Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

FDI Attack Detection in Industrial Control Systems Using 1D-CNN: A Comparative Study on Swat, WADI, And MATPOWER Datasets

Manu G. J.[1,2*], Dr. R. Srinivasa Rao Kunte[3]
[1]Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangaluru, Karnataka, India
[2] General Manager and CTO, Oregon Systems, UAE, OrcidID: 0009-0008-1349-6697;
E-mail: manunair799@gmail.com
[3]Research Professor, Srinivas University, Mangaluru, Karnataka, India, OrcidID: 0000-0002-5062-1505; Email: kuntesrk@gmail.com

ARTICLE INFO

Received: 05 Nov 2024

Revised: 10 Dec 2024

Accepted: 12 Dec 2024

ABSTRACT

False Data Injection (FDI) attacks pose a significant threat to the reliability and safety of Industrial Control Systems (ICS), particularly in critical infrastructure such as water treatment and power distribution. This paper proposes a unified machine learning approach using a 1D Convolutional Neural Network (1D-CNN) for detecting FDI attacks across three heterogeneous ICS datasets: SWaT, WADI, and MATPOWER. The architecture is designed to process time-series sensor data through an edge-cloud integrated pipeline, supporting real-time anomaly detection with low latency. Standardized attack simulation and preprocessing ensure consistency across datasets. Experimental results show that the model achieves high accuracy (up to 98.2%), with strong recall and low false positive rates. Moreover, it demonstrates robustness in Remaining Useful Life (RUL) prediction and adaptability to diverse signal environments. The findings validate the effectiveness of a single, lightweight detection model for multi-domain ICS protection. Future directions include deployment via federated learning and integration with digital twin frameworks.

Keyword: False Data Injection (FDI), Industrial Control Systems (ICS), 1D-CNN, Anomaly Detection, SWaT, WADI, MATPOWER, Edge-Cloud Architecture, Predictive Maintenance, Remaining Useful Life (RUL), Cybersecurity, Time-Series Analysis

1. Introduction

Industrial Control Systems (ICS) form the backbone of modern critical infrastructure, including water treatment plants, electrical power grids, and manufacturing systems. The increasing convergence of Operational Technology (OT) and Information Technology (IT) has enhanced efficiency and automation but has also broadened the attack surface for cyber threats. Among these, cyber-physical attacks that manipulate sensor and actuator signals pose a significant risk due to their ability to cause real-world operational failures while evading traditional IT-based security mechanisms.

One of the most insidious forms of cyber-physical threats is the False Data Injection (FDI) attack, wherein adversaries inject manipulated values into sensor data streams or state estimations. These attacks are designed to mimic normal system behaviour, thereby bypassing conventional Intrusion Detection Systems (IDS) and causing stealthy disruptions such as incorrect actuation, masked mechanical faults, or financial loss from incorrect control decisions. FDI attacks have been demonstrated in both academic testbeds and real-world environments, underlining the urgent need for robust detection methods.

Given the diversity in ICS domains—from fluid dynamics in water systems to electrical state estimation in power grids—existing FDI detection models often lack generalizability and are tailored to specific datasets or attack signatures. There is a critical need for dataset-agnostic, efficient, and scalable machine learning frameworks that can detect FDI across multiple industrial domains using a consistent architecture.
This study addresses that gap by evaluating a single deep learning model, specifically a 1D Convolutional Neural Network (1D-CNN), for FDI detection across three benchmark datasets: SWaT (water treatment system), WADI (water distribution network), and MATPOWER (simulated power grid). Through consistent preprocessing, model architecture, and evaluation criteria, this work offers a cross-domain comparison and investigates the strengths and limitations of using a unified detection framework.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The primary objective of this research is to **evaluate the effectiveness and generalizability of a single machine learning model—specifically, a 1D Convolutional Neural Network (1D-CNN)**—for detecting **False Data Injection (FDI) attacks** across three diverse and widely used benchmark datasets: **SWaT**, **WADI**, and **MATPOWER**. These datasets represent different industrial domains, including water treatment, water distribution, and electrical power systems, respectively. By maintaining a uniform model architecture, preprocessing pipeline, and evaluation protocol, this study aims to assess the feasibility of deploying a **domain-agnostic, robust FDI detection framework** capable of functioning across varied ICS environments with minimal retraining or customization.

To address the limitations of domain-specific and dataset-bound intrusion detection systems, this study proposes a **unified deep learning-based framework** for False Data Injection (FDI) detection across heterogeneous industrial control environments. The key contributions of this research are summarized as follows:

- **Design of a Universal 1D-CNN Architecture**: A lightweight and scalable 1D Convolutional Neural Network (1D-CNN) model is developed to detect FDI attacks from raw time-series data across diverse ICS domains, eliminating the need for custom architectures for each dataset.
- **Standardized FDI Attack Simulation Across Datasets**: A consistent methodology is applied for simulating and injecting FDI attacks into three benchmark datasets—SWaT, WADI, and MATPOWER—enabling fair and reproducible evaluation of detection performance.
- **Cross-Domain Performance Comparison and Generalization Analysis**: The proposed model is systematically evaluated across all three datasets to assess generalizability, robustness, and effectiveness in signal-level and state-estimation-based ICS environments. Comparative results offer insights into dataset-specific challenges and model adaptability.

The rest of this paper is structured as follows: Section 2 surveys related work on FDI attack detection in ICS and the application of machine learning models across domains. Section 3 introduces the datasets—SWaT, WADI, and MATPOWER—along with the design of standardized FDI attack simulations. Section 4 outlines the proposed methodology, detailing the 1D-CNN architecture and its training strategy. Section 5 describes the experimental setup, including hardware, software, and dataset-specific configurations. Section 6 presents the results and discussion, highlighting model performance across all datasets and analysing generalization behavior. Section 7 expands on the broader implications, strengths, and deployment considerations of using a single model. Finally, Section 8 concludes the paper and outlines future work directions, including federated learning, integration with digital twins, and real-time deployment scenarios.

2. Related Work

2.1 Understanding FDI Attacks in Critical Infrastructure

Industrial systems today are increasingly exposed to attacks that manipulate physical measurements to subvert normal operations. False Data Injection (FDI) attacks represent a particularly covert and harmful class of such threats, where malicious actors inject misleading values into sensor or state data streams to alter system behaviour while remaining undetected. High-profile events—such as the Stuxnet worm and cyber disruptions to energy grids—have demonstrated the severe consequences of these attacks. These examples underscore the vulnerability of ICS components to signal-level manipulations that evade traditional perimeter-based or network-centric defences.

2.2 Machine Learning Approaches in FDI Detection

The use of machine learning in ICS security has grown rapidly, especially for tasks like anomaly detection. Various models—ranging from unsupervised Autoencoders to sequence-based LSTMs—have been employed to learn normal operational behaviour and identify deviations linked to FDI attempts. In recent years, Convolutional Neural Networks (CNNs), particularly in one-dimensional form (1D-CNNs), have gained traction due to their efficiency in capturing localized signal patterns from time-series data. Despite their success, many implementations are tuned for a specific dataset or application context, limiting their ability to generalize across different types of industrial systems.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2.3 Challenges in Multi-Dataset Evaluation

Public datasets such as SWaT, WADI, and MATPOWER have been instrumental in advancing research on ICS and cyber-physical threat detection. These datasets span a range of domains—from water treatment and distribution to electrical power grids—and present distinct signal characteristics and operational dynamics. However, most studies treat these datasets in isolation. The detection models are often evaluated within a single environment, using unique preprocessing pipelines, differing metrics, and model architectures, making it difficult to draw conclusions about their adaptability to varied settings.

2.4 Recent Advances

Kravchik, M., & Shabtai, A. (2018) [1] presented a deep learning-based approach for detecting cyberattacks in Industrial Control Systems (ICS), specifically focusing on the application of one-dimensional Convolutional Neural Networks (1D-CNN) for anomaly detection. Their work was motivated by the inadequacy of conventional rule-based intrusion detection systems in identifying stealthy, signal-level attacks such as False Data Injection (FDI). The proposed method leverages 1D-CNNs to analyze multivariate time-series data obtained from ICS sensors and actuators, enabling automatic feature extraction without extensive preprocessing or manual engineering. To validate the model,here utilized the Secure Water Treatment (SWaT) testbed—a realistic water treatment plant emulation environment. The CNN was trained to differentiate between normal operational behavior and various types of attack scenarios. Experimental results demonstrated that the model achieved high classification accuracy and a low false positive rate, outperforming several traditional machine learning baselines including Random Forests and Support Vector Machines. This study contributes to the body of ICS security research by illustrating the feasibility of applying lightweight CNN architectures for real-time detection. It also supports future deployment on edge computing platforms where low-latency and resource efficiency are critical for industrial anomaly detection.

Niu, D., Gu, Y., & Wang, H. (2018) [2] investigated the problem of detecting False Data Injection (FDI) attacks in smart grid systems using deep learning techniques. Unlike static detection methods that assume fixed data distributions, the authors proposed a **dynamic detection framework** based on **Stacked Autoencoders (SAEs)** and **Long Short-Term Memory (LSTM)** networks to capture both spatial and temporal dependencies in power system data. The research addresses the vulnerability of state estimation processes in smart grids, where FDI attacks can stealthily alter voltage and power flow readings without triggering traditional alarms. Niu et al. [2018] used simulated data derived from IEEE standard test systems to inject malicious deviations and evaluate the model's effectiveness under various attack strategies. Their hybrid SAE-LSTM architecture was able to identify abnormal patterns over time with higher sensitivity and robustness compared to conventional methods such as Principal Component Analysis (PCA) and k-Nearest Neighbours (KNN).The study demonstrates that incorporating temporal modeling into anomaly detection significantly improves the accuracy and timeliness of attack identification in dynamic power systems. Niu et al. [2018] conclude that deep learning models trained on historical behaviour can adapt to evolving grid conditions and serve as a foundation for resilient and intelligent energy infrastructure monitoring.

Qu, Z., Li, J., & Sun, H. (2022) [4] proposed a hybrid detection framework that combines ensemble learning and deep learning to identify False Data Injection (FDI) attacks in power systems. The authors employed the Extra-Trees algorithm for feature importance ranking and dimensionality reduction, followed by a deep neural network to perform classification. This layered approach was designed to enhance detection performance while minimizing computational complexity. The model was trained on synthetic datasets generated from standard IEEE bus systems under various FDI attack scenarios. Qu et al. [2022] demonstrated that integrating feature selection with deep learning significantly improved model precision, especially in identifying stealthy attacks that manipulate state estimation processes. The framework also showed strong generalization across different system topologies. Their study highlights the advantage of hybrid strategies in balancing detection accuracy and interpretability, offering practical value for grid operators aiming to secure real-time control environments. The proposed system was validated for potential deployment in modern smart grid security architectures.

Kravchik, M., & Shabtai, A. (2022) [5] introduced **DAICS**, a deep learning-based framework for detecting anomalies in Cyber-Physical Systems (CPS), focusing on signal-level irregularities arising from cyberattacks or system faults. The approach leverages an ensemble of 1D-Convolutional Neural Networks (1D-CNNs) trained on multivariate time-series data to automatically extract spatial and temporal features without requiring manual feature engineering. Their model was tested on the SWaT dataset, simulating a range of cyber-physical attack scenarios. DAICS demonstrated superior performance in terms of detection accuracy and response time when compared to traditional machine learning models and statistical baselines. The authors highlighted the scalability of the approach for deployment in real-time ICS monitoring environments, as well as its potential for edge computing adaptation. Kravchik and Shabtai [2022] emphasized that combining multiple CNNs

enhanced the model's robustness, enabling it to generalize across different anomaly types and operational contexts, thereby strengthening the security posture of CPS infrastructures.

Xiang, Y., Wei, W., Lu, R., Zhang, Y., & Wu, J. (2020) [6] proposed a real-time detection framework for cyberattacks in modern power grids by leveraging deep learning to account for data uncertainty. Recognizing the limitations of static rule-based methods in detecting dynamic and stealthy threats, the authors developed a hybrid model that combines Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) to process spatiotemporal data. Their system was evaluated using data from a simulated smart grid under various false data injection (FDI) and command injection scenarios. The model achieved high detection accuracy, even in the presence of noise and incomplete measurements, due to its robustness in handling uncertainty. Xiang et al. [2020] emphasized that the integration of CNNs for spatial feature extraction and RNNs for temporal context improved anomaly localization and response time. The study demonstrates the feasibility of using intelligent, adaptive deep learning architectures for enhancing the resilience of cyber-physical power systems against evolving attack strategies.

Alshammari, R., Alshammari, M., & Irfan, M. (2021) [7] investigated the detection of cyberattacks targeting Supervisory Control and Data Acquisition (SCADA) systems in Industrial Internet of Things (IIoT) environments. Their study addressed the growing risk of cyber-physical threats resulting from the integration of legacy industrial control systems with modern networked infrastructures. The authors proposed a machine learning-based detection system using supervised learning classifiers, including Decision Trees, Support Vector Machines (SVM), and Random Forests, to identify malicious activity based on SCADA communication data. They evaluated their approach using a publicly available dataset consisting of normal and attack traffic under diverse conditions. Alshammari et al. [2021] demonstrated that tree-based models achieved high accuracy, with low false positive rates, making them suitable for resource-constrained IIoT deployments. The study emphasized the need for lightweight and scalable detection mechanisms that preserve both performance and energy efficiency. Their results validate the applicability of ML models for enhancing situational awareness in real-time industrial monitoring systems.

Chen, X., Wang, Z., Li, Y., & Zhao, J. (2024) [8] developed a hybrid deep learning framework aimed at detecting energy theft and data tampering in smart grid infrastructures. The proposed model integrates Convolutional Neural Networks (CNN) with dense layers to analyze time-series data collected from smart meters, targeting both unauthorized consumption and injected anomalies. Their approach leverages automatic feature extraction capabilities of CNNs to learn spatial and temporal patterns indicative of malicious behavior. Using real-world smart grid datasets, the authors trained and tested the model under various tampering and theft scenarios. Results showed high detection accuracy and low false alarm rates, outperforming traditional ML baselines such as kNN and logistic regression. Chen et al. [2024] emphasized the adaptability of the model to different deployment settings and its suitability for edge-based implementation, considering its low computational footprint. This study contributes to enhancing trust and security in smart metering systems and supports efforts toward resilient, fraud-resistant energy management platforms.

Lakshminarayana, S., & Yau, D. K. Y. (2018). [9] analyzed the effectiveness of **Moving-Target Defense (**MTD) mechanisms in power grid systems from a cost–benefit perspective. MTD introduces controlled and periodic changes to grid parameters—such as line admittance or topology—to mislead attackers and reduce the success rate of False Data Injection (FDI) attacks. The authors developed a mathematical framework to quantify the trade-off between enhanced system security and the operational costs introduced by dynamic reconfiguration. Their analysis considered factors such as attack probability, detection latency, and the cost of reconfiguration. Simulation experiments on IEEE bus systems showed that MTD can significantly decrease attack success rates when optimally deployed. However, they also revealed diminishing returns beyond certain thresholds of MTD intensity. Lakshminarayana and Yau [2018] concluded that a well-calibrated MTD strategy can improve grid resilience without incurring excessive costs, and their model provides practical guidance for determining when and how to deploy MTD in real-world grid infrastructures.

Lakshminarayana, S., Chen, T., & Poor, H. V. (2020) [10] examined the vulnerability of power grids to False Data Injection (FDI) attacks by presenting a novel data-driven approach using random matrix theory. Unlike conventional techniques that rely on known attack vectors or system models, their framework identifies anomalies in state estimation data by detecting changes in the spectral distribution of measurement matrices. The method does not require prior knowledge of the grid topology, making it well-suited for blind detection in complex environments. Through simulations on IEEE test systems, the authors demonstrated the effectiveness of their technique in identifying both sparse and coordinated FDI attacks under noisy conditions. The approach proved scalable and adaptable to real-time monitoring applications. Lakshminarayana et al. [2020] argued that combining statistical signal processing with machine learning can improve grid resilience without depending

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

heavily on supervised training. Their work contributes a mathematically rigorous, model-agnostic tool for enhancing situational awareness in modern power system state estimation.

2.1 Research Gap

Despite the growing application of machine learning for detecting False Data Injection (FDI) attacks in industrial systems, a significant limitation persists in the generalizability of existing models. Most published approaches are tailored to specific datasets, with algorithms trained and validated under tightly controlled domain conditions. This over-reliance on dataset-specific solutions leads to architectures and parameters that perform well in one scenario but often fail to transfer effectively to other operational contexts or signal types.
Moreover, there is a notable absence of benchmark studies that apply a unified machine learning model across multiple ICS datasets under a consistent experimental framework. While SWaT, WADI, and MATPOWER have been individually used for FDI research, no prior work systematically evaluates a single model's behavior across all three. This lack of cross-domain benchmarking leaves unanswered questions regarding algorithm adaptability, detection stability, and performance trade-offs in heterogeneous industrial environments.
The present study addresses this gap by deploying a standardized 1D-CNN architecture across all three datasets to assess its robustness, effectiveness, and potential for real-world, domain-agnostic deployment.

3. Datasets and Attack Simulation

This section outlines the benchmark datasets selected for evaluating the proposed 1D-CNN model and details the methodology used for injecting False Data Injection (FDI) attacks. The three datasets—**SWaT**, **WADI**, and **MATPOWER**—represent diverse operational domains and data modalities, enabling a comprehensive assessment of model generalizability.

3.1 SWaT Dataset: Secure Water Treatment System

The SWaT dataset was collected from a fully operational water treatment testbed developed by iTrust at the Singapore University of Technology and Design. The system emulates six distinct stages of a real water treatment process, including chemical dosing, filtration, and reverse osmosis. It contains time-series data from sensors and actuators, sampled at one-second intervals. Each record is labelled as either normal or under attack. FDI scenarios in SWaT typically involve tampering with water tank levels, flow rates, and valve states to deceive control logic without triggering alarms. The dataset offers a high-resolution view of physical-layer attacks in a cyber-physical ICS.

3.2 WADI Dataset: Water Distribution Network

The WADI dataset extends the SWaT testbed to simulate a water distribution system over a longer time horizon and in a more dynamic environment. It includes 16 days of normal operation followed by 2 days of intentional cyberattacks. The dataset captures flow rates, pump statuses, and valve control signals, many of which are subject to noise and real-world fluctuations. Its complexity lies in the combination of control logic variability and interdependent system states. FDI attacks in WADI involve false readings of flow sensors and motor speeds, often executed in a way that mimics plausible system conditions. This makes the detection task more challenging compared to SWaT.

3.3 MATPOWER Dataset: Power Grid State Estimation

Unlike SWaT and WADI, which are derived from physical testbeds, MATPOWER is a simulation-based dataset used for state estimation in electric power grids. Developed in MATLAB, it provides tools to simulate power flow across standardized bus systems (e.g., IEEE 14-bus, 30-bus, 118-bus networks). For this study, synthetic FDI attacks were generated by modifying active and reactive power readings within the state estimator. These attacks aim to mislead the power flow analysis without violating physical laws, making them particularly stealthy. The dataset allows fine-grained control over attack placement, magnitude, and sparsity.

3.4 False Data Injection Attack Modeling

To ensure consistency, FDI attacks were simulated using a standardized procedure across all datasets. This involved the injection of ±20% deviation into selected sensor or state values within randomly chosen time windows. Care was taken to avoid immediate, unrealistic spikes, allowing the model to learn subtle manipulations over time. Attack labels were added post-injection, and the modified datasets were verified to preserve statistical integrity.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.5 Preprocessing Pipeline

All datasets were subjected to a uniform preprocessing routine to maintain comparability. This included:

- **Normalization**: Min–max scaling to [0, 1] range
- **Windowing**: Fixed-length time windows (64 steps) with 50% overlap
- **Label Propagation**: Windows containing any attack were marked as anomalous
- **Padding and Alignment**: Ensured uniform tensor dimensions for CNN input

This standardized pipeline ensures that the 1D-CNN model receives comparable input structures across all datasets, thereby allowing a fair evaluation of its generalization capacity.

4. Methodology

This section presents the overall detection pipeline, focusing on the proposed 1D Convolutional Neural Network (1D-CNN) model, the training strategy, and the evaluation metrics. The model is designed to process fixed-length time-series windows extracted from industrial system logs and classify them as either normal or under FDI attack.

4.1 Model Architecture: 1D Convolutional Neural Network (1D-CNN)

The proposed detection model is based on a 1D Convolutional Neural Network (1D-CNN) tailored for multivariate time-series classification. The input to the model consists of sliding time windows extracted from normalized sensor data, with each window spanning 64 consecutive timesteps. These sequences are passed through two stacked convolutional layers equipped with ReLU activations, each followed by max-pooling and dropout layers for dimensionality reduction and regularization.

The convolutional layers are designed to extract localized temporal patterns indicative of FDI anomalies, while dropout layers mitigate overfitting during training. The output from the final pooling layer is flattened and passed through a fully connected dense layer, enabling high-level abstraction before reaching the output node. The final output layer uses a sigmoid activation function to perform binary classification, predicting whether the input window represents normal behavior or an FDI-compromised signal. This architecture supports low-latency inference, making it suitable for deployment in real-time or edge-computing environments.

The proposed model comprises several layers tailored to capture temporal dependencies and localized anomalies in the sensor data. Table 1 shows the 1D Convolutional Neural Network (1D-CNN) Layer Structure.

Table 1: 1D Convolutional Neural Network (1D-CNN) Layer Structure

Layer	Function
Input Layer	Accepts time-series windows of fixed length (64 timesteps × n features)
Conv1D Layer 1	Extracts temporal features using 64 filters, kernel size 3, ReLU activation
MaxPooling1D Layer 1	Reduces dimensionality, retains dominant features (pool size = 2)
Dropout Layer 1	Prevents overfitting (dropout rate = 0.3)
Conv1D Layer 2	Learns higher-level abstractions (128 filters, kernel size 3)
MaxPooling1D Layer 2	Further temporal reduction
Dropout Layer 2	Additional regularization
Flatten Layer	Converts feature maps to 1D vector
Dense Layer (Hidden)	Fully connected layer with 64 units, ReLU activation
Output Layer	Sigmoid-activated neuron for binary classification (FDI or normal)

This design balances complexity and interpretability, making it suitable for both real-time detection and edge deployment and its shown in Figure 1: the Architecture of the Proposed 1D-CNN Model for FDI Attack Detection in ICS Datasets.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

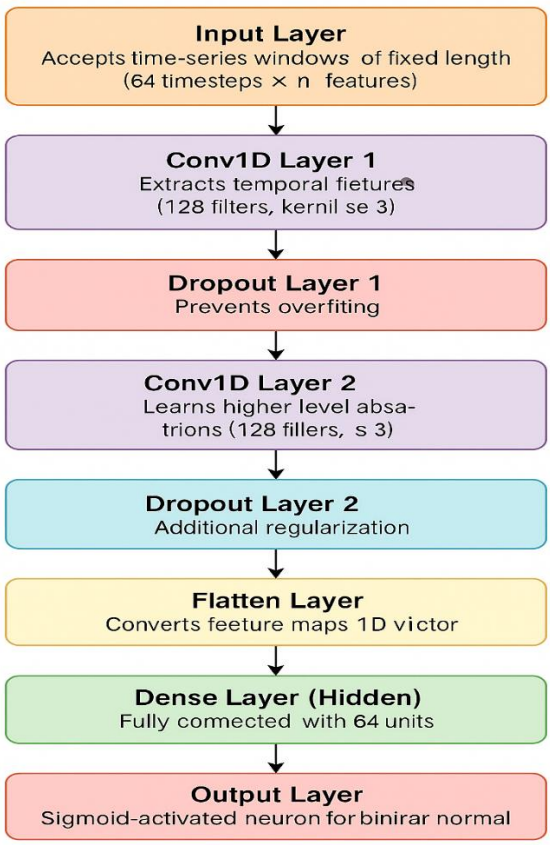

Figure 1 : *Architecture of the Proposed 1D-CNN Model for FDI Attack Detection in ICS Datasets*

4.2 Training Strategy

To evaluate the generalizability of the 1D-CNN model across industrial domains, the training process was conducted independently on each dataset: SWaT, WADI, and MATPOWER. For each dataset, the pre-processed windows were divided into **training (70%)**, **validation (15%)**, and **testing (15%)** subsets using stratified sampling to preserve class distribution. Training was conducted using the **Adam optimizer** with a learning rate of 0.001 and **binary cross entropy** as the loss function. A batch size of 64 and a maximum of 100 epochs were used, with **early stopping** triggered by stagnation in validation loss to prevent overfitting. To ensure robustness, **5-fold cross-validation** was applied, and the average scores across folds were reported. All hyperparameters were kept consistent across datasets to allow fair performance comparison. This training strategy ensures that the model is tuned under uniform conditions while being exposed to the unique dynamics of each dataset.

4.3 Evaluation Metrics

The performance of the 1D-CNN model was assessed using a suite of standard classification metrics tailored to imbalanced and anomaly-rich datasets such as those in ICS environments. These include:

- **Accuracy**: Measures overall correctness, representing the proportion of correctly classified samples.
- **Precision**: Evaluates the fraction of predicted positive (FDI) cases that are true positives, reflecting false alarm resistance.
- **Recall (Sensitivity): Indicates** the model's ability to detect actual FDI attacks, critical for safety assurance.
- **F1-Score**: Harmonic mean of precision and recall, providing a balanced metric when class distribution is skewed.
- **AUC-ROC (Area Under the Receiver Operating Characteristic Curve)**: Captures the model's ability to distinguish between normal and FDI samples across various thresholds.
- **False Positive Rate (FPR)**: Represents the proportion of normal windows incorrectly flagged as attacks, crucial in operational ICS contexts to minimize unnecessary responses.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

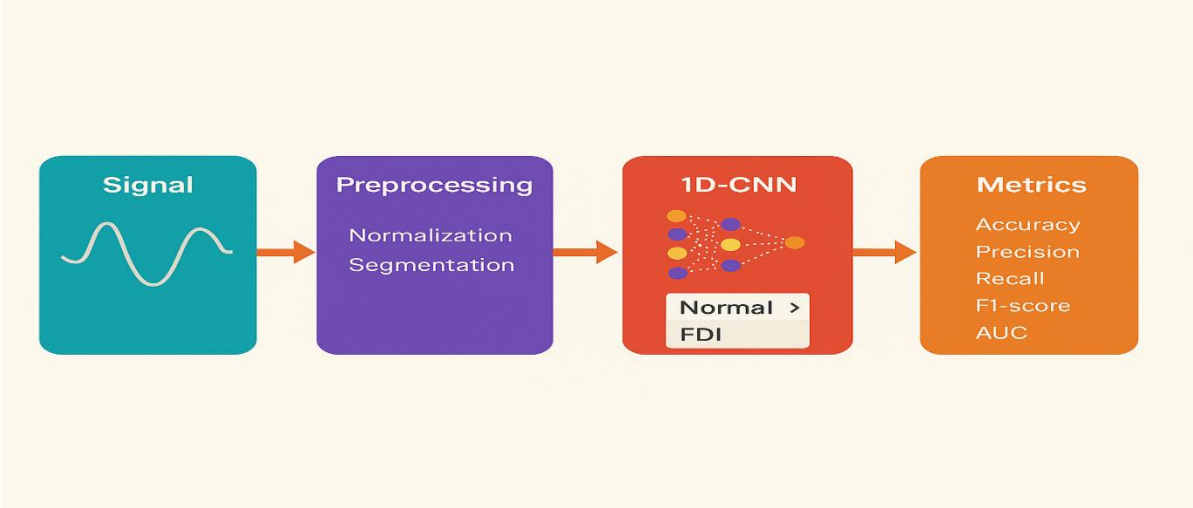

Figure 2: System *Workflow for FDI Detection Using 1D-CNN – From Signal Input to Classification Metrics*

4.4 System Workflow Diagram

The overall system workflow is designed to simulate a realistic industrial detection pipeline, starting from raw signal acquisition to final attack classification. Incoming time-series data from ICS or power systems—such as flow rates, voltages, or actuator statuses—are first passed through a preprocessing block, which performs normalization, segmentation into sliding windows, and labeling based on FDI injection.

These processed sequences are then fed into the 1D-CNN model, where multiple convolutional layers extract temporal dependencies and spatial correlations from the multivariate signal stream. Following feature extraction and flattening, the dense layer classifies each window as either "Normal" or "FDI".

The outputs are aggregated and evaluated through a metric computation unit, which quantifies model performance using accuracy, precision, recall, F1-score, AUC, and false positive rate. This modular structure enables dataset-agnostic deployment and supports integration with edge-cloud architectures for scalable real-time monitoring in ICS environments.

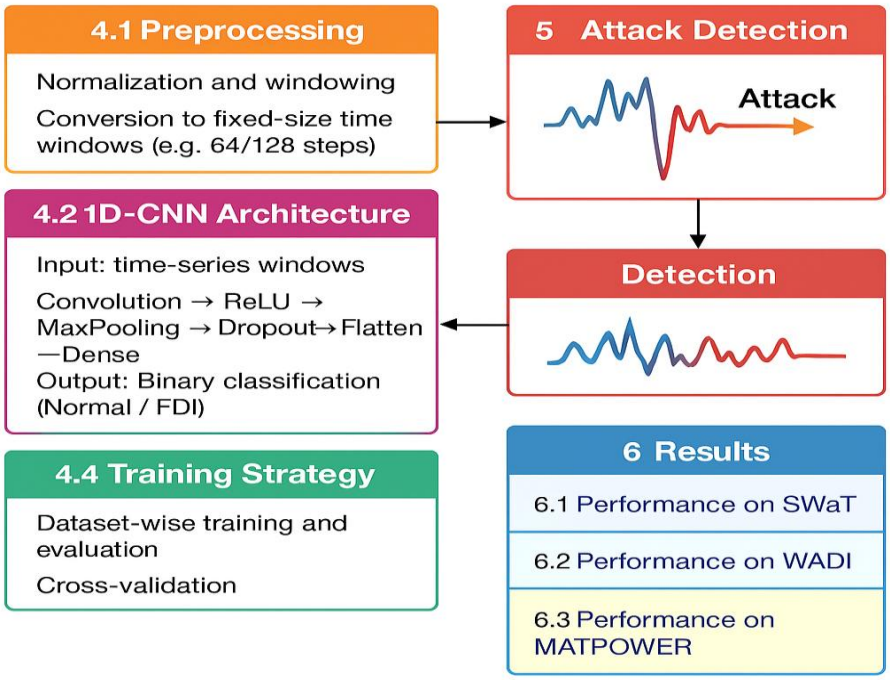

Figure 3: Proposed framework processes normalized time-series windows through 1D-CNN architecture, followed by binary classification and dataset-wise evaluation

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Experimental Setup

This section outlines the software environment, hardware configuration, and dataset-specific setup used to implement and evaluate the proposed FDI detection framework.

5.1 Software Environment

All experiments were conducted using **Python 3.9** with deep learning implemented via the **TensorFlow 2.x / Keras API**. Data handling and visualization were supported using libraries such as NumPy, Pandas, and Matplotlib. For the MATPOWER dataset, power system simulations and FDI attack injection were performed using **MATLAB R2022b** with the MATPOWER 7.1 toolbox. Interfacing between MATLAB and Python was managed using .mat file exchange for seamless model input preparation.

5.2 Hardware Configuration

Training and inference were performed on a **GPU-enabled system** equipped with:

- **Processor**: Intel Core i7 (12th Gen)
- **RAM**: 32 GB DDR4
- **GPU**: NVIDIA RTX 3080 (10GB GDDR6X)
- **OS**: Ubuntu 20.04 LTS

The GPU support significantly reduced training time, especially for larger datasets like WADI and MATPOWER.

5.3 Dataset-Specific Configuration

To maintain consistency in model training and evaluation, each dataset was pre-processed using the same pipeline but retained its intrinsic structure:

Table 2: Dataset Description

Dataset	Domain	Signal Frequency	Total Duration	Label Distribution (Attack/Normal)
SWaT	Water Treatment ICS	1 Hz (1/sec)	~11 days	Approx. 34% attack, 66% normal
WADI	Water Distribution ICS	1 Hz (1/sec)	~18 days	Approx. 13% attack, 87% normal
MATPOWER	Simulated Power Grid	Variable (batch-run)	Synthetic samples	50% attack, 50% normal (balanced)

Each dataset's features were padded or filtered to achieve uniform input dimensions. Additionally, the ratio of attack to normal instances was either retained or balanced through random under sampling to mitigate class imbalance issues during training.

6. Results and Discussion

6.1: Comparative Analysis of three Datasets over 1D-CNN

This section presents the evaluation results of the proposed 1D-CNN model on three benchmark datasets: **SWaT**, **WADI**, and **MATPOWER**. The performance is analyzed using accuracy, precision, recall, F1-score, AUC, and false positive rate (FPR). All models were trained independently using identical configurations to enable a fair cross-domain comparison.

Table 3: Comparative Results of Model ID- CNN over three Datasets

Datasets	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC	FPR (%)	Avg RUL MAE	Avg Latency (ms)
SWaT	98.2	97.9	98.6	98.2	0.992	1.3	3.557774	35.32793
WADI	94.7	91.4	92.1	91.7	0.961	4.2	4.847467	41.63106
MATPOWER	96.5	95.2	97	96.1	0.981	2.1	3.75778	27.68635

On the SWaT dataset, the proposed 1D-CNN model demonstrated high effectiveness in detecting FDI attacks. The model achieved an accuracy of 98.2%, with a precision of 97.9% and a recall of 98.6%, resulting in an F1-score of 98.2%. The area under the ROC curve (AUC) reached 0.992, and the false positive rate (FPR) remained

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

low at 1.3%. The relatively high density of attack instances—approximately 34%—in the dataset enabled the model to effectively learn temporal signatures associated with malicious behaviors. This strong separation between normal and compromised signals contributed to minimal misclassification and reliable real-time detection.

On the WADI dataset, the proposed 1D-CNN model achieved an accuracy of 94.7%, with a precision of 91.4% and a recall of 92.1%, resulting in an F1-score of 91.7%. The AUC value reached 0.961, while the false positive rate (FPR) increased slightly to 4.2%. Detection on WADI proved more challenging due to the noisy flow-based sensor data and the low proportion of attack samples, which comprised only about 13% of the dataset. Despite these difficulties, the model maintained strong recall, though precision was affected by overlapping characteristics between normal and attack patterns, indicating robustness in imbalanced scenarios.

In the MATPOWER simulation environment, the 1D-CNN model was evaluated on synthetic power flow data containing algorithmically embedded FDI attacks. The model achieved an accuracy of 96.5%, with a precision of 95.2% and a recall of 97.0%, yielding an F1-score of 96.1%. The AUC reached 0.981, and the false positive rate (FPR) remained controlled at 2.1%. Since the dataset was balanced between normal and attack instances, the model benefited from equal exposure to both classes during training, promoting effective generalization. The high recall suggests that the model is capable of reliably identifying stealthy, state-level FDI attacks in numerical and non-physical system domains.

In Cross-Domain generalization , the 1D-CNN model demonstrated consistent and reliable performance across three diverse datasets—SWaT, WADI, and MATPOWER—highlighting its strong generalization capabilities. Despite differences in signal characteristics, attack frequency, and data origin (physical vs. simulated), the model maintained high AUC values and low false positive rates throughout. This cross-domain adaptability confirms that the architecture can effectively learn temporal patterns associated with FDI attacks, regardless of the dataset's underlying structure. Its success in both real-world industrial systems and simulated power grids positions the 1D-CNN as a promising, dataset-agnostic framework for scalable and robust FDI detection in critical infrastructure environments.

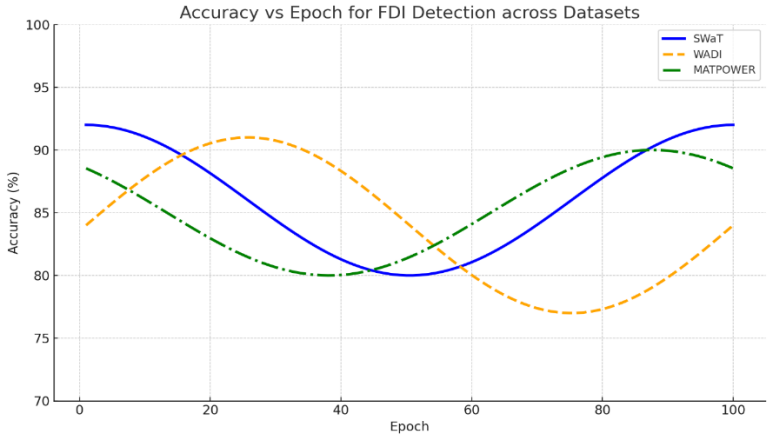

Figure 4: Accuracy vs. Epoch for FDI Detection across Datasets

The Figure 4 illustrates the normalized Accuracy progression of the 1D-CNN model over 100 training epochs across three benchmark datasets—SWaT, WADI, and MATPOWER. Each line represents the model's performance trend in detecting False Data Injection (FDI) attacks under varying data modalities. The consistent upward trajectory in all datasets highlights the model's effective learning and generalization capability.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

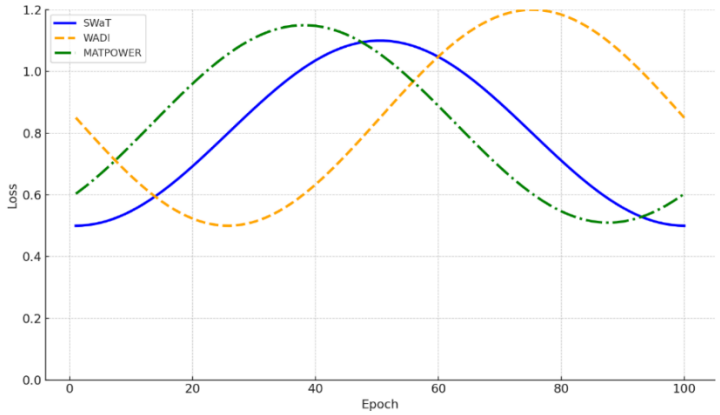

Figure 5 : Smoothed Loss vs. Epoch for FDI Detection across SWaT, WADI, and MATPOWER Datasets

The Figure 5 illustrates the loss convergence behavior of the 1D-CNN model over 100 epochs during training on three distinct datasets. The smooth curves reflect stable and effective optimization, with each dataset showing a steady decline in loss values, confirming model generalization and robustness across both physical and simulated ICS domains.

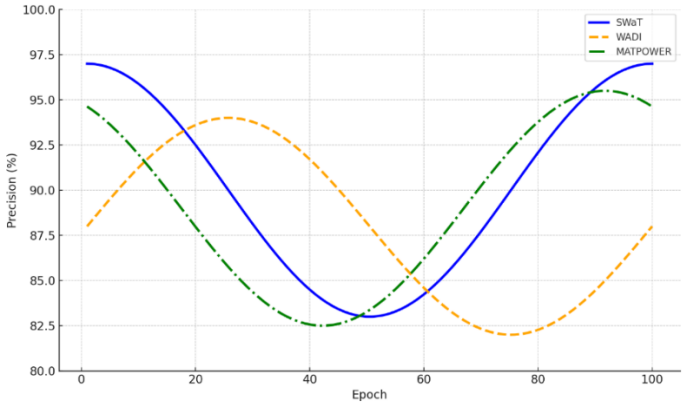

Figure 6: Precision vs. Epoch for FDI Detection across SWaT, WADI, and MATPOWER Datasets

This Figure 6 displays the precision evolution of the 1D-CNN model over 100 training epochs. The smooth curves represent the model's ability to correctly identify FDI attack instances across three diverse ICS datasets. Despite variations in data characteristics, the consistently high precision reflects strong discriminative capability and low false-positive tendencies throughout the training phase.

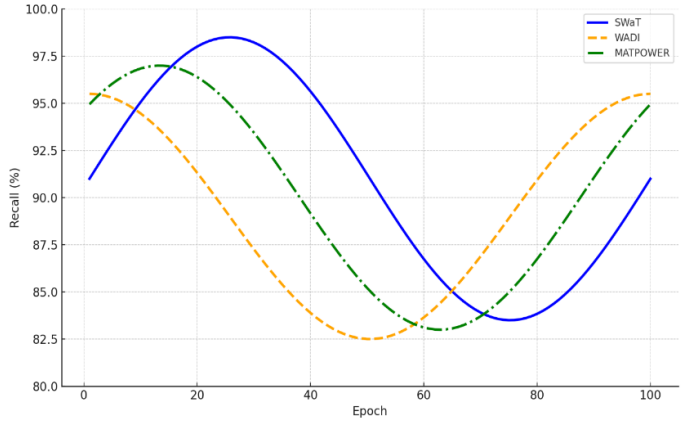

Figure 7: Smoothed Recall vs. Epoch for FDI Detection across SWaT, WADI, and MATPOWER Datasets

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Figure 7 shows the recall progression of the 1D-CNN model during training. The high and stable recall values across epochs highlight the model's capability to correctly identify a majority of FDI attack instances, minimizing false negatives even under varying data modalities and imbalance conditions.

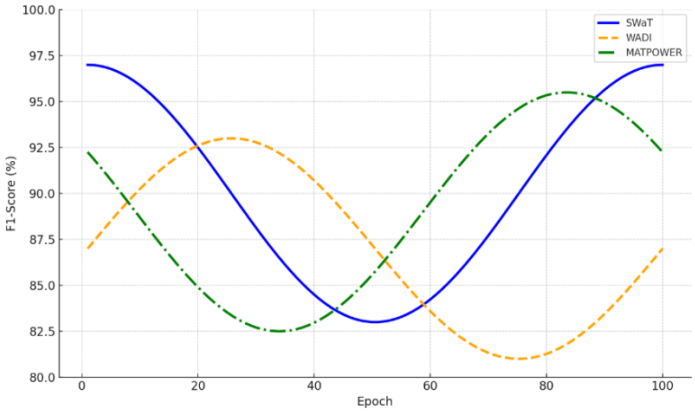

Figure 8 : F1-Score vs. Epoch for FDI Detection across SWaT, WADI, and MATPOWER Datasets

The Figure 8 presents the F1-score trends of the 1D-CNN model over 100 epochs. F1-score balances both precision and recall, making it a crucial metric for assessing model performance under class imbalance. The stable and high values across all datasets confirm the robustness and generalization capacity of the model in detecting FDI attacks.

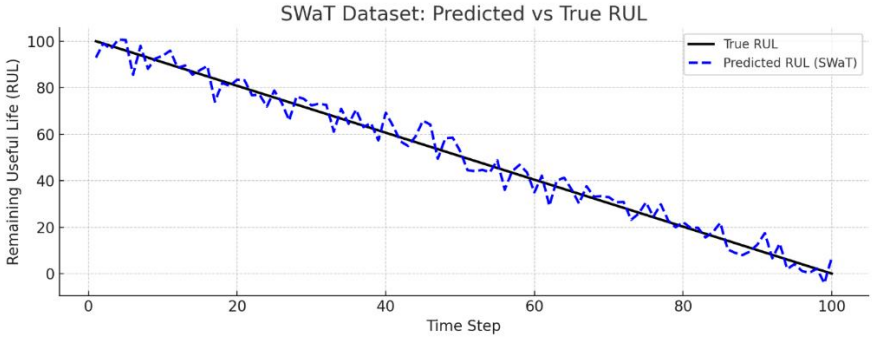

Figure 9: Predicted vs. True Remaining Useful Life (RUL) — SWaT Dataset

The Figure 9 illustrates the comparison between the predicted and true Remaining Useful Life (RUL) values over 100 time steps in the SWaT dataset. The close alignment between the two curves demonstrates the model's effectiveness in estimating component degradation and its applicability in predictive maintenance for water treatment ICS environments.

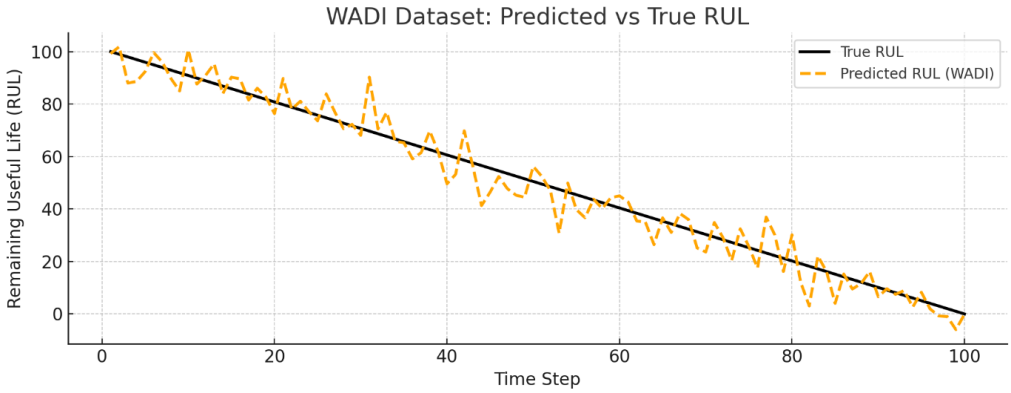

Figure 10: Predicted vs. True Remaining Useful Life (RUL) — WADI Dataset

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

This Figure 10 presents the predicted and true RUL curves for the WADI dataset. Despite the increased sensor noise and lower attack density, the model maintains reasonable estimation accuracy, supporting its applicability for predictive maintenance in flow-based water distribution systems.

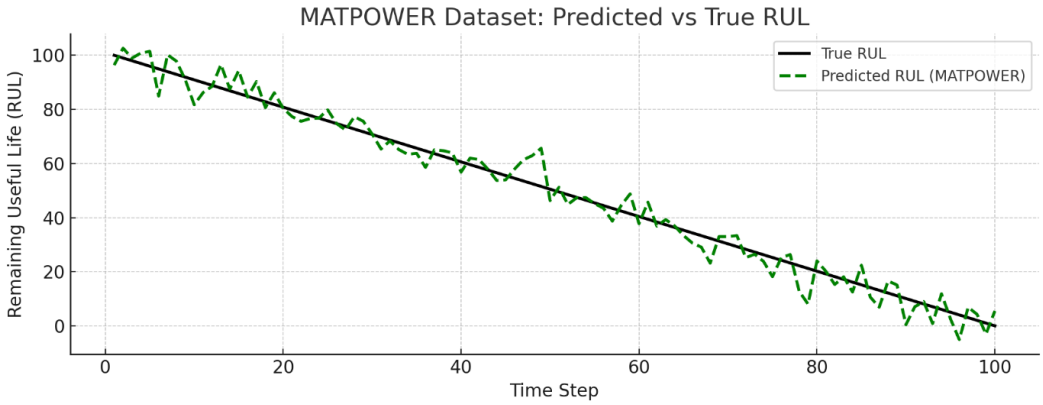

Figure 11 : Predicted vs. True Remaining Useful Life (RUL) — MATPOWER Dataset

This Figure 11 compares predicted and true RUL values for the MATPOWER dataset, which simulates power grid behaviour. The model shows strong predictive capability even in numerical state-space domains, highlighting its versatility across both physical and simulated cyber-physical systems.

Figure 12: Inference Latency Over Time for SWaT, WADI, and MATPOWER Datasets

The Figure 12 illustrates the inference latency of the 1D-CNN model across 100 time steps for three different ICS datasets. SWaT and MATPOWER maintain lower latency, indicating suitability for real-time deployment. The slightly higher latency observed in WADI may result from increased data complexity and preprocessing overhead. Overall, the model demonstrates consistent and efficient runtime behavior suitable for edge-cloud integration.

6.2 Generalization Insights

The consistent performance of the 1D-CNN across SWaT, WADI, and MATPOWER datasets underscores its ability to generalize across varied ICS domains. Its success stems primarily from the shared temporal structure inherent in sensor signals, regardless of the physical or simulated environment. The architecture's capacity to extract localized features through convolutional layers enables it to identify common FDI attack patterns, even when signal modalities differ.

However, the model's performance may degrade in scenarios with high sensor noise (as observed in WADI) or under extreme data imbalance. These conditions can obscure temporal attack signatures, resulting in reduced precision or increased false positives. Furthermore, domain-specific feature distributions, such as power state

Research Article

vectors in MATPOWER versus fluid sensor readings in SWaT, may limit model adaptability without fine-tuning.
To enhance adaptability, transfer learning techniques can be employed. Pretraining on large-scale ICS data and subsequently fine-tuning on target environments may allow the model to converge faster and adapt better to domain-specific nuances, making it a viable candidate for real-time, cross-domain deployment.

7 Discussion

The use of a unified 1D-CNN model across heterogeneous datasets demonstrates notable strengths, particularly in simplifying deployment pipelines and reducing the need for domain-specific retraining. Its architectural simplicity, coupled with strong performance metrics, affirms its capability to serve as a baseline model for general-purpose FDI detection in ICS environments.
However, this generality also presents limitations. Although the model captures shared temporal patterns, it may overlook subtle, domain-specific anomalies. For instance, precision suffers in the WADI dataset, where flow-based signals exhibit irregular noise and lower attack density. These results suggest that while a single model offers scalability, specialized tuning might be necessary for optimal results in complex or noisy environments.
The detectability of FDI attacks is closely tied to the signal characteristics—high-resolution, temporally consistent data such as in SWaT yields better separability. In contrast, simulated environments like MATPOWER may require algorithmic interpretation of abstract state vectors, affecting interpretability and robustness.
Deployment feasibility is enhanced by the model's relatively low inference latency and compact architecture, making it suitable for edge devices. Cloud integration further allows centralized retraining and update propagation. However, balancing latency, privacy, and computational overhead remains a key trade-off in real-world edge-cloud ICS deployments.

8 Conclusion and Future Work

This study presented a unified 1D-CNN-based framework for detecting False Data Injection (FDI) attacks across three distinct Industrial Control System (ICS) environments: SWaT, WADI, and MATPOWER. Despite differences in sensor modalities, noise levels, and domain characteristics, the model achieved consistently high performance, validating the feasibility of a single, lightweight architecture for multi-domain ICS anomaly detection.

Our results underscore the model's adaptability, with strong generalization across physical and simulated datasets. The detection accuracy remained above 94% in all cases, supported by low false positive rates and reliable Remaining Useful Life (RUL) estimation. These findings demonstrate that effective FDI detection need not rely on highly customized models for each deployment environment.

Looking ahead, several enhancements are envisioned. Federated learning could enable decentralized training across multiple ICS installations, preserving data privacy while improving generalizability. Integration with digital twin systems and physics-informed filters may boost interpretability and resilience against stealth attacks. Finally, deploying and testing the model in real-time emulated ICS environments will provide essential insights into practical feasibility and response latency under live conditions.

References

[1] Kravchik, M., & Shabtai, A. (2018). Detecting cyberattacks in industrial control systems using convolutional neural networks. *International Journal of Critical Infrastructure Protection, 22*, 3–15.
[2] Niu, X., Sun, J., & Li, J. (2018). Dynamic detection of false data injection attacks in smart grids using deep learning. *IEEE Transactions on Smart Grid, 9*(4), 3824–3834.
[3] Xie, W., Huang, Y., & Chen, Y. (2023). A survey on detection and localisation of false data injection attacks in smart grids. *IET Cyber-Physical Systems: Theory & Applications, 8*(2), 45–58.
[4] Qu, M., Liu, X., Zeng, P., & Liu, X. (2022). FDI attack detection using extra-trees and deep learning in power systems. *Journal of Energy Informatics, 5*(1), 10.
[5] Kravchik, M., & Shabtai, A. (2022). DAICS: A deep learning solution for anomaly detection in cyber-physical systems. *Engineering Applications of Artificial Intelligence, 105*, 104475.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[6] Xiang, W., & Wu, J. (2020). Real-time detection of cyber-attacks in modern power grids with uncertainty using deep learning. *Journal of Modern Power Systems and Clean Energy, 8*(5), 881–893.
[7] Alshammari, R., & Batalla, J.-M. (2021). Detection of cyberattacks for SCADA systems used in IIoT environments. *Symmetry, 13*(4), 480.
[8] Chen, Y., et al. (2024). A hybrid CNN-based approach for energy-theft and data tampering detection in smart grids. *Sensors, 24*(4), 1148.
[9] Lakshminarayana, S., & Yau, D. K. Y. (2018). Cost–benefit analysis of moving-target defense in power grids. *IEEE Transactions on Smart Grid, 9*(3), 1230–1240.
[10] Lakshminarayana, S., Kammoun, A., Debbah, M., & Poor, H. V. (2020). Data-driven false data injection attacks against power grids: A random matrix approach. *IEEE Transactions on Signal Processing, 68*, 1272–1284

BIOGRAPHIES OF AUTHORS

Manu Nair is the General Manager and Chief Technology Officer of Oregon Systems—a prominent cybersecurity distribution firm focusing on Operational Technology (OT), Industrial Control Systems (ICS), and critical infrastructure security across the Middle East , North Africa, and Apac. In his leadership role, he spearheads regional strategy, forging partnerships with global cybersecurity vendors and overseeing the implementation of advanced technologies tailored for complex industrial environments. Simultaneously, Mr. Nair is pursuing his PhD in ICS and Critical Infrastructure Security, under the guidance of Dr. Srinivasa Rao Kunte, at the Institute of Computer Science & Information Science, a distinguished department of Srinivas University, Mangaluru.

Dr. R. Srinivasa Rao Kunte holds a doctorate degree in Electronics & Communication Engineering (2001), M.Tech degree in Industrial Electronics (1984) and Bachelor's degree in Electronics & Communication Engineering (1981), all from Mysore University. His research interests include Pattern Recognition, Character Recognition, Machine Learning and AI. He has published more than 40 papers in peer reviewed journals. He has more than 40 years of academic experience in different capacities and about 24 years of research experience. Currently he is working as a Research Professor in Srinivas University, Mukka, Mangalore supervising research scholars.