 IEEE 16th International Conference on Application of Information and Communication Technologies (AICT)*, Oct. 2022, pp. 1–5, doi: 10.1109/AICT55583.2022.10013581.
- [18] C. Wang, B. Wang, H. Liu, and H. Qu, "Anomaly detection for industrial control system based on autoencoder neural network," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–10, Aug. 2020, doi: 10.1155/2020/8897926.
- [19] J. Goh, S. Adepu, K. N. Junejo, and A. Mathur, "A dataset to support research in the design of secure water treatment systems," in *Critical Information Infrastructures Security (CRITIS 2016)*, Cham, Switzerland: Springer, 2017, pp. 88–99, doi: 10.1007/978-3-319-71368-7_8.
- [20] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *2018 Workshop on Cyber-Physical Systems Security and Privacy*, Jan. 2018, pp. 72–83, doi: 10.1145/3264888.3264896.
- [21] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *Science*, vol. 313, no. 5786, pp. 504–507, Jul. 2006, doi: 10.1126/science.1127647.
- [22] D. Fährmann, N. Damer, F. Kirchbuchner, and A. Kuijper, "Lightweight long short-term memory variational auto-encoder for multivariate time series anomaly detection in industrial control systems," *Sensors*, vol. 22, no. 8, Apr. 2022, doi: 10.3390/s22082886.
- [23] H. Sun, Y. Huang, L. Han, C. Fu, H. Liu, and X. Long, "MTS-DVGAN: anomaly detection in cyber-physical systems using a dual variational generative adversarial network," *Computers & Security*, vol. 139, Apr. 2024, doi: 10.1016/j.cose.2023.103570.
- [24] V. Krysanova and M. White, "Advances in water resources assessment with SWAT—an overview," *Hydrological Sciences Journal*, vol. 60, no. 5, pp. 771–783, Apr. 2015, doi: 10.1080/02626667.2015.1029482.
- [25] J. G. Arnold *et al.*, "SWAT: model use, calibration, and validation," *Transactions of the ASABE*, vol. 55, no. 4, pp. 1491–1508, 2012, doi: 10.13031/2013.42256.

BIOGRAPHIES OF AUTHORS



Sara Tahiri obtained her bachelor's degree (B.Sc.) in Mathematics and Computer Science in 2018 and her master's degree in Big Data and Cloud Computing in 2020, both from the Faculty of Sciences, Ibn Tofail University, Kenitra, Morocco. Currently, she is pursuing a Ph.D. at the Computer Science Research Laboratory (LaRI), focusing on big data, machine learning, deep learning, and IoT. She can be contacted at email: sara.tahiri@uit.ac.ma.



Mouad Choukhairi    received his bachelor's degree (B.Sc.) in 2018 in Mathematics and Computer Science and his master's degree in Big Data and Cloud Computing in 2020 from Faculty of Sciences, Ibn Tofail University, Kenitra, Morocco. He is currently a Ph.D. student in Computer Science Research Laboratory (LaRI) in the field of cybersecurity, IDS, big data, machine learning, deep learning, and IoT. He can be contacted at email: mouad.choukhairi@uit.ac.ma.



Youssef Fakhri    obtained a Bachelor of Science degree in Electronics and a Diploma of Advanced Scientific Studies (DESA) in Computer Science and Telecommunications from the Faculty of Sciences of Rabat (Mohammed V University - Agdal, Rabat, Morocco), in 2001 and 2003 respectively. He obtained a Ph.D. Thesis on November 17, 2007 from the University Mohammed V - Agdal, Rabat, Morocco in collaboration with the Polytechnic University of Catalonia (UPC), Spain. His research topics are information theory, signal processing, wireless telecommunications (WSN), and routing protocols. He is now a professor of higher education in Computer Science at the Faculty of Sciences, Ibn Tofail University, Kenitra. He is a member of Research Laboratory in Computer Science (LaRI). He can be contacted at email: fakhri@uit.ac.ma.



Amnai Mohamed    obtained his bachelor's degree in IEEE (Computer Science, Electronics, Electricity and Automation) at the University Moulay Ismail in the city of Errachidia. Then he obtained his master's degree in 2007, his Ph.D. in 2011 in Telecommunications and Computer Science at the University Ibn Tofail of Kenitra, Morocco. His current research interests include QoS in wireless communication, ad hoc networks and telecommunication traffic. He is also a member of Research Laboratory in Computer Science (LaRI) and he is currently working as a Computer Science professor at the University Ibn Tofail of Kenitra, Morocco. He can be contacted at email: mohamed.amnai@uit.ac.ma.