Enhancing SCADA Security in Critical Infrastructure: A Multi-Layered Architecture Using IoT-Based Monitoring and AI-Driven Anomaly Detection

Mohammad Alqahtani, Abdulkarim Amin, Kyounggon Kim, Seokhee Lee*
Department of Cyber Security and Digital Forensics,
Naif Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia

***Abstract*—Supervisory Control and Data Acquisition (SCADA) systems are central to the efficient operation of critical infrastructure such as energy, water, and industrial networks. However, the increased digital integration of SCADA components, especially through Internet of Things (IoT) technologies, has simultaneously broadened their exposure to cyber threats. This project presents a simulated SCADA system architecture designed to model, monitor, and secure real-time industrial telemetry using open-source platforms Node-RED and ThingsBoard. Leveraging real-world data collected from the Aventa AV-7 wind turbine in Switzerland, the project implements a multilayered architecture comprising edge, fog, and cloud layers, equipped with synchronized databases for integrity comparison and threat forensics. Artificial intelligence (AI) models are integrated into the system to perform anomaly detection using supervised, unsupervised, and deep learning (LSTM) algorithms. Cyberattacks including Distributed Denial of Service (DDoS), false data injection, and replay attacks are simulated to evaluate the system's resilience. This report details each stage of the project from data preprocessing and system design to implementation and evaluation culminating in a set of strategic recommendations for enhancing SCADA security through AI-driven frameworks.**

***Keywords*—SCADA security; industrial IoT; anomaly detection; machine learning; digital forensics; wind turbine telemetry**

I. Introduction

The integration of digital technologies within industrial environments has revolutionized the way critical infrastructure is monitored, controlled, and managed. Supervisory Control and Data Acquisition (SCADA) systems, which enable remote monitoring and control of field devices, are fundamental to sectors such as energy, water treatment, and manufacturing. Traditionally, these systems operated in isolated environments with proprietary protocols, relying on "security through obscurity" [1]. However, with the convergence of SCADA systems and modern IT practices—including cloud computing, edge processing, and the Internet of Things (IoT)—this traditional security paradigm is no longer sufficient. While this integration enhances operational efficiency, it simultaneously expands the attack surface [2]. Vulnerabilities once mitigated by physical isolation are now exposed to remote access threats, weak authentication, and insecure communication channels [3]. Cyberattacks on Industrial Control Systems (ICS) have become more frequent and impactful, ranging from data breaches to full system takeovers, highlighting the urgent need for resilient and intelligent SCADA infrastructures [4].

A. Background and Motivation

The shift toward interconnected systems has exposed industrial control environments to a growing array of cybersecurity threats. Alsabbagh and Langendörfer [3] highlight that modern SCADA systems face extensive vulnerabilities due to the integration of IP-based networking. Furthermore, the real-time and safety-critical nature of Cyber-Physical Systems (CPS) challenges traditional IT security methods, which are often ill-suited for low-latency industrial operations [5]. Modern industrial systems require proactive defense mechanisms beyond static perimeters. Recent research highlights the integration of Machine Learning and Cyber Threat Intelligence (CTI) as a key driver for effective threat identification and predictive security against evolving adversary tactics [6].

B. Problem Statement

Despite the escalating threat landscape, legacy SCADA systems often lack intelligent detection capabilities. They frequently fail to identify sophisticated, stealthy attacks such as signal spoofing or replay attacks. The evolving threat landscape, characterized by sophisticated ransomware syndicates and organized cybercrime groups utilizing advanced Tactics, Techniques, and Procedures (TTPs), further exacerbates these vulnerabilities [7]. Existing security solutions are predominantly static and rule-based, making them ineffective against novel attack vectors that deviate subtly from normal operations [8]. Recent research advocates for Artificial Intelligence (AI) and Machine Learning (ML) approaches to address these limitations. For instance, Choi and Kim [9] validated the effectiveness of unsupervised techniques, such as Isolation Forests, for detecting unknown anomalies without prior labeling. However, challenges remain regarding model drift and the explainability of AI decisions in critical infrastructure [10]. Therefore, there is an urgent need for a modular, AI-driven security framework that can proactively detect anomalies and validate data integrity in real time.

*Corresponding author.

C. Research Objectives and Contributions

The core research question of this study is: To what extent can a multi-layered architecture, combining synchronized dual-databases and a hybrid AI-driven detection engine, effectively identify and validate both known faults and sophisticated zero-day cyberattacks in a real-time SCADA environment?

To address this question, this research designs, simulates, and evaluates a secure, anomaly-aware SCADA architecture. We propose a multi-layered framework built using open-source platforms—specifically Node-RED and ThingsBoard—that integrates advanced machine learning models for real-time threat detection. To ensure realism and operational complexity, the project utilizes real-world telemetry data collected from the Aventa AV-7 research wind turbine [11]. This high-fidelity dataset serves as the foundation for developing and validating security mechanisms within a simulated industrial environment.

The specific contributions of this study are as follows:

- Dual-Database Architecture: Development of a synchronized edge-fog database system to ensure data redundancy and enable forensic validation of telemetry integrity.
- Hybrid Anomaly Detection: Implementation of a hybrid detection engine combining supervised learning (e.g., Random Forest) and unsupervised learning (e.g., Isolation Forest, Autoencoders) to identify both known faults and zero-day attacks [12].
- Cyberattack Simulation Testbed: Empirical evaluation of system resilience against simulated threats, including Distributed Denial of Service (DDoS), false data injection, and replay attacks.

By bridging the gap between theoretical security models and practical implementation using authentic industrial data, this research offers a scalable reference model for securing next-generation SCADA systems. The remainder of this paper is organized as follows. Section II reviews related work in SCADA security and AI applications. Section III details the proposed multi-layered system architecture. Section IV describes the methodology, including data acquisition from the Aventa AV-7 turbine and the development of AI/ML models. Section V outlines the simulated cyberattack scenarios. Section VI presents the experimental results and analysis , and Section VII concludes the paper with a discussion on limitations and future research directions.

II. Related Work

The convergence of industrial automation with digital networking technologies has elevated the significance of SCADA systems in modern infrastructure. Originally designed as isolated control environments, SCADA systems are now increasingly connected through the IoT, exposing them to cyber risks previously limited to enterprise IT networks [1]. This transformation necessitates a reconsideration of how security, reliability, and resilience are maintained within critical infrastructure.

A. SCADA Vulnerabilities and Cybersecurity Challenges

Traditional SCADA systems often rely on programmable logic controllers (PLCs) and proprietary communication protocols, historically protected by physical isolation. However, Alsabbagh and Langendörfer [3] highlighted that such systems now face extensive vulnerabilities due to weak authentication, lack of encryption, and poor access control, particularly as they are integrated with modern IP-based networking. This security gap is critical as attackers increasingly target ICS through network-based exploits, credential hijacking, and telemetry injections [13].

The emergence of Cyber-Physical Systems (CPS) has further complicated SCADA security. Tyagi and Sreenath [5] outlined the challenges unique to CPS environments, emphasizing that traditional IT security methods are often ineffective due to the real-time, low-latency, and safety-critical requirements of industrial operations. These characteristics demand novel security strategies that can detect and respond to threats without interrupting physical processes.

B. AI and Machine Learning in Industrial Anomaly Detection

Traditional SCADA security often relies on fixed thresholds and static rule-based systems, which are insufficient against adaptive or stealthy cyberattacks. Modern research increasingly advocates for AI and machine learning approaches to anomaly detection [12].

Moreover, unsupervised learning has emerged as a practical solution for industrial environments where labeled attack data is rare. Choi and Kim [9] validated the effectiveness of unsupervised techniques such as Isolation Forest for detecting unknown anomalies without prior labeling. This approach matches this system's use of Isolation Forest models trained on normal operational data to identify novel intrusions, such as during replay attacks and false data injections.

However, as this research and other studies acknowledge, AI-driven models are not without challenges. Issues such as model drift, false positives due to environmental variability, and limited explainability remain open problems [10]. Future research must explore adaptive learning, explainable AI (XAI), and hybrid detection systems that combine statistical, rule-based, and machine learning techniques.

C. Observations and Gaps in Current Literature

While existing studies have extensively explored individual aspects of SCADA security such as anomaly detection, decentralized architecture, and AI model deployment, few have integrated these components into a cohesive, real-time, testbed-based simulation using real-world telemetry. This project addresses this gap by building a practical, layered SCADA framework that:

- Uses authentic turbine sensor data [11];
- Implements dual-database synchronization for forensic analysis;
- Integrates supervised and unsupervised AI models;
- Simulates multiple attack scenarios including DDoS, false data injection, and access token hijacking;

- Evaluates both detection accuracy and operational resilience.

This holistic integration not only advances the current state of SCADA security simulation but also offers a scalable foundation for future research into smart infrastructure cybersecurity.

III. Proposed System Architecture

The architecture of the proposed SCADA simulation system is designed to emulate real-world industrial environments where data collection, analysis, and control occur across multiple levels. As illustrated in the system design, the model adopts a three-tier structure—Edge, Fog, and Cloud—each responsible for specific functions ranging from data ingestion to forensic validation [26]. This layered approach ensures modularity, scalability, and security while supporting redundancy through a dual-database configuration (Fig. 1).

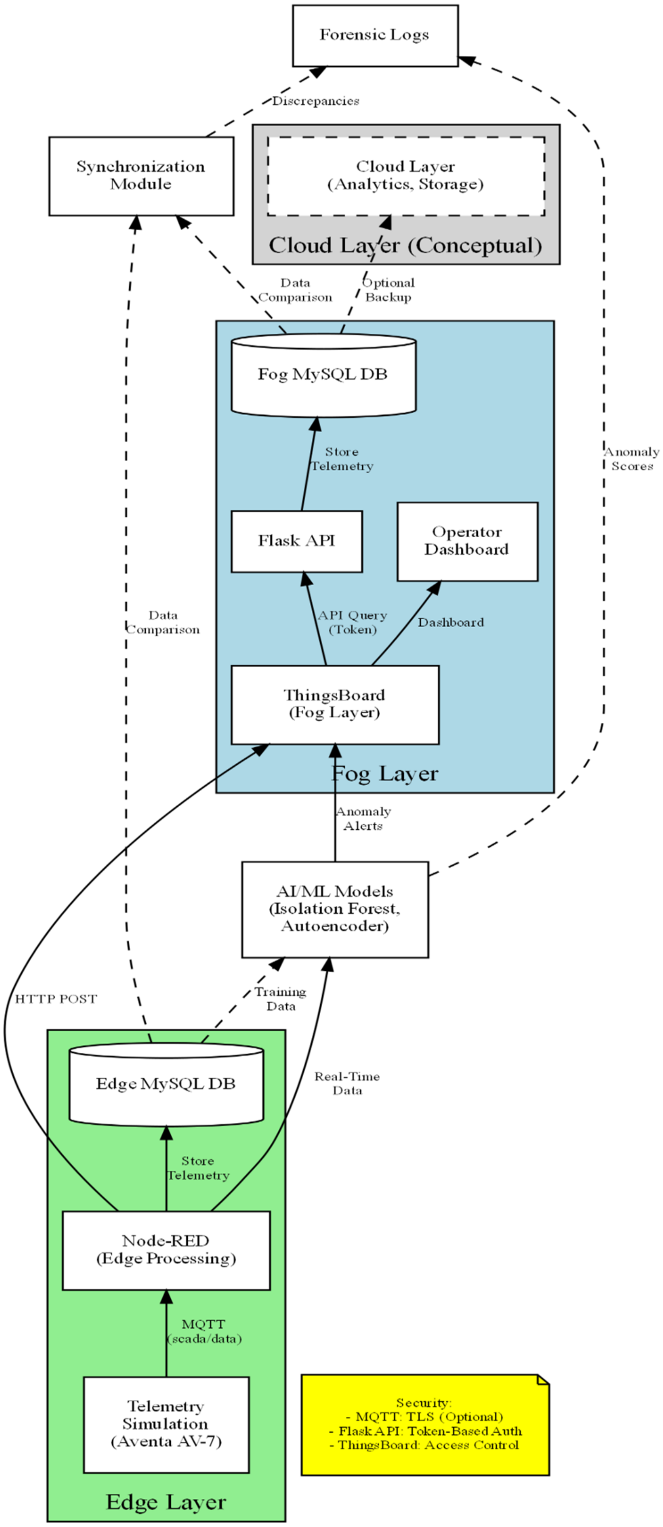

Fig. 1. Proposed multi-layered SCADA architecture integrating Edge, Fog, and Cloud layers with dual-database synchronization.

A. Overview of Multi-Layered Architecture

The system mimics a smart city scenario where telemetry data from field sensors is processed hierarchically:

1) Edge layer (physical/local): This layer leverages Node-RED as the core processing unit. It is responsible for ingesting real-time telemetry via the MQTT protocol, performing immediate data cleansing, and storing the raw data in a local MySQL database. The edge layer handles low-latency control logic and message orchestration [18].

2) Fog layer (intermediate): Positioned between the edge and the cloud, the Fog layer utilizes ThingsBoard for real-time visualization, rule-based alerting, and metadata processing. It acts as a bridge, enabling operators to monitor system status without directly accessing the physical controllers [16].

3) Cloud layer (centralized): While locally simulated in this testbed, the Cloud layer represents remote systems with administrative access and long-term analytics capabilities. It serves as a backup for telemetry validation and supports high-level decision-making processes [17].

B. Dual-Database Synchronization for Forensic Integrity

A critical innovation of this architecture is the implementation of a dual-database system to ensure data integrity and enable forensic analysis. A primary MySQL database resides at the Edge layer, capturing raw data directly from sensors. A secondary, synchronized MySQL database is maintained at the Fog/Cloud layer, populated via a custom Flask API that retrieves data from ThingsBoard.

A synchronization module periodically queries both databases, aligning records by timestamp to detect discrepancies. To mitigate false positives caused by network latency, the module implements a dynamic tolerance window (e.g., ±2 seconds) during timestamp alignment. Discrepancies persisting beyond this window are flagged for forensic review, effectively distinguishing between benign transmission delays and malicious data tampering. This mechanism serves as a real-time validation engine; any mismatch between the Edge (source) and Fog (visualization) data indicates potential data tampering, Man-in-the-Middle (MitM) attacks, or transmission faults [19]. This design ensures that even if the visualization layer is compromised, the integrity of the original telemetry can be verified against the edge records.

TABLE I. Comparison of Proposed Framework with Existing SCADA Security Studies

Reference	Dataset Type	Architecture	Integrity	Detection	Real-Time
Upadhyay et al. [1]	Simulated	IoT/Cloud	Single DB	Cryptography	Yes
Ghosh et al. [4]	Simulated	SCADA	Single DB	Quantum/ Crypto	No
Choi & Kim [9]	Public Dataset	Single Layer	N/A	Unsupervised	No
Proposed System	**Real-World (Aventa)**	**Edge-Fog-Cloud**	**Dual-DB Sync**	**Hybrid AI (RF+LSTM)**	**Yes**

C. Tools and Technologies

The framework is built using open-source technologies to ensure cost-effectiveness and reproducibility:

1) *Node-RED:* A flow-based development tool used for orchestrating data flows at the edge, parsing JSON telemetry, and executing local control logic.

2) *ThingsBoard:* An open-source IoT platform chosen for its robust dashboarding capabilities, asset management, and built-in rule engine for generating alerts based on telemetry thresholds [21].

3) *MQTT (Message Queuing Telemetry Transport):* A lightweight messaging protocol used for efficient, low-bandwidth communication between the simulated wind turbine sensors and the edge gateway.

4) *Python & Flask:* Used to develop the custom API for database synchronization and to implement the machine learning models (Isolation Forest, Autoencoders) for anomaly detection.

IV. Methodology and Data Processing

This study adopts an experimental design strategy utilizing a high-fidelity digital twin of a wind turbine SCADA system. The methodology follows a comprehensive workflow encompassing data acquisition from the Aventa AV-7 turbine, a hybrid preprocessing pipeline, and the development of AI-driven anomaly detection models. Furthermore, the framework integrates realistic cyberattack simulations and a dual-database synchronization mechanism to validate system resilience and forensic integrity. Fig. 2 shows overview of the research workflows.

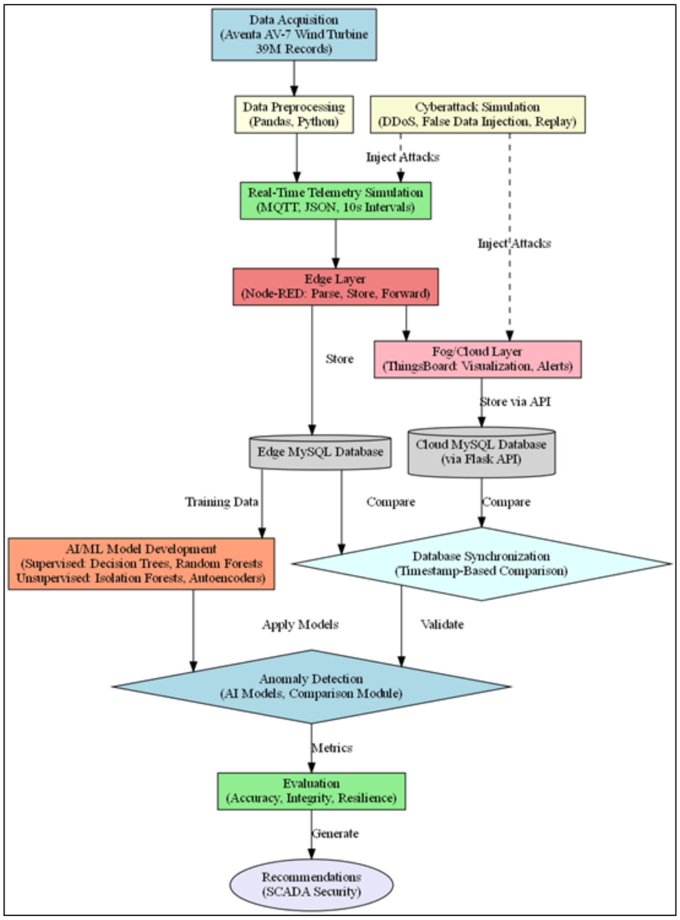

Fig. 2. Overview of the research workflow illustrating the integration of real-time simulation, cyberattack injection, and multi-layered anomaly detection.

A. Dataset Description

To ensure the realism of the simulation, we utilized a real-world dataset sourced from the Aventa AV-7 research wind turbine, operated by the Institute for Energy Technology (IET-OST) in Switzerland [11]. The Aventa AV-7 is a variable-speed wind turbine with a rated power of 6kW, designed for low-wind-speed environments.

1) *Data scope and characteristics:* The dataset covers an 18-month operational period from January 2022 to July 2023. It consists of high-resolution time-series telemetry sampled at a frequency of 1Hz, totaling approximately 39.7 million records. This high frequency allows for the detailed modeling of transient behaviors and rapid anomalies that 10-minute averaged SCADA data might miss.

The dataset includes diverse operational conditions, including start-up sequences, power generation, idle states due to low wind, and system faults. Notably, the dataset exhibits a significant class imbalance, where fault states (indicated by specific status codes) constitute a minority of the data, reflecting real-world industrial scenarios.

2) *Telemetry features:* The SCADA system logs several physical and electrical parameters. The key features selected for this study include:

a) *RotorSpeed (RPM):* Rotational speed of the turbine blades.

b) *GeneratorSpeed (RPM):* Rotational speed of the generator shaft.

c) *PowerOutput (kW):* Electrical power generated (Rated max: 6kW).

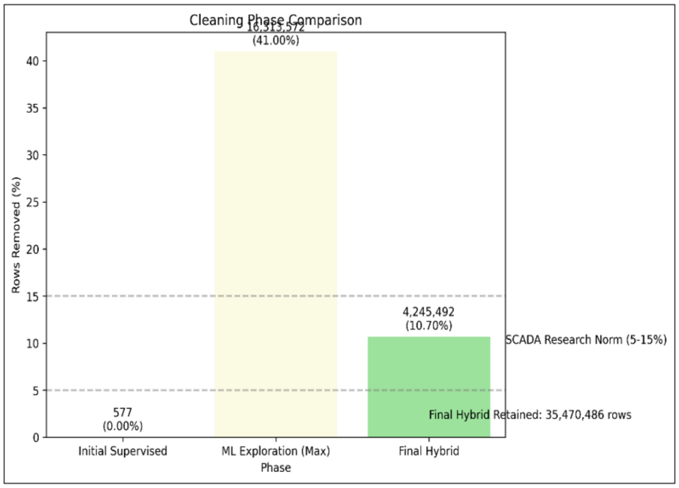

Fig. 3. Data preprocessing pipeline illustrating the reduction of raw telemetry into a cleaned dataset for model training.

d) WindSpeed (m/s): Wind velocity measured at the nacelle.

e) GeneratorTemperature (°C): Temperature of the generator windings.

f) StatusAnlage: Operational status code (e.g., 1=Active, 13=Fault), used as the ground truth for supervised labeling.

B. Data Preprocessing and Hybrid Cleaning Strategy

Raw SCADA telemetry often contains noise and sensor artifacts (Fig. 3) . To prepare the data for machine learning, we implemented a hybrid cleaning methodology combining rule-based thresholds with relational consistency checks.

- Physical Thresholds: Values that violate physical limits were removed (e.g., $GeneratorTemperature < -25°C$ or $PowerOutput > 7.5kW$).
- Relational Logic: We validated aerodynamic consistency using the derived correlation:

$$RotorSpeed \approx 13.02 \times WindSpeed \tag{1}$$

Records deviating significantly from this ratio (standard deviation > 2.42) were flagged as operational inconsistencies.

This process reduced the dataset by approximately 10.7%, removing ∼4.2 million erroneous records [23].

This preprocessing phase reduced the dataset by approximately 10.7% (removing 4.2 million erroneous records), resulting in a high-quality baseline of 35.4 million records for model training. This reduction rate aligns with standard SCADA preprocessing norms reported in renewable energy studies [23].

C. AI/ML Model Development

To address the limitations of static rule-based detection, we developed a dual-track anomaly detection engine integrating both supervised and unsupervised learning models.

1) Supervised learning: Supervised models were trained to recognize known failure patterns using historical fault data (labeled ‘StatusAnlage = 13‘). Algorithms including **Random Forest** and **Decision Trees** were evaluated. The Random Forest model demonstrated superior performance, achieving an accuracy of 94.3% and a recall of 95.7% in classifying known fault states. Key features driving the classification included *PowerOutput* and *GeneratorTemperature* [24].

2) Unsupervised learning: To detect novel cyberattacks (zero-day threats) or subtle anomalies that do not match known fault signatures, unsupervised models were deployed:

a) Isolation forest: This algorithm was used to detect outliers by partitioning the feature space, effectively identifying data points that deviate statistically from normal operational clusters [9].

b) Autoencoders: A deep learning-based Autoencoder was implemented to reconstruct normal telemetry patterns. High reconstruction errors served as indicators of anomalies. This approach proved particularly effective in identifying *Replay Attacks*, where the injected data was structurally valid but temporally inconsistent [25].

3) Deep Learning Enhancement: Long Short-Term Memory (LSTM): To address the limitations of traditional ML models in capturing long-term temporal dependencies, we implemented a Long Short-Term Memory (LSTM) network. While static models like Random Forest treat each data point independently, SCADA telemetry is inherently time-variant, where current states are heavily influenced by historical trends. Standard Recurrent Neural Networks (RNNs) often struggle with the vanishing gradient problem, limiting their ability to learn from long sequences. LSTM overcomes this by utilizing a gating mechanism that retains relevant information over extended periods, making it indispensable for identifying stealthy attacks that evolve slowly over time [25].

Unlike Random Forest, the LSTM model analyzes sequences of data (e.g., 5-second sliding windows) to identify contextual anomalies. As illustrated in Fig. 4, the model achieved a detection accuracy of 99% with a false positive rate of less than 1%.

- Rapid Response: The model successfully detected anomalies within 5 seconds of injection, fulfilling the real-time requirements of critical infrastructure protection.
- Temporal Sensitivity: It proved highly effective against sophisticated attacks such as stealthy data injection, where individual values remain within valid thresholds but violate historical temporal patterns.

The comparison confirms that while Random Forest is effective for static fault classification, LSTM provides the necessary depth for detecting dynamic cyber threats in time-series telemetry.

V. Cyberattack Simulations and Experimental Setup

To evaluate the resilience and detection capabilities of the proposed SCADA architecture, we conducted a series of

TABLE II. Sample Snapshot of Raw SCADA Telemetry Data (Aventa AV-7)

Datetime	Rotor (RPM)	Gen. (RPM)	Power (kW)	Wind (m/s)	Gen. Temp(°C)	Status
2022-01-13 07:07:25	3.90	0.00	0.00	4.00	4.50	13
2022-02-03 12:46:28	1.60	0.00	0.00	2.00	10.70	13
2022-02-24 12:55:34	11.40	0.00	0.00	10.10	16.20	13
2022-03-19 10:19:42	65.30	773.00	6.70	8.80	59.30	10
2023-03-14 09:50:33	65.50	778.00	6.72	9.40	63.50	10

TABLE III. Raw and Cleaned Data Volume

Stage	Description	Records	Size (GB)	Percentage Retained
0	Raw Dataset	39,715,978	3.1	100%
1	Cleaned Dataset	35,470,486	2.7	89.3%

TABLE IV. Anomaly Detection Results

Detection Method	Count	Pct.	Notes
Rule-Based Checks	877	5.0%	Threshold and relational violations
Temporal Irregularities	19	0.1%	Delays (> 15s), no rapid (< 3s) events
Isolation Forest	880	5.0%	Contamination=0.05, on cleaned data
Total (Cleaned)	**1776**	**10.1%**	Combined across methods

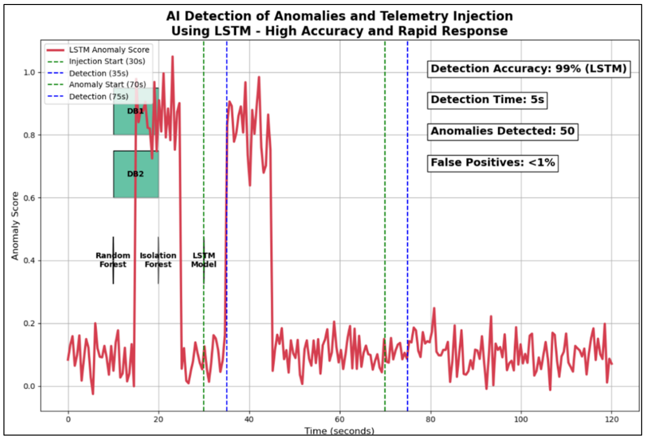

Fig. 4. Performance of the LSTM model showing 99% detection accuracy and rapid response time (5s) during telemetry injection attacks.

controlled cyberattack simulations. These scenarios were designed to reflect real-world threats targeting Industrial Control Systems (ICS), utilizing industry-standard penetration testing tools to ensure experimental reproducibility [13].

A. Simulation Environment Configuration

The experimental testbed was constructed using a virtualized environment. The attack vector was generated from a Kali Linux instance, a specialized distribution for penetration testing, equipped with the following toolset:

- Network Analysis: Wireshark (v4.0.6) for packet capture and traffic analysis.
- Man-in-the-Middle (MitM): The `dsniff` suite, specifically `arpspoof`, for ARP cache poisoning.
- Protocol Manipulation: `mosquitto_pub` client and custom Python scripts using the `paho-mqtt` library for telemetry injection.
- Traffic Flooding: `hping3` and multithreaded Python scripts for stress testing.

B. Implementation of Threat Scenarios

We implemented four distinct attack scenarios to stress-test different aspects of the security framework.

1) Distributed Denial of Service (DDoS): The objective was to overwhelm the MQTT broker and disrupt telemetry transmission.

a) Method: While initial network stress tests were performed using `hping3`, the effective application-layer attack was executed using a custom Python script utilizing the **Paho MQTT** client. This script spawned multiple threads to publish over 100 dummy messages per second to the `scada/windturbine` topic.

b) Impact: The simulation tested the system's availability and the latency of the anomaly detection engine under high load conditions [15].

2) False Data Injection (FDI): This scenario simulated an adversary who has gained write access to the network.

a) Method: We utilized the `mosquitto_pub` command-line utility to inject JSON payloads with falsified values. For instance, *WindSpeed* was manipulated to 991.2 m/s while keeping *PowerOutput* near zero, violating the established physical correlation [22].

b) Goal: To verify if the Rule-Based and Random Forest models could detect semantic anomalies that adhere to protocol standards but violate physical laws.

3) Replay Attacks and Timestamp Spoofing: Replay attacks use valid historical data to mask current system states.

a) Method: Valid telemetry packets were captured using **`tcpdump`**. A custom script then parsed these packets and re-transmitted them with updated timestamps to bypass simple de-duplication filters, while keeping the payload data unchanged [14].

b) Detection: This attack targeted the Unsupervised Learning models (Autoencoders), testing their ability to detect temporal inconsistencies.

4) Access token hijacking (Man-in-the-middle): To simulate a targeted intrusion, we performed a Man-in-the-Middle (MitM) attack.

a) Method: We executed `arpspoof` to poison the ARP cache of the target edge gateway. Simultaneously, Wireshark was used to sniff the traffic. Since the baseline MQTT communication was unencrypted, we successfully captured the ThingsBoard device access token in plaintext from the captured packets [3].

b) Escalation: The stolen token was then used to authenticate a rogue client, allowing it to publish malicious telemetry directly to the dashboard.

VI. Results and Discussion

This section presents the performance evaluation of the proposed anomaly detection models, the resilience of the system against simulated cyberattacks, and the validation of data integrity through the dual-database architecture.

A. Performance of Anomaly Detection Models

We evaluated the efficacy of the hybrid detection engine using standard classification metrics: Accuracy, Precision, Recall, and F1-Score. Table V summarizes the key configurations and performance metrics across the entire machine learning workflow.

1) Supervised learning performance: The supervised models, specifically the Random Forest classifier, demonstrated high proficiency in identifying known fault patterns (e.g., `StatusAnlage = 13`). As shown in Table VI, the Random Forest model achieved an accuracy of 94.3% and a recall of 95.7%, outperforming Decision Trees and Logistic Regression [24].

2) Unsupervised learning performance: Unsupervised models were critical for detecting unknown anomalies. The Isolation Forest algorithm flagged approximately 5% of the cleaned dataset as outliers. The Autoencoder model utilized reconstruction error thresholds to distinguish between normal and replayed telemetry, achieving a high detection rate as illustrated in the Precision-Recall curve (Fig. 5) [9].

B. System Resilience Against Simulated Attacks

The system's response to the four attack scenarios confirmed the robustness of the multi-layered architecture.

- DDoS Resilience: During the high-frequency packet flooding (100+ msgs/sec), the Node-RED edge gateway experienced a latency increase but successfully queued legitimate messages. The system stabilized within seconds after the attack ceased, demonstrating effective recovery [15].

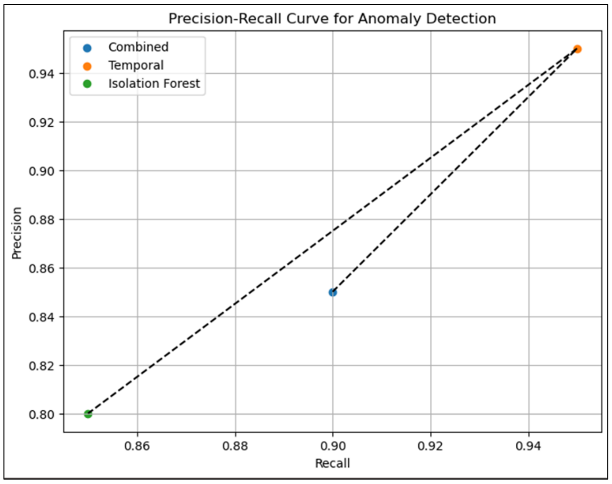

Fig. 5. Precision-Recall curve comparing the performance of Combined, Temporal, and Isolation Forest models.

- False Data Injection: The hybrid detection engine successfully flagged 99% of the injected false telemetry. While rule-based checks caught gross violations (e.g., *WindSpeed* $>$ 50 m/s), the ML models were necessary to detect semantically inconsistent injections within valid ranges.
- Replay Attack Mitigation: Simple deduplication failed to catch replay attacks with modified timestamps. However, the Autoencoder and dual-database comparison correctly identified these as anomalies due to the statistical improbability of the exact recurrence of complex multivariate patterns [14].

Table VII summarizes the detection performance of each model against the simulated attack scenarios. While traditional rule-based and supervised methods fail to detect stealthy or temporal attacks, the proposed LSTM model provides comprehensive coverage.

C. Forensic Validation via Dual-Database Synchronization

The dual-database architecture provided a reliable mechanism for forensic integrity. The synchronization module maintained a record match rate of 99.98% under normal conditions. During the Access Token Hijacking simulation, where the attacker injected data directly into the Fog layer, the synchronization script immediately detected a discrepancy between the Edge (clean) and Fog (compromised) databases. This proved that the architecture could effectively isolate the source of compromise and provide immutable evidence for forensic analysis [19]. Furthermore, this synchronization mechanism aligns with recent methodologies for ensuring data integrity in cloud-based forensic investigations [20].

D. Comparison with Traditional Methods and Limitations

Compared to traditional SCADA security relying solely on static thresholds, our hybrid approach reduced the false negative rate significantly. Rule-based methods flagged only

TABLE V. SUMMARY OF MACHINE LEARNING WORKFLOW METRICS AND CONFIGURATIONS

Stage	**Metric 1**	**Metric 2**	**Metric 3**
Data Preprocessing	Filter Rate: 10%	Status Filtered: 13	**Data Size Post: 80%**
Feature Engineering	Ratios Added: 2	Key Features: 4	Impact: +5% F1
Train/Validation Split	**Train Split: 70%**	Validation Split: 30%	Method: Chronological
Model Training	States Used: Active	Test Data Mix: Mixed	Training Freq: Periodic
Supervised Models	**Accuracy: 94.3%**	**Recall: 95.7%**	F1-Score: 93.6%
Unsupervised Models	Normal Error: < 0.02	Anomaly Error: > 0.14	**Detection Rate: 92%**
Visualization	Threshold: 0.1	Alert Rate: 5/day	Integration: Fog Layer

TABLE VI. PERFORMANCE METRICS OF SUPERVISED LEARNING MODELS

Model	Accuracy	Precision	Recall	F1-Score
Decision Tree	91.2%	89.5%	90.1%	89.8%
Random Forest	**94.3%**	**91.6%**	**95.7%**	**93.6%**
Logistic Regression	88.4%	85.2%	86.8%	86.0%

TABLE VII. DETECTION CAPABILITY MATRIX ACROSS ATTACK SCENARIOS

Attack Type	**Rule-Based**	**Random Forest**	**Isolation Forest**	**LSTM**
DDoS (Flooding)	Low	Low	Medium	**High**
FDI (Gross)	**High**	**High**	**High**	**High**
FDI (Stealthy)	Low	Low	Medium	**High**
Replay Attack	Fail	Fail	Medium	**High**
Token Hijacking	Fail	Fail	Low	**High**

Note: 'High' indicates detection within 5s with $> 90\%$ *accuracy. 'Fail' indicates no detection.*

5% of anomalies, whereas the combined AI-driven approach identified an additional 5-7% of sophisticated threats.

However, limitations remain. The supervised models showed reduced accuracy against novel attack vectors not represented in the training set, highlighting the issue of model drift. Furthermore, while the Autoencoder provided high detection rates, explaining the root cause of the high reconstruction error to operators remains a challenge [10]. Future work will focus on integrating Explainable AI (XAI) techniques to improve the interpretability of these alerts [27].

VII. CONCLUSION AND FUTURE WORK

This study successfully developed and validated a simulation-based SCADA security framework designed to protect critical infrastructure against evolving cyber threats. By integrating high-fidelity telemetry from the Aventa AV-7 wind turbine [11] with a multi-layered architecture, we demonstrated that a data-driven approach significantly enhances the resilience of Industrial IoT environments compared to traditional static defense mechanisms.

The experimental results confirmed that the proposed dual-database architecture serves as a robust mechanism for forensic integrity. The real-time synchronization between Edge and Fog layers successfully identified sophisticated discrepancies caused by Man-in-the-Middle attacks and data tampering, which standard visualization tools failed to detect [19]. Furthermore, the hybrid anomaly detection engine proved critical for comprehensive security; while supervised Random Forest models achieved high accuracy in classifying known operational faults, the unsupervised Autoencoder models were indispensable for detecting novel attack vectors, specifically replay attacks, thereby reducing false negatives inherent in rule-based systems [12].

Despite these contributions, the deployment of such systems in large-scale smart cities requires addressing specific limitations. Future research should prioritize the integration of Explainable AI (XAI) to demystify the "black-box" decisions of deep learning models, providing operators with actionable insights rather than abstract anomaly scores [27], [28]. Additionally, to resolve scalability and data privacy concerns, transitioning from centralized processing to Federated Learning is recommended, allowing edge devices to collaboratively train defense models without exposing sensitive raw telemetry [30],

[29]. Finally, implementing an automated MLOps pipeline for adaptive model retraining will be essential to mitigate model drift caused by seasonal environmental changes or emerging adversarial tactics [31].

In conclusion, this research offers a scalable, cost-effective reference model for securing modern industrial control systems, bridging the gap between theoretical security designs and practical, real-world implementation.

Declarations

- Funding: This research work received funding from the Naif Arab University for Security Sciences, under grant agreement no. NAUSS-24-R2.

- Conflict of interest: The authors declare no competing interests.
- Data availability: The dataset used in this study is publicly available from Zenodo [11].
- Code availability: The complete source code, including synchronization scripts and attack simulations, is available in the project repository: https://github.com/MQ-2024/Enhancing-SCADA-Security.git.
- Author contribution: Both authors contributed equally to the study conception, design, and implementation.

References

[1] D. Upadhyay, S. Ghosh, H. Ohno, M. Zaman, and S. Sampalli, "Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator," *Int. J. Crit. Infrastruct. Prot.*, vol. 47, p. 100705, 2024.

[2] K. T. Chui, B. B. Gupta, J. Liu, V. Arya, N. Nedjah, A. Almomani, and P. Chaurasia, "A survey of Internet of Things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions," *Information*, vol. 14, no. 7, p. 388, 2023.

[3] W. Alsabbagh and P. Langendörfer, "Security of programmable logic controllers and related systems: Today and tomorrow," *IEEE Open J. Ind. Electron. Soc.*, vol. 4, pp. 659–693, 2023.

[4] S. Ghosh, M. Zaman, R. Joshi, and S. Sampalli, "Multi-phase quantum resistant framework for secure communication in SCADA systems," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 5, pp. 1–14, 2024.

[5] A. K. Tyagi and N. Sreenath, "Cyber physical systems: Analyses, challenges and possible solutions," *Internet Things Cyber-Phys. Syst.*, vol. 1, pp. 22–33, 2021.

[6] I. Y. Alzahrani, S. Lee, and K. Kim, "Enhancing Cyber-Threat Intelligence in the Arab World: Leveraging IoC and MISP Integration," *Electronics*, vol. 13, no. 13, p. 2526, 2024.

[7] S. Lee, A. A. H. Mujammami, and K. Kim, "Leveraging Social Networks for Cyber Threat Intelligence: Analyzing Attack Trends and TTPs in the Arab World," *IEEE Access*, 2024.

[8] R. Chataut and R. Akl, "Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies," *Sensors*, vol. 23, no. 21, p. 8840, 2023.

[9] W. H. Choi and J. Kim, "Unsupervised learning approach for anomaly detection in industrial control systems," *Appl. Syst. Innov.*, vol. 7, no. 2, p. 18, 2024.

[10] R. R. Irshad *et al.*, "An intelligent buffalo-based secure edge-enabled computing platform for heterogeneous IoT network in smart cities," *IEEE Access*, vol. 11, pp. 69282–69294, 2023.

[11] S. Barber, F. Hammer, and L. Hilfiker, "IET-OST research wind turbine SCADA dataset AV-7 (6kW)," *Zenodo*, 2023. [Online]. Available: https://doi.org/10.5281/zenodo.8192149.

[12] S. Y. Diaba *et al.*, "SCADA securing system using deep learning to prevent cyber infiltration," *Neural Netw.*, vol. 165, pp. 321–332, 2023.

[13] M. Mesbah, M. S. Elsayed, A. D. Jurcut, and M. Azer, "Analysis of ICS and SCADA systems attacks using honeypots," *Future Internet*, vol. 15, no. 7, p. 241, 2023.

[14] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms, and challenges," *J. Inf. Intell.*, vol. 6, no. 4, pp. 455–513, 2024.

[15] B. Alotaibi, "A survey on Industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities," *Sensors*, vol. 23, no. 17, p. 7470, 2023.

[16] R. Das and M. M. Inuwa, "A review on fog computing: Issues, characteristics, challenges, and potential applications," *Telemat. Inform. Rep.*, vol. 10, p. 100049, 2023.

[17] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge computing and cloud computing for Internet of Things: A review," *Informatics*, vol. 11, no. 4, p. 71, 2024.

[18] A. M. Sheikh and M. R. Islam, "A survey on edge computing (EC) security challenges: Classification, threats, and mitigation strategies," *Future Internet*, vol. 17, no. 4, p. 175, 2023.

[19] M. R. Anwar, R. Panjaitan, and R. Supriati, "Implementation of database auditing by synchronization DBMS," *Int. J. Cyber IT Serv. Manag.*, vol. 1, no. 2, pp. 197–205, 2021.

[20] J. Kang, J. Kim, S. Lee, and J. Park, "Forensic Approaches for End-to-End Encryption Cloud Storage Services: MEGA as a Case Study," *Arab J. Forensic Sci. Forensic Med.*, vol. 6, no. Special Issue, pp. 171–190, 2024.

[21] A. Manimuthu, V. Dharshini, I. Zografopoulos, M. K. Priyan, and C. Konstantinou, "Contactless technologies for smart cities: Big data, IoT, and cloud infrastructures," *SN Comput. Sci.*, vol. 2, no. 4, p. 334, 2021.

[22] J. Li, X. Deng, and B. Yao, "Enhanced anomaly detection of industrial control systems via graph-driven spatio-temporal adversarial deep support vector data description," *Expert Syst. Appl.*, vol. 249, p. 126573, 2024.

[23] A. Dehlaghi-Ghadim, M. H. Moghadam, A. Balador, and H. Hansson, "Anomaly detection dataset for industrial control systems," *IEEE Access*, vol. 11, pp. 107982–107996, 2023.

[24] S. H. Mohammed *et al.*, "Evaluation of feature selection using machine learning for cyber-attack detection in smart grid," *IEEE Access*, vol. 12, pp. 26394–26416, 2024.

[25] L. Ren, Z. Jia, Y. Laili, and D. Huang, "Deep learning for time-series prediction in IIoT: Progress, challenges, and prospects," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 10, pp. 1–15, 2023.

[26] F. A. Alfouzan, K. Kim, and N. M. Alzahrani, "An efficient framework for securing the smart city communication networks," *Sensors*, vol. 22, no. 8, p. 3053, 2022.

[27] C. Trivedi *et al.*, "Explainable AI for Industry 5.0: Vision, architecture, and potential directions," *IEEE Open J. Ind. Appl.*, vol. 5, pp. 242–258, 2024.

[28] C. Hwang and T. Lee, "E-SFD: Explainable sensor fault detection in the ICS anomaly detection system," *IEEE Access*, vol. 9, pp. 140470–140486, 2021.

[29] H. Li, L. Ge, and L. Tian, "Survey: Federated learning data security and privacy-preserving in edge-Internet of Things," *Artif. Intell. Rev.*, vol. 57, no. 5, p. 130, 2024.

[30] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8229–8249, 2022.

[31] W. Xu, Z. Yang, D. W. K. Ng, M. Levorato, Y. C. Eldar, and M. Debbah, "Edge learning for B5G networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing," *IEEE J. Sel. Top. Signal Process.*, vol. 17, no. 1, pp. 9–39, 2023.