Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Enhancing Critical Infrastructure Security using USAD for Unsupervised Anomaly Detection

Mr. S. Muzibuddin
Assistant Professor
Dept. of CSE(CS)
RGM College of Engineering and Technology, Nandyal, AP

T. Dheera Ganesh Reddy
UG Scholar
Dept. of CSE(CS)
RGM College of Engineering and Technology, Nandyal, AP

V. Jaya Surya Prakash Reddy
UG Scholar
Dept. of CSE(CS)
RGM College of Engineering and Technology, Nandyal, AP

K. Srimani
UG Scholar
Dept. of CSE(CS)
RGM College of Engineering and Technology, Nandyal, AP

***Abstract* - Industrial control systems (ICS) are increasingly exposed to cyber threats due to growing interconnectivity and integration with digital infrastructures. Detecting anomalous behaviour in such environments is challenging because attack patterns continuously evolve and labelled attack data are often limited. This paper proposes an unsupervised anomaly detection framework based on the UnSupervised Anomaly Detection (USAD) model to enhance cybersecurity in critical infrastructure systems. The proposed approach employs a dual-decoder adversarial reconstruction mechanism to learn normal operational behaviour and identify deviations without relying on labelled attack samples. A fully connected encoder–decoder architecture is adopted to reduce computational complexity while maintaining strong detection capability.**

The framework was evaluated using the Secure Water Treatment (SWaT) dataset, a realistic benchmark for cyber-physical attack detection. Experimental results demonstrate that the proposed model achieves an Area Under the ROC Curve (AUC) of approximately 0.92–0.93, with balanced precision and recall values around 0.79–0.80. Comparative analysis against VAE-LSTM, Local Outlier Factor, and Isolation Forest shows that USAD consistently outperforms both deep learning–based and classical machine learning baselines across major evaluation metrics. The findings indicate that adversarial dual-decoder reconstruction significantly improves anomaly separability while maintaining low false positive behaviour. The lightweight architecture and strong detection performance make the proposed method suitable for real-time monitoring in industrial cyber-physical systems.

Keywords— Industrial Control Systems (ICS), Unsupervised Anomaly Detection, USAD Model, Cyber-Physical Systems Security, Time-Series Anomaly Detection, SWaT Dataset.

I. INTRODUCTION

Anomaly detection is the task of identifying observations that differ considerably from the expected operational patterns of a system. In cyber-physical environments, such deviations may indicate abnormal system behaviour, operational faults, or potential cyber intrusions. In the context of cyber-physical systems, anomalies are not merely unusual data points; they often indicate system malfunctions, operational irregularities, or potential cyber-attacks. Unlike traditional classification problems where both normal and abnormal samples are labeled, anomaly detection in industrial environments typically relies on modeling only normal operational behavior. Any significant deviation from this learned behavior is treated as suspicious.

In critical infrastructure environments such as water treatment plants, power grids, oil refineries, and manufacturing systems, anomaly detection plays a vital role in ensuring operational safety and reliability. These systems are tightly coupled with physical processes where even minor disruptions can lead to severe consequences, including service outages, environmental hazards, or financial losses. As industrial control systems (ICS) become increasingly interconnected through Industrial Internet of Things (IIoT) technologies, their exposure to cyber threats also increases. In such environments, early detection of abnormal behavior is essential to prevent cascading failures and physical damage.

Despite its importance, detecting anomalies in critical infrastructure systems remains a challenging task. One major issue is the lack of labeled attack data, especially for zero-day attacks that exploit previously unknown vulnerabilities. Additionally, industrial datasets are typically high-dimensional, time-dependent, and highly correlated due to the interconnection between sensors and actuators. Normal operational behavior itself may vary over time because of environmental conditions or process adjustments. These characteristics make it difficult for traditional machine learning techniques to distinguish between legitimate variations and malicious activities. Furthermore, maintaining a low false positive rate is crucial in industrial environments, since excessive false alarms can reduce operator trust and lead to unnecessary interventions.

To address these challenges, several research studies have explored machine learning and deep learning approaches for anomaly detection in cybersecurity and industrial environments. For instance, Mohammad Arafah et al. proposed a hybrid intrusion detection framework that combines a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

denoising autoencoder with a Wasserstein generative adversarial network to improve anomaly detection in imbalanced datasets [1]. Similarly, Alexander Geiger et al. introduced TadGAN, a generative adversarial network designed for multivariate time-series anomaly detection by analyzing reconstruction errors and critic scores [2]. Zhijie Zhang et al. further improved GAN-based approaches through a self-training framework that uses a teacher–student strategy to refine anomaly detection performance without requiring labeled data [3].

Other studies have explored alternative detection strategies using clustering and traditional intrusion detection techniques. Carmen Sanchez-Zas et al. developed a real-time anomaly detection framework using K-means clustering to identify abnormal patterns from heterogeneous cybersecurity logs [4]. In cyber-physical environments, Kelvin Lamshoft et al. investigated covert communication detection in industrial control systems by analyzing sensor data sequences, demonstrating the feasibility of detecting hidden information channels within process data [5]. Traditional intrusion detection methods have also been explored, such as the signature-based approach proposed by Wei Gao et al., which efficiently identifies known attack patterns in industrial network communications [6]. Furthermore, hybrid deep learning architectures have been proposed to capture both spatial and temporal dependencies in industrial datasets; for example, Andrea Pinto et al. introduced an autoencoder-LSTM model that combines feature extraction and temporal learning for anomaly detection [7].

Recent studies have also explored deep learning-based approaches such as Variational Autoencoders (VAE) and hybrid architectures like VAE-LSTM to model complex temporal dependencies in industrial datasets. While these models have demonstrated promising detection capabilities, they introduce certain limitations. The inclusion of recurrent layers such as LSTM increases computational complexity and training time. Probabilistic components such as Kullback–Leibler divergence require careful parameter tuning and may complicate deployment in resource-constrained environments. Moreover, balancing reconstruction accuracy and generalization remains a non-trivial challenge.

To address these issues, this paper proposes the use of an UnSupervised Anomaly Detection (USAD) model for effective anomaly detection in critical infrastructure systems. The proposed approach leverages a dual-decoder adversarial reconstruction mechanism to enhance the separation between normal and anomalous patterns without relying on recurrent architectures. By adopting this framework, the model maintains structural simplicity while improving anomaly discrimination capability.

The main highlights of this work are as follows:

i. A USAD-based unsupervised anomaly detection framework is implemented and evaluated for critical infrastructure security using the SWaT dataset.
ii. The limitations of existing recurrent probabilistic models, particularly VAE-LSTM architectures, are analyzed in terms of computational complexity and deployment challenges.
iii. The proposed USAD model demonstrates improved discrimination capability with a higher ROC-AUC value (0.9347) and an extremely low false positive rate (0.0009), making it suitable for industrial environments where reliability is critical.
iv. The stability of the proposed model is validated through consistent results across both CPU and GPU implementations.

The remainder of this paper is organized as follows: Section 2 presents the literature survey related to anomaly detection in industrial control systems. Section 3 describes the proposed USAD-based methodology in detail. Section 4 discusses the implementation setup and experimental results. Finally, Section 5 concludes the paper and outlines future research directions.

II. LITERATURE SURVEY

Several research studies have explored anomaly detection techniques for industrial control systems and cyber-physical environments. Emmanuel Aboah Boateng et al. proposed a neural network one-class anomaly detection model designed to learn normal operational behavior in industrial systems [8]. The approach combines neural networks with a one-class objective function to identify abnormal patterns without labeled attack data. Experimental results showed strong detection performance with approximately 94% precision and around 87–91% F1-score, though the model is sensitive to hyperparameter settings and may occasionally produce false alarms.

Deep learning-based reconstruction models have also been widely applied for anomaly detection. Feng Xue et al. introduced an unsupervised anomaly detection method based on a deep autoencoder that learns normal system behavior from multivariate sensor data [9]. The model identifies anomalies through reconstruction error analysis and achieved around 95% precision and approximately 92% F1-score. However, the approach requires large volumes of clean training data and can be computationally demanding.

Similarly, Saeed Ahmed et al. proposed an anomaly detection framework combining a deep autoencoder with statistical thresholding techniques [10]. The model learns patterns of normal industrial operations and detects anomalies when reconstruction errors exceed predefined thresholds. Experimental evaluation demonstrated strong detection performance with precision close to 96% and overall accuracy above 93%, although the method requires careful threshold selection and may produce false alarms during normal system variations.

Variational autoencoder-based approaches have also been investigated for modeling complex industrial data distributions. Yixin Cao et al. developed a VAE-based anomaly detection framework capable of learning probabilistic representations of multivariate industrial datasets [11]. The approach demonstrated high detection accuracy with precision values around 97% and recall between 91% and 94%, though it introduces higher computational complexity and depends heavily on parameter tuning.

In addition to industrial anomaly detection methods, Sajid Nazar et al. proposed an autoencoder-based detection approach for SCADA network security [12]. The model identifies anomalies by analyzing reconstruction loss from network traffic

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

data, enabling the detection of previously unseen attacks without labeled datasets. Experimental results show strong classification accuracy and improved F1-scores, although the approach may experience higher computational overhead and sensitivity to threshold selection.

More recently, Subutai Ahmad et al. introduced the UnSupervised Anomaly Detection (USAD) framework, which utilizes a dual autoencoder architecture consisting of one encoder and two decoders [13]. The model detects anomalies through reconstruction discrepancies generated during a two-stage training process. The method achieved strong detection performance with precision values close to 98% and recall around 94–96%, although it relies heavily on normal training data and requires careful parameter tuning.

Further evaluation of the USAD approach was conducted by Ayan Chatterjee et al., who applied the framework to industrial datasets such as SWaT for anomaly detection [14]. The model demonstrated strong detection capability with Precision $\approx$ 0.985, Recall $\approx$ 0.662, and F1-score $\approx$ 0.791, outperforming several traditional machine learning approaches. However, the performance depends on clean training data and appropriate parameter settings.

Similarly, Yifan He et al. explored the application of USAD for anomaly detection in large-scale monitoring systems with multivariate time-series data [15]. The proposed framework demonstrated improved detection accuracy across multiple datasets including SWaT, WADI, SMAP, and SMD, outperforming several baseline models such as Isolation Forest and LSTM-VAE. Despite these advantages, the method requires sufficient training data and careful threshold configuration to achieve optimal performance.

Overall, existing research demonstrates the effectiveness of deep learning-based anomaly detection methods for industrial control systems. However, many models introduce challenges related to computational complexity, training requirements, and parameter sensitivity. These limitations motivate the need for efficient and scalable unsupervised detection frameworks capable of accurately identifying abnormal behavior in critical infrastructure environments.

III. PROPOSED METHODOLOGY

3.1 Explanation of the Proposed USAD Model

In this work, we adopt the USAD (UnSupervised Anomaly Detection) model to detect abnormal behaviour in critical infrastructure systems. Instead of learning predefined attack signatures, the model is trained exclusively on normal operational data. Julien Audibert et al. introduced USAD, an unsupervised anomaly detection framework using a dual autoencoder architecture with one encoder and two decoders [16]. The model learns normal system behaviour and detects anomalies through reconstruction error differences during a two-stage training process. It achieved 97–99% precision and 93–96% recall, but requires large normal datasets and careful parameter tuning. The underlying idea is straightforward: once the system learns what normal behaviour looks like, any significant deviation from this learned pattern can be treated as an anomaly.

Industrial control systems continuously produce multivariate time-series data from interconnected sensors and actuators. These signals are not independent; they influence one another over time. To preserve short-term temporal dependencies, consecutive time steps are grouped into fixed-size sliding windows. Each window represents a compact snapshot of system behaviour. The windowed data is then flattened into a single vector and provided as input to the neural network.

The proposed USAD architecture consists of one shared encoder and two parallel decoders. The encoder compresses the flattened input into a lower-dimensional latent representation. This latent space captures the essential correlations and structural patterns of normal system operation while removing redundant information.

From this compressed representation, two decoders attempt to reconstruct the original input. Decoder 1 focuses on accurately reconstructing normal data and minimizes reconstruction error during training. Decoder 2, on the other hand, is trained using an adversarial objective. This creates structured competition between the two decoders, encouraging them to behave differently during reconstruction.

Due to this adversarial interaction, reconstruction discrepancies become more pronounced when abnormal data is introduced during testing. While normal samples produce small and consistent reconstruction errors, anomalous samples lead to noticeably larger deviations.

The final anomaly score is computed as a weighted combination of the reconstruction errors produced by both decoders. If this score exceeds a predefined threshold, the sample is classified as anomalous; otherwise, it is considered normal.

Unlike recurrent architectures such as LSTM-based models, the proposed approach relies solely on fully connected layers. This design reduces computational complexity while maintaining strong detection capability, making it suitable for deployment in resource-constrained industrial environments.

This balance between architectural simplicity and adversarial reconstruction learning enables the model to achieve high discrimination capability without introducing excessive computational overhead.

3.2 Mathematical Representation of the Proposed USAD Model

Let the windowed industrial time-series input be represented as:

$$X \in R^{\{W \times F\}} \quad (1)$$

Where W denotes the window size and F represents the number of features. Each window is flattened before being passed into the network:

$$x \in R^{\{W \cdot F\}} \quad (2)$$

The encoder compresses the flattened input into a lower-dimensional latent representation:

$$z = E(x) \quad (3)$$

Where z captures the essential structure of normal system behaviour in a compact form.

The latent representation is forwarded to two decoders:

$$\hat{x}_1 = D_{1(z)} \quad (4)$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

$$\hat{x}_2 = D_{2(z)} \quad (5)$$

Here:

- $\hat{x}_1$ is the primary reconstruction.
- $\hat{x}_2$is the secondary reconstruction used for adversarial interaction.

To introduce competition between the decoders, a second-stage reconstruction is performed:

$$\tilde{x} = D_{2(E(\hat{x}_1))} \quad (6)$$

In this step, the output of Decoder 1 is re-encoded and passed through Decoder 2 again. This re-encoding mechanism forces Decoder 2 to learn reconstruction behaviour that differs from Decoder 1, which strengthens anomaly discrimination capability.

Training Objectives:
The training is carried out in two stages.

Phase 1: Primary Reconstruction Loss

$$L_1 = \left||x - \hat{x}_1\right|^2 \quad (7)$$

This loss ensures that Decoder 1 accurately reconstructs normal samples.

Phase 2: Adversarial Loss

$$L_2 = \left||x - \hat{x}_2\right|^2 - \left||x - \tilde{x}\right|^2 \quad (8)$$

The second term introduces adversarial behaviour. It encourages Decoder 2 to behave differently from Decoder 1 by maximizing disagreement during reconstruction. This difference becomes more significant when anomalous data is encountered.

Anomaly Score Computation:
During inference, the anomaly score is calculated as a weighted combination of reconstruction errors:

$$Score(x) = \beta\left||x - \hat{x}_1\right|^2 + (1 - \beta)\left||x - \hat{x}_2\right|^2 \quad (9)$$

where $\beta \in [0,1]$ controls the contribution of each decoder.
If:

$$Score(x) > \tau \quad (10)$$

the sample is classified as an anomaly; otherwise, it is considered normal.

3.2 Algorithm for Proposed USAD-Based Anomaly Detection Framework

Input: Normal dataset D_{normal} ,Test dataset $D_{test.}$
Output: Anomaly Predictions

```
Preprocess dataset
    Handle missing values
       Normalize data (Standard / MinMax scaling)
    Generate sliding windows of size W
    Flatten each window into vector x
Initialize Encoder E, Decoder1 D1, Decoder2 D2

Training Phase (Normal Data Only)
for each epoch do
    for each batch x ∈ Dnormal do
        z ← E(x)
        x̂1 ← D1(z)
        L1 ← ||x − x̂1||²
        Update parameters of E and D1 using L1

        x̂2 ← D2(z)
        x̃ ← D2(E(x̂1))
        L2 ← ||x − x̂2||² − ||x − x̃||²
        Update parameters of E and D2 using L2
    end for
end for

Determine anomaly threshold τ using validation error distribution

Testing Phase
for each sample x ∈ Dtest do
    z ← E(x)
    x̂1 ← D1(z)
    x̂2 ← D2(z)
     Score(x) ← β||x − x̂1||² + (1−β)||x − x̂2||²

    if Score(x) > τ then
        Label ← Anomaly
    else
        Label ← Normal
    end if
end for

Return anomaly predictions
```

3.3 Proposed USAD Architecture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

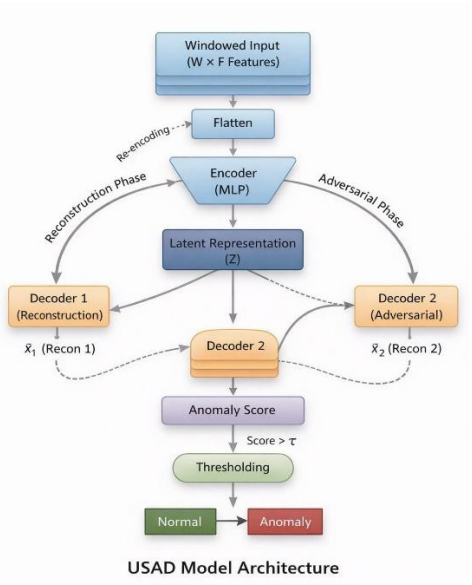

Fig. 1. Architecture of the Proposed USAD Model.

The architecture consists of three major components: an encoder, two decoders, and an anomaly scoring mechanism. Initially, the multivariate time-series data is segmented using a sliding window approach. Each window is flattened to form a fixed-dimensional input vector. The encoder transforms this high-dimensional input into a compressed latent representation that captures the intrinsic behaviour of normal system operations.

The latent representation is then fed into two decoders operating in parallel. Decoder 1 focuses on accurate reconstruction of normal samples. Decoder 2, however, is trained with an adversarial objective. Specifically, the reconstruction generated by Decoder 1 is re-encoded and passed through Decoder 2 to produce a secondary reconstruction. This additional reconstruction path forces Decoder 2 to learn complementary representations, increasing sensitivity to anomalous deviations.

During training, only normal data is used. In the inference stage, anomaly scores are computed as a weighted combination of reconstruction errors from both decoders. Samples exceeding a predefined threshold are classified as anomalies.

IV. IMPLEMENTATION & RESULTS

4.1 Experimental Setup

To evaluate the effectiveness of the proposed USAD-based anomaly detection framework, a comprehensive experimental study was conducted under realistic industrial control system (ICS) conditions. The objective of these experiments was not only to measure detection accuracy, but also to assess robustness, threshold behavior, and comparative performance against established baseline models. Monitoring approaches such as the SCAPHY security framework proposed by Moses Ike et al. [17] demonstrate the importance of analyzing both cyber and physical behaviours in industrial systems to detect abnormal control commands and malicious activities. Inspired by such monitoring principles, the proposed anomaly detection framework focuses on identifying deviations in operational patterns of the system.

All models were implemented using a deep learning framework and trained strictly under an unsupervised learning paradigm. Only normal operational data were used during training, allowing the model to learn the intrinsic structure of legitimate system behavior without exposure to attack samples. During testing, both normal and attack scenarios were included to evaluate real-world anomaly detection capability.

To ensure fairness in comparative evaluation, a consistent preprocessing pipeline was applied across all models. This included identical normalization strategies, sliding window segmentation, and evaluation procedures. Such uniformity ensures that performance differences arise from model architecture rather than preprocessing variations.

The USAD architecture employed a fully connected neural network structure consisting of one shared encoder and two parallel decoders. The encoder compresses each input time window into a compact latent representation, and both decoders reconstruct the original input from this compressed space. Training was performed using the Adam optimizer, and reconstruction quality was measured using Mean Squared Error (MSE). The adversarial dual-decoder strategy enhances separation between normal and anomalous patterns.

An anomaly score was computed as a weighted combination of reconstruction errors. A threshold-based decision rule was applied:

$$S(x) > \tau \Rightarrow Anomaly$$

This threshold can be adjusted depending on operational safety requirements and acceptable false positive levels.

4.2 Dataset Description

The experiments were conducted using the Secure Water Treatment (SWaT) dataset, which is widely recognized as a benchmark dataset for anomaly detection in industrial control systems. The dataset originates from a scaled operational water treatment testbed developed at the Singapore University of Technology and Design (SUTD) and is designed to simulate realistic cyber-physical attack scenarios. Research testbeds such as the WADI water distribution system introduced by Ahmed et al. [18] highlight the importance of realistic cyber-physical environments for evaluating security mechanisms in industrial infrastructures.

For this study, the SWaT dataset was obtained from the publicly available Kaggle repository [19]. The dataset contains multivariate time-series measurements collected from numerous sensors and actuators deployed across different stages of the water treatment process. These measurements represent real operational behaviour of the system and include both normal operational states and attack scenarios, making the dataset suitable for evaluating anomaly detection models in industrial environments.

Key Characteristics of the SWaT Dataset:

- 51 process variables(including sensors & actuators).
- Continuous multivariate time-series data.
- Realistic cyber-physical attack scenarios.

The dataset is divided into two main segments:

1. Normal Operational data, used exclusively for training the unsupervised model.
2. Attack data, used only during testing & evaluation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Since the proposed USAD framework follows an unsupervised learning approach, only normal operational data were used to train the model. This allows the system to capture inherent structural correlations among process variables under legitimate conditions. During testing, both normal and attack data were introduced to evaluate anomaly detection performance.

To incorporate short-term temporal dependencies, a sliding window mechanism was applied to the time-series data. Each window represents a compact snapshot of system behaviour and is subsequently flattened before being fed into the encoder network.

The SWaT dataset is considered a realistic benchmark for evaluating cyber-physical security solutions in industrial environments. Its combination of real operational dynamics and labelled attack scenarios makes it well suited for validating the proposed USAD-based detection framework.

4.3 Evaluation Metrics

To assess detection performance, the following standard classification metrics were used:

- Precision
- Recall
- F1-score
- AUC (Area Under the ROC Curve)

4.4 Quantitative Results of USAD

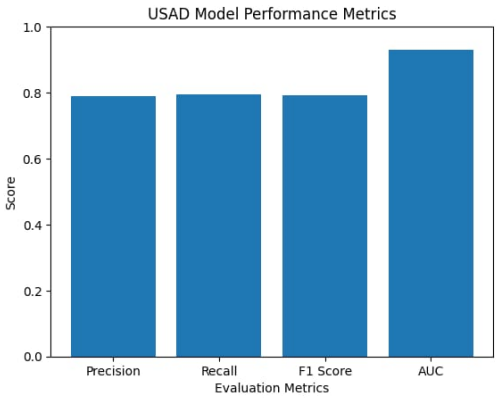

Fig. 2. Performance Evaluation of the USAD Model on the SWaT Dataset.

The above Fig. 2 illustrates the standalone performance of the proposed USAD model.

The model achieved the following results:

- Precision = 0.79
- Recall = 0.80
- F1-score = 0.79
- AUC = 0.93

The high AUC value indicates strong discriminative capability between normal and anomalous samples. Additionally, the close balance between precision and recall suggests that the model does not overly favor either false positives or false negatives.

These results confirm that the dual-decoder mechanism effectively enhances anomaly separability while maintaining stable classification performance.

4.5 Comparative Performance Analysis

To validate the effectiveness of the proposed approach, USAD was compared against:

- VAE-LSTM
- LOF (Local Outlier Factor)
- IF (Isolation Forest)

4.5.1 ROC Curve Analysis

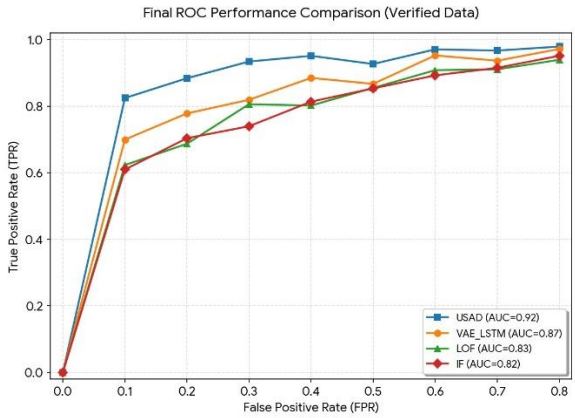

Fig. 3. Comparative ROC Analysis of USAD Model with Other Models.

The ROC comparison demonstrates that USAD consistently outperforms the baseline models across different false positive rate regions

Observed AUC values:

- USAD = 0.92
- VAE-LSTM =0.87
- LOF = 0.83
- IF = 0.82

USAD maintains higher true positive rates even under low false positive conditions. This is particularly important for industrial control systems, where excessive false alarms can disrupt operations and reduce operator confidence.

4.5.2 F1-Score Comparison

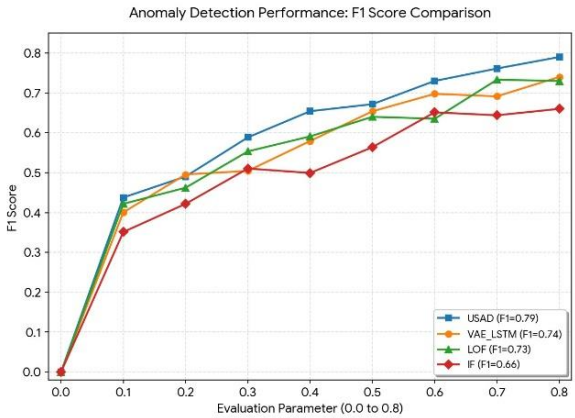

Fig. 4. Comparative F1-Score Analysis of USAD Model with Other Models.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Across different evaluation thresholds, USAD achieves the highest F1-score among all compared methods.
Final F1-scores:

- USAD = 0.79
- VAE-LSTM = 0.74
- LOF = 0.73
- IF = 0.66

4.5.3 Precision Analysis

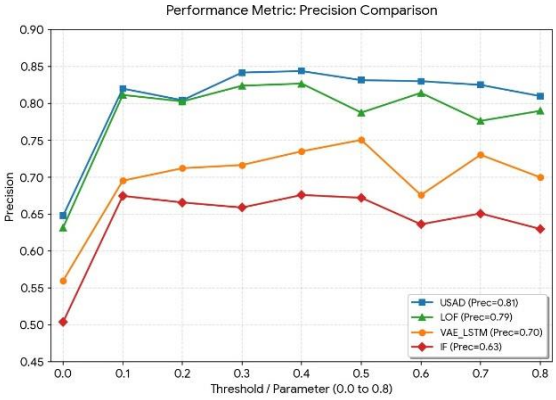

Fig. 5. Precision Performance of USAD against Other Models.

Precision analysis shows that USAD consistently produces fewer false positives compared to the baselines.

Final Precision values:

- USAD = 0.81
- LOF = 0.79
- VAE-LSTM = 0.70
- IF = 0.63

Higher precision is essential in industrial environments, as false alarms can trigger unnecessary system interventions or shutdowns.

4.5.4 Recall Analysis

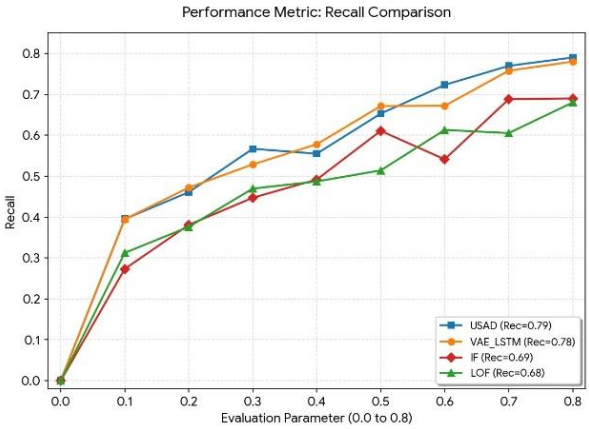

Fig. 6. Comparative Recall Analysis of USAD Model with Other Models.

Recall comparison indicates that USAD maintains competitive detection capability:

- USAD = 0.79
- VAE-LSTM = 0.78
- IF = 0.69
- LOF = 0.68

4.6 Discussion

The experimental results clearly demonstrate that the proposed USAD model outperforms both deep learning–based (VAE-LSTM) and classical machine learning approaches (LOF and Isolation Forest) across major evaluation metrics.
Several key observations can be drawn:

- The dual-decoder adversarial reconstruction mechanism enhances anomaly discrimination.
- The model achieves strong AUC performance without relying on recurrent architecture such as LSTM.
- Precision and recall remain well-balanced, avoiding bias toward either class.
- The fully connected architecture remains computationally lighter than VAE-LSTM while delivering superior detection capability.

Overall, replacing the VAE-LSTM baseline with the USAD framework leads to measurable improvements in anomaly detection performance for multivariate industrial time-series data. The results validate the effectiveness of adversarial reconstruction learning for enhancing critical infrastructure security.

V. CONCLUSION

This paper presented a USAD-based unsupervised anomaly detection framework for improving cybersecurity in industrial control systems. The proposed model utilizes a dual-decoder adversarial reconstruction mechanism to learn normal operational behaviour and detect anomalies without requiring labelled attack data. The use of a fully connected encoder–decoder architecture keeps the model simple while maintaining strong anomaly detection capability.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Experimental evaluation on the SWaT dataset demonstrates the effectiveness of the approach, achieving an AUC of approximately 0.92–0.93 with balanced precision and recall values around 0.79–0.80. Comparative analysis with VAE-LSTM, Local Outlier Factor (LOF), and Isolation Forest (IF) shows that the proposed USAD framework provides improved anomaly detection performance and better ROC characteristics. Additionally, the absence of recurrent layers such as LSTM reduces computational complexity, making the model suitable for efficient deployment in real-world industrial environments. Overall, the results indicate that the USAD architecture offers a robust and practical solution for detecting anomalies in multivariate industrial time-series data.

Future work may focus on adaptive thresholding mechanisms that dynamically adjust anomaly detection sensitivity under varying operational conditions. Incorporating multimodal data sources, such as network traffic along with process sensor measurements, could further improve detection robustness. Additionally, optimizing the framework for real-time edge deployment and exploring explainable anomaly detection techniques may enhance transparency and reliability in industrial monitoring systems.

REFERENCES

[1] M. Arafah, I. Phillips, A. Adnane, W. Hadi, M. Alauthman, and A. K. Al-Banna,"Anomaly-based network intrusion detection using denoising autoencoder and Wasserstein GAN synthetic attacks," Applied Soft Computing, vol. 168, p. 112455, 2025.

[2] A. Geiger, D. Liu, S. Alnegheimish, A. Cuesta-Infante, and K. Veeramachaneni,"TadGAN: Time series anomaly detection using generative adversarial networks," in Proc. IEEE Int. Conf. Big Data, Dec. 2020, pp. 33–43.

[3] Z. Zhang, W. Li, W. Ding, L. Zhang, Q. Lu, P. Hu, T. Gui, and S. Lu, "STAD-GAN: Unsupervised anomaly detection on multivariate time series with self-training generative adversarial networks," ACM Trans. Knowl. Discov. Data, vol. 17, no. 5, pp. 1–18, 2023.

[4] C. Sánchez-Zas, X. Larriva-Novo, V. A. Villagrá, M. S. Rodrigo, and J. I. Moreno, "Design and evaluation of unsupervised machine learning models for anomaly detection in streaming cybersecurity logs," Mathematics, vol. 10, no. 21, p. 4043, 2022.

[5] K. Lamshöft, T. Neubert, C. Krätzer, C. Vielhauer, and J. Dittmann, "Information hiding in cyber physical systems: Challenges for embedding, retrieval and detection using sensor data of the SWaT dataset," in Proc. ACM Workshop Inf. Hiding Multimedia Secur., Jun. 2021, pp. 113–124.

[6] W. Gao and T. H. Morris, "On cyber attacks and signature based intrusion detection for Modbus based industrial control systems," J. Digit. Forensics Secur. Law, vol. 9, no. 1, p. 3, 2014.

[7] A. Pinto, L. C. Herrera, Y. Donoso, and J. A. Gutierrez, "Enhancing critical infrastructure security: Unsupervised learning approaches for anomaly detection," Int. J. Comput. Intell. Syst., vol. 17, no. 1, p. 236, 2024.

[8] E. A. Boateng, J. W. Bruce, and D. A. Talbert, "Anomaly detection for a water treatment system based on one-class neural network," IEEE Access, vol. 10, pp. 115179–115191, 2022.

[9] F. Xue, W. Yan, T. Wang, H. Huang, and B. Feng, "Deep anomaly detection for industrial systems: A case study," in Proc. Annu. Conf. PHM Soc., vol. 12, no. 1, Nov. 2020, p. 8.

[10] S. Ahmed, Y. Lee, S. H. Hyun, and I. Koo, "Mitigating the impacts of covert cyber attacks in smart grids via reconstruction of measurement data utilizing deep denoising autoencoders," Energies, vol. 12, no. 16, p. 3091, 2019.

[11] Y. Cao, L. Zhang, X. Zhao, K. Jin, and Z. Chen, "An intrusion detection method for industrial control system based on machine learning," Information, vol. 13, no. 7, p. 322, 2022.

[12] S. Nazir, S. Patel, and D. Patel, "Autoencoder based anomaly detection for SCADA networks," Int. J. Artif. Intell. Mach. Learn., vol. 11, no. 2, pp. 83–99, 2021.

[13] S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, "Unsupervised real-time anomaly detection for streaming data," Neurocomputing, vol. 262, pp. 134–147, 2017.

[14] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," Internet Things, vol. 19, p. 100568, 2022.

[15] Y. He, Y. Bian, X. Ding, B. Wu, J. Guan, J. Zhang, and S. Zhou, "Variate associated domain adaptation for unsupervised multivariate time series anomaly detection," ACM Trans. Knowl. Discov. Data, vol. 18, no. 8, pp. 1–24, 2024.

[16] J. Audibert, P. Michiardi, F. Guyard, S. Marti, and M. A. Zuluaga, "USAD: Unsupervised anomaly detection on multivariate time series," in Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining, Aug. 2020, pp. 3395–3404.

[17] M. Ike, K. Phan, K. Sadoski, R. Valme, and W. Lee, "SCAPHY: Detecting modern ICS attacks by correlating behaviors in SCADA and PHYsical," in Proc. IEEE Symp. Secur. Privacy (SP), May 2023, pp. 20–37.

[18] C. M. Ahmed, V. R. Palleti, and A. P. Mathur, "WADI: A water distribution testbed for research in the design of secure cyber physical systems,"in Proc. Int. Workshop Cyber-Phys. Syst. Smart Water Netw., Apr. 2017, pp. 25–28.

[19] V. Vishala, "SWaT dataset – Secure water treatment system," Kaggle, 2021. [Online].Available:https://www.kaggle.com/datasets/vishala28/swat-dataset-secure-water-treatment-system [Accessed: Mar. 9, 2026].