IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER-PHYSICAL ATTACK DETECTION AND DECEPTION FRAMEWORK FOR WATER PLANT SCADA NETWORKS

ANBARASI.R[1], MAHALAKSHMI.V[2], SUBISHA.E[3], RAJESHWARI.S[4], KAVIYA.G[5]

[1]Assistant Professor, [2]Student,

Department of CSE, Nelliandavar Institute of Technology, Pudhuppalayam, Tamil Nadu, India

ABSTRACT - Supervisory Control and Data Acquisition (SCADA) water-treatment plants manage chemical dosing, pH and chlorine levels, and pumping operations, but increasing connectivity has exposed them to cyber risks such as unauthorized access, insider tampering, falsified sensor data, and malicious PLC commands. These attacks can silently alter treatment parameters and disrupt operations while appearing normal. Traditional SCADA security methods based on thresholds and signatures often miss slow, evolving attacks and still expose raw operational data, creating both security and privacy risks. This project proposes an intrusion detection framework that leverages a Temporal Convolutional Network (TCN) autoencoder to learn normal operating patterns across SCADA signals that are commonly targeted by Cyber-Physical Process Manipulation Attacks, including chemical dosing, pH and chlorine behavior, pump and tank dynamics, network activity, user interactions, and PLC control operations. The system learns normal plant behavior over time and automatically detects unusual changes that may indicate an attack, without needing predefined attack rules. Believable sensor readings and PLC responses are generated so that malicious commands only affect the virtual system, while the actual plant remains fully protected. This detection-then-protection strategy ensures service continuity, prevents physical damage, enables attacker behavior analysis, and significantly reduces operational risk in modern water-treatment facilities.

Keywords : Cyber-Physical Systems (CPS),SCADA Security,Water Treatment Plant Monitoring,Intrusion Detection Systems (IDS),Anomaly Detection, Deception Technology ,Honeypots,Industrial Control Systems (ICS),Network Security,Critical Infrastructure Protection,Machine Learning in Cybersecurity, Attack Mitigation Strategies,Real-Time Monitoring,Threat Intelligence.

1. INTRODUCTION

Water is one of the most precious resources on Earth, essential for all forms of life. However, growing urbanization, industrial activities, and improper waste disposal have significantly polluted water sources. This is where wastewater treatment plants (WTPs) play a vital role in protecting the environment and ensuring access to clean and safe water. A water treatment plant (WTP) is a facility designed to remove impurities, contaminants, and harmful substances from water, making it suitable for various uses such as drinking, irrigation, industrial processes, and safe discharge into the environment. These plants use advanced technologies and processes similar to the sewage treatment plant process to treat raw water, which could be sourced from rivers, lakes, groundwater, or even wastewater. SCADA, or Supervisory Control and Data Acquisition, is a sophisticated system used for monitoring and controlling industrial processes. SCADA water treatment systems are designed to collect real-time data from various sensors and devices, process and display this data, and enable remote control of equipment.

2. LITERATURE REVIEW

In this paper[1] This study proposes a comprehensive tri-phase cybersecurity framework designed to enhance the security of DNP3-based SCADA communication in smart grid environments. The framework initially performs intrusion detection by identifying abnormal network behavior within SCADA communication traffic. Once anomalies are detected, the system proceeds to a classification stage where the identified intrusions are categorized into specific
cyber-attack types. In the final phase, the framework integrates privacy-preserving mechanisms to protect sensitive operational data and metadata exchanged in SCADA communication. The effectiveness of the framework is validated using k-fold cross-validation techniques and evaluated on multiple datasets to ensure robustness and generalization. Additionally, the framework is implemented on an edge-device platform to examine its feasibility for real-time SCADA deployment scenarios.

In this paper [2], This research proposes a deep learning based anomaly detection model for identifying cyber-physical attacks in Water Distribution Systems (WDS). The approach uses a Conditional Variational Autoencoder (CVAE) architecture to learn the normal operational behavior of the water network by modeling the probability distribution of sensor measurements. The model reconstructs the input data through the encoder-decoder structure and measures reconstruction error between the original and reconstructed signals. When abnormal deviations appear, they are identified as potential cyber-physical attacks. The framework is capable of detecting attacks such as pump manipulation, tank overflow conditions, and water quality tampering that may arise from malicious SCADA control actions. The generated traffic includes multiple network-level cyber-attacks such as port scanning, brute force login attempts, ICMP flooding, SYN flooding, Xmas scanning, and IEC-104 protocol flooding.

In this paper [3], This work focuses on developing a realistic intrusion detection dataset specifically designed for SCADA networks operating under the IEC-60870-
5-104 communication protocol. The dataset is generated using a hybrid physical-virtual testbed environment consisting of real Remote Terminal Units (RTUs), Human Machine Interfaces (HMIs), and simulated control servers. The testbed produces both normal operational traffic and various attack scenarios to simulate real industrial communication behavior. The generated traffic includes multiple network-level cyber-attacks such as port scanning, brute force login attempts, ICMP flooding, SYN flooding, Xmas scanning, and IEC-104 protocol flooding. The integrity and validity of the dataset are verified using well-known intrusion detection tools including Snort and Suricata.

In this paper [4], This study introduces an adaptive intrusion detection approach for Industrial Control Systems using Deep Reinforcement Learning (DRL). Instead of relying on static classification models, the IDS learns optimal detection policies through a reward-based reinforcement learning framework. The system interacts with the SCADA dataset environment, observes network states, and selects actions to classify traffic while receiving feedback rewards for correct or incorrect decisions. Six different DRL models are trained using mini-batch sampling and reinforcement feedback to improve detection performance over time. The approach enables the IDS to dynamically adapt to evolving cyber-attack patterns in modern operational technology networks.

III. METHODOLOGY

A Natural Language Processing (NLP) module is employed to analyze textual and spoken responses, ensuring accurate understanding of candidate answers. The system incorporates a speech recognition module to convert voice input into text, followed by semantic analysis to evaluate correctness, relevance, and fluency. Simultaneously, a computer vision module captures facial expressions, eye contact, and body language using a webcam to assess non-verbal communication. These multimodal inputs are processed using machine learning and deep learning models to generate a comprehensive performance evaluation. The system also includes a feedback engine that provides real-time suggestions and improvement tips based on detected weaknesses. Additionally, adaptive questioning techniques are implemented, where the difficulty and type of questions dynamically change according to the candidate's performance. The entire framework is deployed using a cloud-based architecture to ensure scalability, accessibility, and efficient data handling. Finally, the

system stores user performance data for continuous learning and improvement, enabling personalized training over time. This methodology ensures an effective, intelligent, and user-centric interview preparation platform.

3.1. ARCHITECTURE DIAGRAM

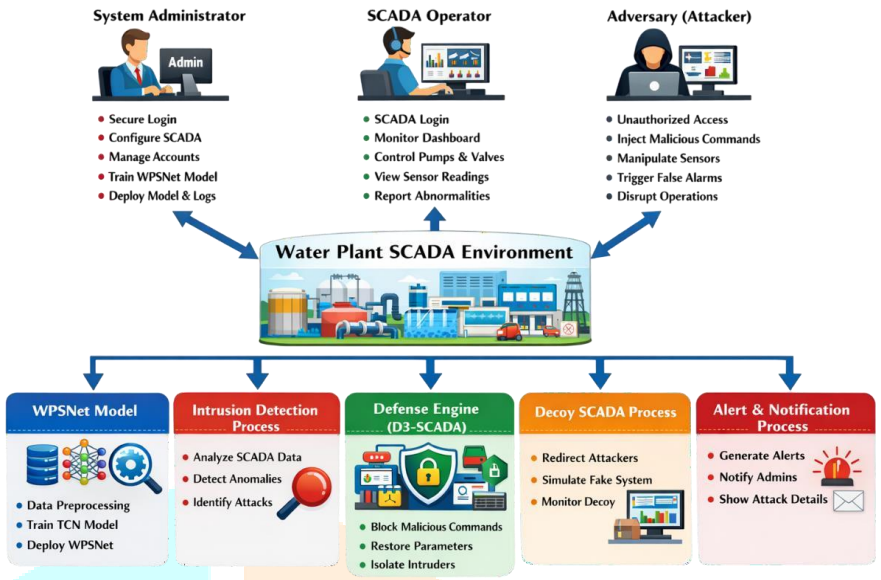


Fig : 3.3 Architecture Diagram

IV. EXPREIMENTAL RESULTS

The experimental evaluation of the AI Powered Virtual Job Interview Simulator was conducted to measure its effectiveness in improving candidate performance and providing accurate assessments. The system was tested with a diverse group of users, including students and job seekers with varying levels of experience. Multiple evaluation metrics such as accuracy, precision, recall, response time, and user satisfaction were considered to analyze system performance. The Natural Language Processing module demonstrated high accuracy in understanding and evaluating candidate responses, achieving reliable semantic interpretation. The speech recognition component performed efficiently under controlled environments, with minimal errors in transcription. The computer vision module successfully detected facial expressions and basic behavioral cues, contributing to non-verbal analysis.

4.1 IMPLEMENTATION RESULT

Water Plant SCADA Environment

This module represents the simulated operational environment of a water-treatment control system. It is developed using Python, Flask, MySQL, Bootstrap, and WAMP Server to create a web-based monitoring interface that mimics a real SCADA dashboard. The module displays important operational parameters such as pH level, chlorine concentration, tank level, pump status, valve operations, and other control signals. These parameters represent the normal functioning of the water-treatment process. The module continuously generates and updates operational data which is later analyzed by the detection system. It acts as the primary platform where system activities are monitored, recorded, and processed. These records represent both normal system behavior and abnormal conditions that may indicate cyber-physical manipulation attempts.

System User

This module manages all users who interact with the system. It controls authentication, authorization, and system access for different user roles. Each user has specific responsibilities and permissions within the system.

System Administrator

The System Administrator is responsible for managing the overall system configuration and security operations. The administrator uploads the dataset, trains the WPSNet model, and deploys the trained model into the system for real-time monitoring. This role also manages user accounts, monitors system logs, and receives alerts about suspicious activities. The administrator ensures that the system operates properly and maintains security policies.

SCADA Operator

The SCADA Operator is responsible for monitoring the operational status of the plant through the system dashboard. The operator observes real-time sensor readings such as pH levels, chlorine concentration, tank levels, and pump status. If abnormal conditions occur, the operator can view alerts generated by the system. This role focuses mainly on maintaining normal operational activities of the plant.

Adversary

The adversary represents a simulated attacker within the system. This role is used to test the security mechanisms by attempting to manipulate system parameters or inject malicious commands. The adversary may attempt actions such as altering sensor values, injecting malicious PLC commands, or triggering abnormal system behavior. These activities help evaluate the effectiveness of the intrusion detection and defense mechanisms.

WPSNet Model – Build and Train

This module focuses on developing the machine learning model used for anomaly detection. The WPSNet model is implemented using the Temporal Convolutional Network (TCN) architecture. The model is trained to learn the normal operational behavior of the control environment. After training, the model is deployed to monitor real-time system activities and detect abnormal patterns.

Dataset Import

In this submodule, the system imports the dataset containing historical operational data. The dataset includes parameters such as sensor readings, control commands, and system activities. These records represent both normal and abnormal operational behavior. The dataset is stored in the database for further processing.

Preprocessing

The preprocessing stage prepares the dataset for model training. It includes data cleaning, removal of missing values, normalization of parameters, and formatting of records into time-series format. These steps ensure that the dataset is consistent and suitable for machine learning analysis.

Feature Extraction

In this stage, important features are extracted from the dataset to improve model performance. Temporal patterns and relationships between different operational parameters are identified. Feature extraction helps the model focus on relevant information needed for anomaly detection.

Classification

This stage involves identifying patterns in the data that distinguish normal system behavior from abnormal behavior. The classification mechanism helps determine whether the system activity represents normal operations or potential intrusion attempts.

Model Training

During model training, the Temporal Convolutional Network learns the normal patterns of system behavior using the prepared dataset. The model adjusts its internal parameters through multiple training iterations. This process helps the system understand how normal operational data behaves over time.

Model Deployment

After the training process is completed, the trained model is deployed into the monitoring system. The deployed model continuously analyzes incoming operational data to detect anomalies. This allows the system to identify suspicious activities in real time.

Adversary Model (Attack Simulation)

This module simulates cyber-physical attacks within the system to test the detection and defense mechanisms. It generates malicious activities such as sensor manipulation, abnormal parameter changes, and injection of unauthorized control commands. These simulated attacks help evaluate how effectively the system can detect abnormal behavior. By simulating different attack scenarios, the system can improve its ability to recognize and respond to real-world threats.

Intrusion Detection

This module continuously monitors the operational environment to detect abnormal activities. It uses the trained WPSNet model to analyze incoming data and identify suspicious patterns.

Live Data Feeding

This submodule collects real-time operational data from the SCADA environment. Sensor readings, PLC commands, and network activities are continuously fed into the detection model for analysis.

Intrusion Detection

The detection mechanism analyzes incoming data using the trained model. The system calculates anomaly scores based on the difference between normal patterns and observed behavior. If the anomaly score exceeds a predefined threshold, the system identifies the activity as suspicious.

Attack Validation & Classification

Once abnormal behavior is detected, the system validates the intrusion and determines the type of attack. This step helps distinguish between different attack scenarios such as sensor manipulation, command injection, or abnormal parameter changes.

Defense Engine

The defense engine is responsible for protecting the system once an intrusion is detected. It activates the D3-SCADA protection mechanism which includes detection, defense, and deception strategies. The module restricts unauthorized control commands and restores safe operational parameters. It also isolates suspicious sessions to prevent further manipulation of system operations. These actions ensure that the control environment continues functioning safely during security incidents.

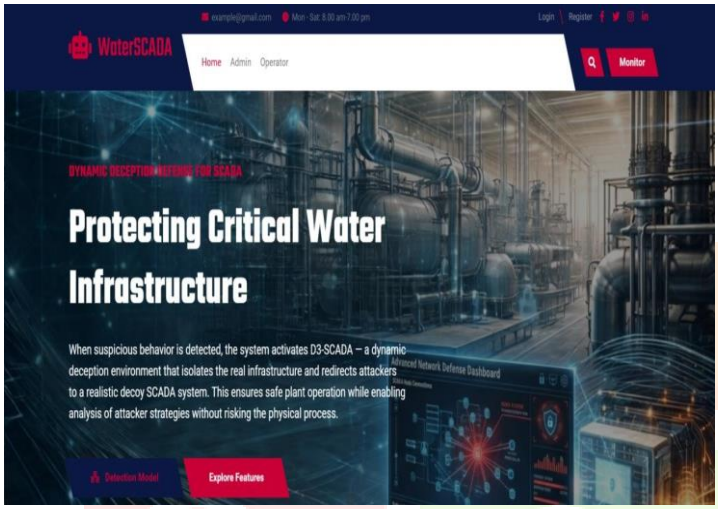
Decoy SCADA

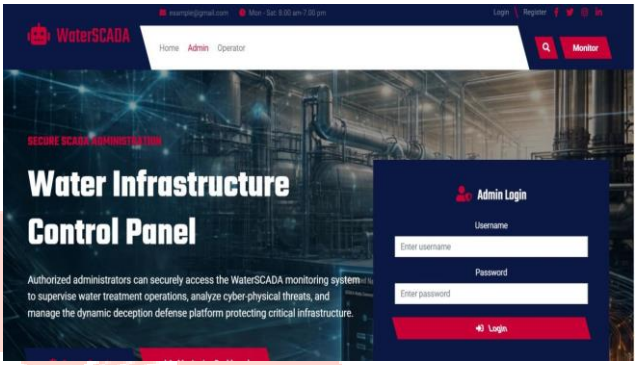
This module creates a simulated environment that mimics the behavior of the real control system. When an attack is detected, the attacker is redirected to this decoy environment. The system generates realistic sensor readings and control responses to make the attacker believe that their actions are successful. Meanwhile, the real system remains protected from manipulation. This module also allows administrators to observe attacker behavior for security analysis.

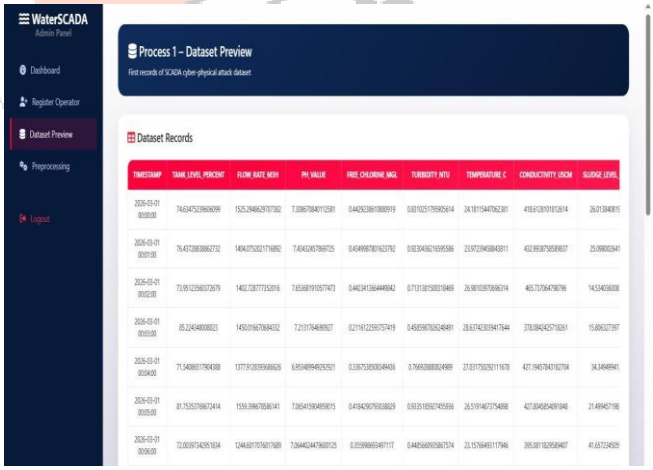
Alert and Notification

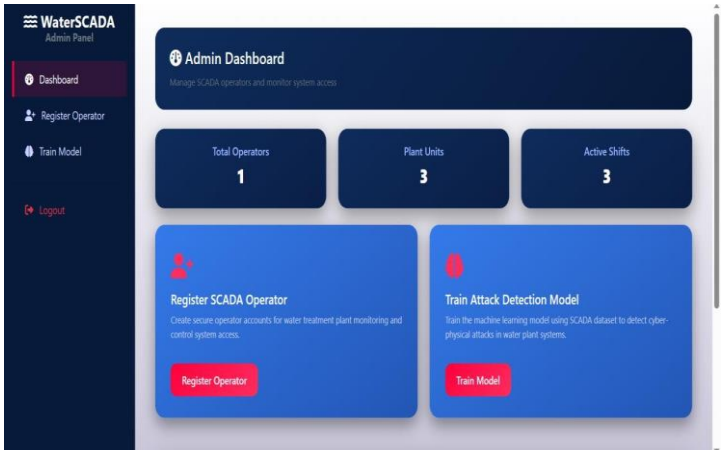
This module is responsible for informing administrators and security teams about detected intrusions. When abnormal activity is identified, the system generates alerts containing details such as attack type, affected components, anomaly scores, and system status. These alerts are displayed on the monitoring dashboard and can also be sent through email or SMS notifications. The module also records all events in system logs for monitoring, reporting, and forensic analysis.

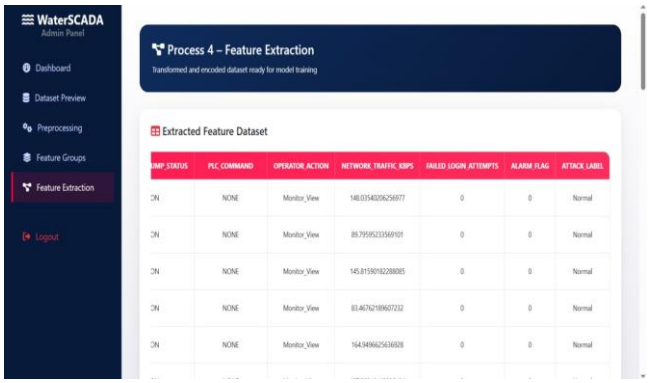
4.2 RESULT

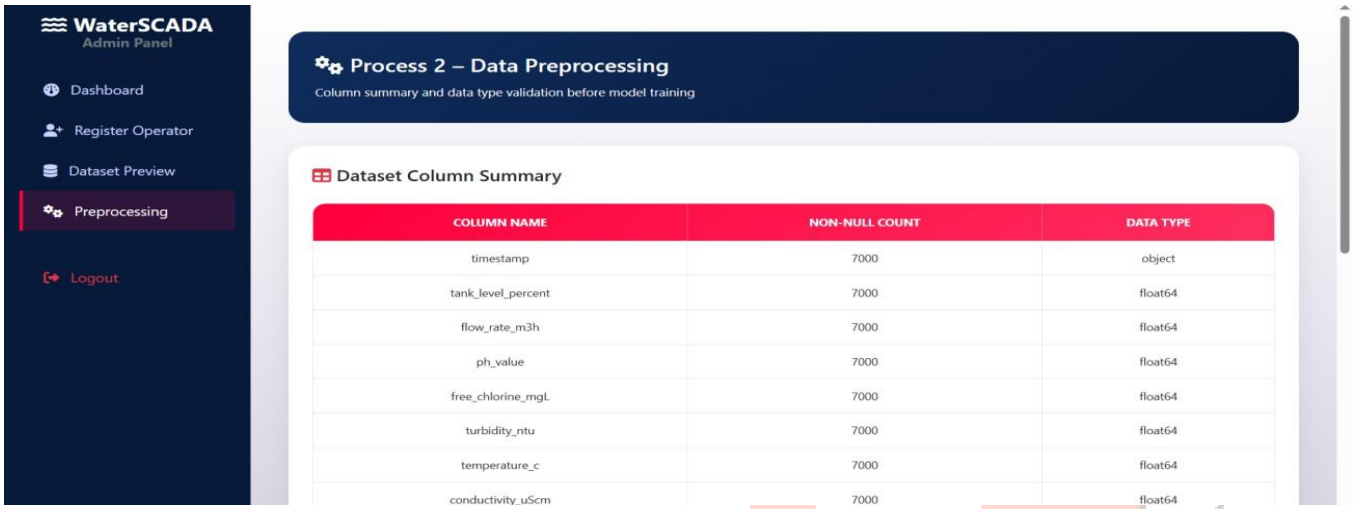


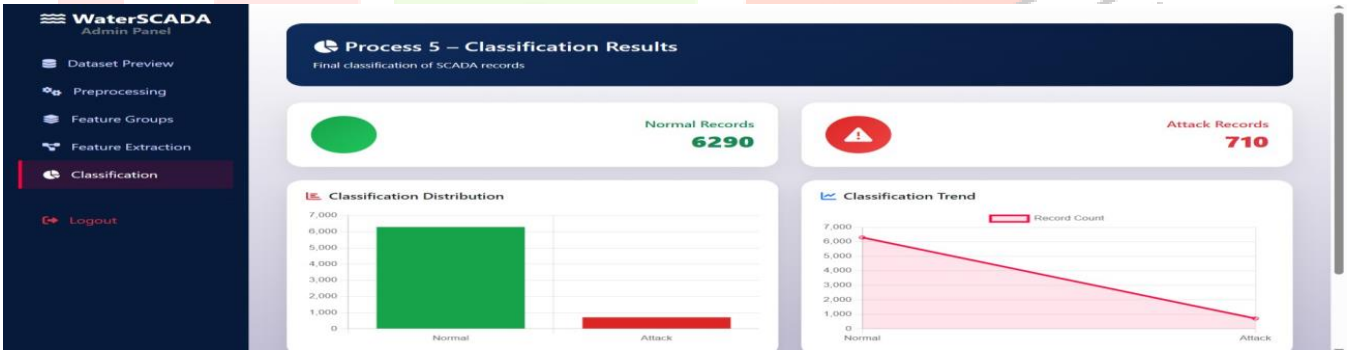





WaterSCADA
Admin Panel
Dashboard
Register Operator
Train Model
Logout
Admin Dashboard
Manage SCADA operators and monitor system access
Total Operators
1
Plant Units
3
Active Shifts
3
Register SCADA Operator
Create secure operator accounts for water treatment plant monitoring and control system access.
Register Operator
Train Attack Detection Model
Train the machine learning model using SCADA dataset to detect cyber-physical attacks in water plant systems.
Train Model


WaterSCADA
Admin Panel
Dashboard
Dataset Preview
Preprocessing
Feature Groups
Feature Extraction
Logout
Process 4 – Feature Extraction
Transformed and encoded dataset ready for model training
Extracted Feature Dataset
PUMP_STATUS
PLC_COMMAND
OPERATOR_ACTION
NETWORK_TRAFFIC_KBPS
FAILED_LOGIN_ATTEMPTS
ALARM_FLAG
ATTACK_LABEL


WaterSCADA
Admin Panel
Dashboard
Register Operator
Dataset Preview
Preprocessing
Logout
Process 2 – Data Preprocessing
Column summary and data type validation before model training
Dataset Column Summary
COLUMN NAME
NON-NULL COUNT
DATA TYPE
timestamp 7000 object
tank_level_percent 7000 float64
flow_rate_m3h 7000 float64
ph_value 7000 float64
free_chlorine_mgL 7000 float64
turbidity_ntu 7000 float64
temperature_c 7000 float64
conductivity_uScm 7000 float64


WaterSCADA
Admin Panel
Dataset Preview
Preprocessing
Feature Groups
Feature Extraction
Classification
Logout
Process 5 – Classification Results
Final classification of SCADA records
Normal Records
6290
Attack Records
710
Classification Distribution
Classification Trend
Record Count
Normal
Attack


Water Treatment System
Monitoring

V. CONCLUSION

In conclusion, this project presents an intelligent framework for securing a SCADA-based water-treatment control environment against cyber-physical attacks. The system integrates advanced machine learning techniques and automated defense mechanisms to monitor operational data and detect abnormal behavior. The Temporal Convolutional Network (TCN) based WPSNet algorithm is used to analyze time-series operational data and identify deviations from normal system patterns. By learning the normal behavior of parameters such as sensor readings, control commands, and operational activities, the algorithm effectively detects suspicious events with high accuracy. Once an intrusion is detected, the D3-SCADA algorithm activates a multi-layered protection strategy that includes detection, defense, and deception. The defense engine secures the real system by restricting unauthorized control commands and restoring safe operational parameters. At the same time, the deception mechanism redirects attackers to a simulated decoy environment that mimics the behavior of the real system. This approach prevents attackers from interacting with the actual infrastructure while allowing administrators to observe malicious activities. The performance evaluation results demonstrate that the system achieves high detection accuracy and reliable security protection.

FUTURE ENHANCEMENT

The system can be enhanced by integrating it directly with real industrial control hardware such as PLCs, RTUs, and edge computing devices. Deploying the detection and protection framework closer to the operational devices allows faster data analysis and immediate response to abnormal activities. This reduces dependency on centralized servers and improves the overall resilience of the control environment. Future versions of the system can include AI-driven dashboards that assist operators in making better decisions during security incidents. These dashboards can visualize attack impact, display system health indicators, and recommend appropriate response actions.

REFERENCE

1. X. Yin, L. Zhang, Z. Liu, J. Qiu, and C. Wang, “A novel transformer model enhanced by scaled-CNN and Bi-LSTM hybrid networks for real-time threat identification within SCADA systems”, IEEE Access, vol. 13, pp. 196579–196593, 2025.
2. J. Vaasudevan, H. Manukonda, A. Pallakonda, R. D. Amar Raj, R. M. R. Yanamala, R. Nazari, and K. K. Prakasha, “A holistic framework for cyber attack detection, classification, and security enhancement of DNP3 protocol in smart grids”, IEEE Access, vol. 13, pp. 200177–200195, 2025.
3. F. Sangoleye, J. Johnson, and E. E. Tsiropoulou, “Intrusion detection in industrial control systems based on deep reinforcement learning”, IEEE Access, vol. 12, pp. 151444–151460, 2024.
4. M. A. S. Arifin, D. Stiawan, B. Y. Suprapto, S. Susanto, T. Salim, M. Y. Idris, M. Shenify, and R. Budiarto, “A novel dataset for experimentation with intrusion detection systems in SCADA networks using IEC 60870-5-104 standard”, IEEE Access, vol. 12, pp. 170553–170566, 2024.
5. H. H. Addeen, Y. Xiao, and T. Li, “A CVAE-based anomaly detection algorithm for cyber physical attacks for water distribution systems”, IEEE Access, vol. 12, pp. 48321–48335, 2024.
6. N. Al-Qirim, A. Bani-Hani, M. Majdalawieh, H. Al Hamadi, and M. K. Hasan, “DiGraph-enabled digital twin and label-encoding machine learning
7. for SCADA network’s cyber attack analysis in Industry 5.0”, IEEE Open Journal of the Communications Society, vol. 6, pp. 3404–3420, 2025.
8. R. Taksana, N. Janjamraj, S. Romphochai, K. Bhumkittipich, and N. Mithulananthan, “Design of power transformer fault detection of SCADA alarm using fault tree analysis, smooth Holt–Winters, and L-BFGS for smart utility control centers”, IEEE Access, vol. 12, pp. 116302–116315, 2024.

9. D. G. Eliades, K. Malialis, S. Vrachimis, and M. M. Polycarpou, “Smart water networks as cyber-physical-socio-environmental systems”, IEEE Transactions on Industrial Cyber-Physical Systems, vol. 3, pp. 95–104, 2025.
10. B. Miller and D. Rowe, “A survey of SCADA and critical infrastructure incidents, Proc”. 1st Annual Conference on Research in Information Technology, pp. 51–56, 2012.
11. R. Mitchell and I. Chen, “A survey of intrusion detection techniques for cyber-physical systems”, ACM Computing Surveys, vol. 46, no. 4, pp. 1–29, 2014.