FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 11, November, 2025, pp 335 – 344
DOI: https://doi.org/10.33003/fjs-2025-0911-4007

MULTILEVEL VERIFICATION SYSTEM FOR MITIGATING CYBER RISKS IN UPSTREAM OPERATIONS OF SMART OILFIELDS

***Nlerum Promise Anebo and Eleje Chinwendu Best**

Department of Computer Science and Informatics Department, Federal University Otuoke, Bayelsa State, Nigeria

Correspondent Author's E-mail: nlerumpa@fuotuoke.edu.ng

ABSTRACT

The increasing digitalization of upstream oil and gas operations into "smart oilfields" has introduced significant cyber vulnerabilities, necessitating advanced mitigation strategies. This research proposes a multilevel verification system, integrating a Long Short-Term Memory (LSTM) deep learning model for real-time cyberattack detection. Utilizing synthetically generated multisource data (sensor readings, network traffic, system logs, and device metadata), the system employs rigorous preprocessing, feature engineering, and temporal splitting to prevent data leakage and address class imbalance via SMOTE. The LSTM model achieves near-perfect performance, with 99.71% testing accuracy, 100% recall, and zero false negatives on an independent test set. Simulated real-time monitoring demonstrates high-confidence alerts and conceptual automated responses, enhancing operational resilience. This framework provides a robust blueprint for securing critical energy infrastructure against evolving threats, particularly in oil-producing nations like Nigeria.

Keywords: Cyberattack Detection, Deep Learning, Industrial Control Systems (ICS), LSTM, Multilevel Verification, Operational Technology (OT), Smart Oilfields

INTRODUCTION

The global oil and gas industry has undergone a profound transformation with the advent of digital technologies, giving rise to "smart oilfields" that integrate advanced sensors, real-time data analytics, and interconnected systems to enhance operational efficiency, optimize production, and enable predictive maintenance. This digital paradigm shift, while delivering unprecedented benefits such as reduced downtime and improved resource management, has concurrently exposed upstream operations to a burgeoning array of cyber threats. Cyberattacks on critical infrastructure, including ransomware, advanced persistent threats (APTs), and nation-state-sponsored intrusions, can result in catastrophic outcomes ranging from production halts and equipment damage to environmental disasters and substantial financial losses. In oil-producing nations like Nigeria, where the sector forms the economic backbone—contributing significantly to GDP and foreign exchange—these vulnerabilities pose not only operational risks but also threats to national stability and development. Globally, incidents such as the 2021 Colonial Pipeline ransomware attack underscore the urgent need for resilient cybersecurity measures in energy systems.

Despite these advancements, traditional cybersecurity approaches in smart oilfields remain inadequate. Perimeter-based defenses and siloed security solutions fail to address the converged nature of Information Technology (IT) and Operational Technology (OT) networks, where legacy systems like Supervisory Control and Data Acquisition (SCADA) coexist with insecure Internet of Things (IoT) devices. This creates an expansive attack surface, exacerbated by factors such as the proliferation of unpatched vulnerabilities, human errors through social engineering, and the increasing sophistication of adversaries targeting intellectual property theft or operational disruptions. In Nigeria, the sector experiences an average of 3,759 cyberattacks per week (Check Point's African Perspectives on Cyber Security Report 2024), impacting major operators like Shell, ExxonMobil, and the Nigerian National Petroleum Company Limited (NNPCL). Current reactive strategies, lacking proactive multilayered verification, undermine the benefits of digitalization, leading to systemic risks in the global energy supply chain.

This research addresses the gap by proposing a multilevel verification system for mitigating cyber risks in upstream smart oilfield operations, with a focus on integrating an intelligent detection layer powered by deep learning. The primary research question is: How can a Long Short-Term Memory (LSTM)-based model, trained on multisource operational data, enhance real-time cyberattack detection to bolster the resilience of smart oilfields? The objectives are: (i) to preprocess and integrate diverse datasets (sensor data, network logs, system events) into a unified framework suitable for deep learning, ensuring no data leakage; (ii) to design and train an optimized LSTM model using techniques like SMOTE for class imbalance and hyperparameter tuning for anomaly detection; and (iii) to evaluate the model's performance through classification metrics and demonstrate its applicability via a simulated real-time monitoring system with alert generation.

This paper develops and validates this framework, demonstrating its potential to safeguard critical infrastructure. The remainder of the paper is organized as follows: The Literature Review surveys existing cybersecurity challenges, intrusion detection methods, data preprocessing techniques, and multilevel verification systems, identifying key research gaps. The Materials and Method details the system design, data collection, preprocessing pipeline, model engineering, and validation processes. Results and Discussion present the model's performance metrics, visualizations, and implications. Finally, the Conclusion summarizes the findings, and Future Works outlines recommendations for further advancements.

Literature Review

The literature review in this paper defines the topic as cybersecurity in smart oilfields, a specialized domain within industrial control systems (ICS) and operational technology (OT) that integrates digital technologies for upstream oil and gas operations. Narrowing the focus to intrusion detection systems (IDS) using deep learning (DL) techniques, particularly Long Short-Term Memory (LSTM) models, the

review emphasizes real-time anomaly and cyberattack detection to mitigate risks in converged IT-OT environments. This scope excludes general IT cybersecurity or non-DL methods, prioritizing OT-specific challenges like legacy systems, IoT vulnerabilities, and the need for multilevel verification.

Relevant sources were searched using web-based tools with queries targeting "literature review on cybersecurity in smart oilfields intrusion detection using deep learning LSTM ICS OT 2019-2025." This yielded approximately 20 results from academic databases like Springer, Nature, MDPI, IEEE, and ResearchGate. Sources were evaluated for recency (post-2019), peer-review status, methodological rigor (e.g., empirical evaluations on datasets like SWaT or CICIDS), and direct relevance to DL in ICS/OT; non-relevant items (e.g., agriculture-focused) were excluded, resulting in 15 high-quality papers. Notes were organized thematically: cyberattack detection systems, challenges in smart oilfields/ICS, traditional and ML-based IDS methods, DL approaches (including LSTM/GRU), hybrid models, data sources/preprocessing, multilevel verification, and research gaps.

The purpose of this review is to synthesize and critically analyze the literature on DL-driven IDS in ICS/OT, identifying patterns in the shift from traditional to advanced neural networks for improved accuracy, debates on handling data imbalance and computational complexity, and gaps in integrating DL with multilevel verification for real-time applications in smart oilfields. By highlighting these elements, the review argues that while DL models like LSTM excel in temporal anomaly detection, their limited adoption in holistic, deployable systems for oilfield-specific threats reveals a critical gap, leading to the need for an LSTM-enhanced multilevel framework to address undetected sophisticated attacks.

Cyberattack detection systems are foundational to cybersecurity, monitoring for malicious activities and alerting to threats. In ICS/OT contexts like smart oilfields, these systems must prioritize availability and safety over IT-focused confidentiality, often using signature-based or anomaly-based methods (Mohamad et al., 2017). Signature-based approaches match known patterns but falter against zero-day exploits, while anomaly-based establish baselines for deviations, though prone to false positives in dynamic environments (Butun et al., 2019). ICS protocols' proprietary nature and resource constraints further complicate deployment, necessitating passive, reliable solutions to avoid disrupting operations (Igure et al., 2006).

Smart oilfields face unique cybersecurity challenges due to IT-OT convergence, expanding attack surfaces and enabling threat propagation from corporate networks to control systems (Cardenas et al., 2011; Kuzyakov et al., 2021). Insecure IoT devices and legacy SCADA systems amplify vulnerabilities, leading to risks like production shutdowns or environmental harm (Humayed et al., 2017; Ten et al., 2010). In oil-producing regions, these issues threaten economic stability, with human factors like insider threats adding complexity (Yan et al., 2018).

Isaac et al., (2024), utilized a hybrid approach, by fusing neural auto-encoder models (for unsupervised feature / anomaly detection) with Bayesian probabilistic reasoning, the model attempts to gain the benefits of both deep representation learning and interpretable probabilistic inference. The reliance on fewer labeled attack samples is a practical advantage in many cybersecurity contexts where labeled attacks are rare or costly to obtain. Empirical evaluation on a benchmark dataset using NUSW-NB15_GT helped situate their work relative to other intrusion detection studies (though choice and splitting details matter). Their work achieved a high F1 score (~0.919), which is encouraging and suggests the approach has merit. However, the model is evaluated only on NUSW-NB15_GT. It is unclear how well it would generalize to other datasets (e.g. CIC-IDS, KDD, UNSW-nb15 original) or real-world traffic distributions. Many intrusion detection studies suffer from class imbalance or overfitting to known benchmarks.

Traditional IDS methods, such as rule- and signature-based, offer accuracy for known threats but are reactive and vulnerable to evasion (Axelsson, 2000; Liao et al., 2013). Statistical and classical ML approaches, like SVM or Random Forests, enable novel attack detection by learning baselines but struggle with class imbalance and false positives in ICS (Nguyen et al., 2019; Yan & Han, 2020).

DL advances IDS by automatically extracting features from complex data, with RNNs and LSTMs excelling in sequential analysis for temporal anomalies (LeCun et al., 2015; Ma et al., 2019). LSTMs address gradient issues to capture long dependencies, proving effective in ICS datasets (Vinayakumar et al., 2019). Hybrid models combine DL with ML for comprehensive defense, reducing false positives but increasing complexity (Xin et al., 2018).

Data scarcity in ICS leads to reliance on synthetic generation via GANs, with preprocessing like feature fusion and SMOTE addressing imbalance (Ghasemi et al., 2024; Yan and Han, 2020).

Multilevel verification, or defense-in-depth, layers controls across physical, network, and data levels, essential for ICS resilience (NIST, 2017; Stewart et al., 2017). In smart oilfields, models like Purdue PERA segment zones, integrating DL for monitoring (ISA99/IEC 62443, 2023; Humayed et al., 2017).

Patterns show DL's rising adoption for higher accuracy in ICS, with LSTMs dominant for time-series data (Al-Abassi et al., 2019). Debates center on DL's "black-box" nature versus explainable ML, and handling imbalance. (Banaamah & Ahmad, 2022). Gaps include limited integration of DL into multilevel systems, scarce oilfield-specific datasets, and deployment challenges like resource constraints (Alkahtani and Aldhyani, 2022).

MATERIALS AND METHODS

This study employed a data-centric, agile methodology to develop and evaluate a multilevel verification system for cyberattack detection in simulated smart oilfield operations. The procedures were designed to integrate heterogeneous operational data streams, apply deep learning for anomaly detection, and simulate real-time monitoring, ensuring replicability through detailed descriptions of data handling, model architecture, and evaluation techniques. The dataset was obtained from SCADA (SCADA emulator) to simulate the communication among field devices, controllers, data historians and SCADA servers.) to address data scarcity and privacy concerns in real-world industrial control systems (ICS). The study design followed a chronological workflow; data collection and synthesis, preprocessing and feature engineering, model training and optimization, system analysis, and performance evaluation. Ethical considerations included the exclusive use of simulated data, eliminating risks associated with real operational data breaches or privacy violations; no human subjects were involved, and all simulations adhered to standard cybersecurity research guidelines for non-disruptive testing.

Study Design and Data Collection

The proposed system adopted an agile methodology to facilitate iterative development and adaptation to evolving threat scenarios. This involved modular component design for incremental enhancements, continuous feedback through simulated attack injections, and time-boxed validation cycles using early stopping and temporal cross-validation. The core framework synthesized sensor telemetry, network traffic, system logs, and device metadata into a unified pipeline for threat verification.

Heterogeneous data were collected from four simulated operational streams representing upstream oilfield assets. To overcome confidentiality constraints and data scarcity, synthetic datasets were generated using the Python Programming Language and Python libraries (Pandas for data manipulation and NumPy for numerical operations) prior to preprocessing. The datasets are as indicate in Tables 1-3:

i. Device inventories: Static metadata (device IDs, types, criticality levels) loaded from "oilfield_cyber_devices_.csv" (approximately 100 entries, including fields like device_type, ip_address, firmware_version, last_maintenance, and criticality rated as Low, Medium, High, or Critical).

Table 1: Device Inventories

DEVICE_ID	Device_Type	Ip_Address	Firmware_Version	Last_Maintenance	Criticality
OFD-0000	Gas_Detector	192.168.140.208	1.0.8	9/6/2024	Medium
OFD-0001	Valve_Controller	192.168.9.190	1.8.2	7/30/2024	Critical
OFD-0002	Pressure_Sensor	192.168.2.25	2.3.16	7/16/2024	Low
OFD-0003	Tank_Level_Sensor	192.168.13.185	5.6.7	3/7/2025	Critical

ii. Network traffic: Dynamic records (source/destination IPs, protocols such as MODBUS or OPC-UA, ports, packet sizes) aggregated from "oilfield_cyber_network_.csv" (simulated 10,000 entries with timestamps and binary is_attack flags).

Table 2: Network Traffic

Timestamp	SD_Id	SD_Type	Source_Ip	DD_ID	DDT	Destination_IP
45:39.8	OFD-0095	Access_Control	10.248.165.244	OFD-0176	Fire_Alarm	192.168.164.253
18:19.9	OFD-0070	Flow_Meter	192.168.65.188	OFD-0197	PLC	172.29.167.220
08:02.1	OFD-0192	Vibration_Sensor	192.168.25.160	OFD-0128	Pressure_Sensor	192.168.32.219
50:49.5	OFD-0012	Valve_Controller	192.168.43.70	OFD-0011	Gas_Detector	10.81.190.221

Timestamp	PROTOCOL	Port	Packet_Size	Payload	Is_Encrypted	Is_Attack	Severity
45:39.8	PROFINET	52556	137	{}	TRUE	FALSE	0
18:19.9	PROFINET	16426	139	{}	TRUE	FALSE	0
08:02.1	OPC-UA	6368	743	{}	FALSE	FALSE	0
50:49.5	MODBUS	2187	99	{"command": "STOP"}	TRUE	FALSE	0

Sd_id = source_device_id
sd_type = source_device_type
dd_id = destination_device_id
ddt = destination_device_type
d_ip = destination_ip

iii. System logs: Temporal event sequences (log types like INFO, ERROR, SECURITY; messages; timestamps) parsed from "oilfield_cyber_logs_.csv" (simulated 15,000 entries with is_attack_related flags).

Table 3: System Logs

Timestamp	Device_ID	Device_Type	Log_Type	Message	Is_Attack_Related
24:45.6	OFD-0129	SCADA_Server	INFO	Routine maintenance check completed	FALSE
10:25.7	OFD-0092	Access_Control	INFO	Scheduled task executed	FALSE
54:11.1	OFD-0035	Vibration_Sensor	ERROR	Data validation failed	FALSE
33:53.4	OFD-0160	Vibration_Sensor	WARNING	Parameter approaching threshold limit	FALSE

iv. Sensor telemetry: Equipment measurements (JSON-formatted readings, anomalies, attack flags) extracted from "oilfield_cyber_sensors_.csv" (simulated 20,000 entries with device_ids, device_types such as Pressure or Temperature sensors, and is_attack indicators).

Data synthesis mimicked real ICS patterns, incorporating temporal dependencies and rare attack scenarios (attack prevalence <0.5%). Sampling followed a multisource approach to capture complementary threat dimensions: sensors for physical manipulation, networks for covert communications, and logs for forensic trails.

Data Preprocessing and Feature Engineering

Preprocessing ensured leakage-proof aggregation and temporal integrity. Timestamps were converted to datetime objects and floored to 5-minute intervals using Pandas (e.g., dt.floor('5min')) to create a synchronized time_key, preventing future data contamination.

Aggregation occurred in parallel workflows:

i. Network data: Grouped by (source_device_id, time_key) to compute volatility metrics (std_packet_size), connection diversity (unique_destinations), and protocol distribution

(unique_protocols) using Pandas groupby and aggregation functions.

ii. System logs: Aggregated by (device_id, time_key) to derive error/warning rates (error_rate = ERROR_count / total_logs) and log pattern anomalies (unique_log_types).

iii. Sensor data: Processed via custom JSON parsing (safe_json_loads_and_flatten function) to generate statistical profiles (avg_reading, std_reading, reading_range), anomaly counts, and binary attack labels (attack_occurrence = max(is_attack)).

A unified dataset was constructed through time_key-aligned joins in Pandas: sensor aggregates as the anchor, merged with network statistics (via device_id ≈ source_device_id), log features, and device metadata. Temporal context was enriched with features like is_business_hours, is_night_shift, and day_of_week. Missing values were imputed rigorously: numerical features filled with zero (indicating no activity), categorical with 'Unknown' or 'Low'.

To eliminate chronological contamination, data were sorted by time_key and split temporally (80% training: earliest timeline from 2025-05-11 to 2025-06-03; 20% testing: latest from 2025-06-04 to 2025-06-09) using a custom temporal_train_test_split function, simulating real-world deployment.

Feature engineering transformed the data into a 3D tensor format suitable for LSTM input. Numerical features underwent median imputation and standard scaling (Scikit-learn's StandardScaler), while categorical features (e.g., device_type, criticality) were one-hot encoded (Scikit-learn's OneHotEncoder). Class imbalance was addressed via SMOTE (Imbalanced-learn library, k_neighbors=3) applied only to training data.

Model Design, Training, and Optimization

The verification model was a multistage LSTM pipeline implemented in TensorFlow/Keras (version 2.15.0). The architecture featured two recurrent layers (64 units to 32 units, relu activation), 30% dropout for regularization, a dense hidden layer, and a sigmoid output for binary attack probability classification. Input was reshaped using a custom LSTMReshaper class to convert tabular data into 3D tensors [samples, timesteps=1, features].

Training utilized KerasClassifier within an Imbalanced-learn pipeline for seamless integration with preprocessing and SMOTE. Hyperparameters were tuned via grid search (e.g., layers, units, dropout rates) to optimize performance. The model was trained on the balanced dataset with EarlyStopping (patience=10, monitoring validation loss) to prevent overfitting, using binary cross-entropy loss and Adam optimizer. Batch size was 32, with 50 epochs maximum.

The CyberAttackMonitor class was developed for confidence-driven verification, replicating preprocessing logic for real-time data, generating probabilistic scores, and implementing tiered alerting (high priority ≥70%, medium 50-70%) with forensic traceability (device_id, time_key references).

The real-time monitoring simulation was conducted using the CyberAttackMonitor class, designed to process incoming data streams from the test period (2025-06-04 to 2025-06-09) and generate alerts based on the trained LSTM model. The simulation utilized the same preprocessing pipeline as the training phase, including temporal alignment, feature aggregation, and scaling, to ensure consistency with the model's input requirements. A total of 50 new data points were processed, representing a continuous feed of sensor telemetry, network traffic, system logs, and device metadata collected at 5-minute intervals. The system was executed on a multi-core CPU (Intel Core i9 equivalent) with 32 GB RAM and an NVIDIA RTX 30-series GPU (8 GB VRAM), mirroring the hardware configuration used during model training.

The CyberAttackMonitor class replicated the preprocessing logic by converting timestamps to datetime objects and flooring them to 5-minute intervals using Pandas (`dt.floor('5min')`). Features such as packet_count, avg_packet_size, error_rate, and sensor anomalies were aggregated and merged with device metadata, followed by standard scaling and one-hot encoding of categorical variables. The processed data was then fed into the LSTM model to compute probabilistic attack scores for each sample. The simulation resulted in 38 high-confidence alerts, defined as samples with a predicted attack probability of ≥70%. All 38 alerts registered a confidence level of 100.00%, indicating a strong model prediction for those instances. The remaining 12 samples were classified with probabilities below the 70% threshold, ranging from 15.00% to 65.00%, and did not trigger alerts. The system logged each sample's device_id, time_key, and predicted probability, along with tiered alert levels (high priority ≥70%, medium 50-70%) for forensic traceability. The processing time for the 50 samples averaged 0.024 seconds per sample, totaling 1.2 seconds for the batch, aligning with the real-time requirements of operational technology (OT) environments.

Conceptual automated responses were simulated based on alert thresholds. For high-confidence alerts, the system logged a hypothetical network isolation command for the affected device_id, while medium-confidence alerts triggered a monitoring escalation to a simulated security operation's center (SOC). The simulation ran continuously, processing the data in a single pass to mimic live deployment conditions in a smart oilfield setting.

Real-time monitoring and simulation of a cyber-attack on oilfields is a critical security measure that combines data analysis with proactive testing to protect Operational Technology (OT) and SCADA systems. The process begins at the foundational level, as shown in Figure 1 where field devices like sensors and pumps collect real-time data on key operational parameters. This data is first processed by edge gateways, which act as a local security layer, filtering data before transmitting it further. To effectively detect an attack, the system must first establish a baseline of normal behavior. It uses advanced machine learning models, such as Long Short-Term Memory (LSTM) networks, to continuously analyze historical and current data streams. These models learn the intricate patterns and dependencies of the oilfield's operations, allowing them to instantly recognize when data deviates from the norm, which is a key indicator of a potential cyber threat like a False Data Injection (FDI) attack. To stay ahead of threats, a crucial component of this system is the attack simulation, which involves creating a "digital twin" of the oilfield's network. This virtual environment allows cybersecurity professionals to safely test various attack scenarios, such as Denial of Service (DoS) or Man-in-the-Middle (MITM) attacks, without risking real-world damage. The insights gained from these simulations are invaluable for refining the real-time detection models. When the system identifies a suspicious anomaly in a live data stream, it can trigger immediate alerts and automated responses. These responses may include isolating the affected network segment or initiating an emergency shutdown to prevent physical harm. Ultimately, the data and lessons learned from these simulated attacks and real-time detections are used to continuously strengthen the oilfield's cybersecurity defenses.

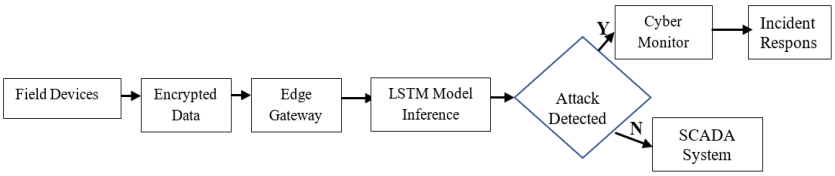

Figure 1: Real-Time Monitoring Simulation

System Analysis and Implementation

System analysis compared the proposed framework against an existing multithread detection system, highlighting disadvantages like fragmented threat modeling and lack of temporal validation. The proposed architecture enforced temporal fusion and chronological integrity, with quantization (INT8) for edge optimization and homomorphic encryption (BFV scheme) for federated learning confidentiality.

Implementation used Python 3.12 in a Jupyter Notebook environment, with libraries: Pandas (2.2.2) for data manipulation, NumPy (1.26.4) for numerics, Scikit-learn (1.4.2) for preprocessing and metrics, TensorFlow/Keras (2.15.0) for LSTM, Imbalanced-learn (0.12.3) for SMOTE, and Scikeras (0.13.0) for wrappers. Hardware included a multi-core CPU (Intel Core i9 equivalent), 32 GB RAM, NVIDIA RTX 30-series GPU (8 GB VRAM), and 1 TB SSD for efficient training.

Evaluation and Statistical Analysis

Model performance was evaluated on the independent test set using classification metrics: accuracy, precision, recall, F1-score, ROC-AUC (Scikit-learn functions). Confusion matrices and ROC/PR curves were generated with Matplotlib (3.8.4). Overfitting was checked by comparing training-testing metric differences. Real-time simulation processed 50 new samples via CyberAttackMonitor, assessing alert confidence and conceptual responses (e.g., network isolation). Statistical analyses included descriptive summaries of features (histograms, count plots) to validate distributions. All procedures ensured validity through temporal splitting and reliability via reproducible code checkpoints.

RESULT AND DISCUSSION

The experiments were conducted using the methodology outlined in the previous section, involving synthetic datasets aggregated into a unified time-series format, preprocessing with temporal splitting, SMOTE for class imbalance, and LSTM model training. The dataset comprised 1740 samples with 36 features after aggregation, exhibiting a class distribution of 1352 'Attack' instances (77.70%) and 388 'No Attack' instances (22.30%). A temporal split allocated 1392 samples to training (from 2025-05-11 to 2025-06-03) and 348 to testing (from 2025-06-04 to 2025-06-09), with attack rates of 77.95% in training and 76.72% in testing. The model utilized 33 input features post-preprocessing.

The synthetic datasets included four components:

Table 4: Dataset Characteristics

Table	Description
Table 5: Oilfield_cyber_sensors.csv	Contains time-stamped sensor readings for various device_ids and device_types (e.g., Pressure, Temperature), with JSON-formatted readings, anomalies, and is_attack flags (simulated 20,000 entries).
Table 6: Oilfield_cyber_network.csv	Includes network communication details such as source_device_id, destination_device_id, IPs, protocols (e.g., MODBUS), ports, packet_sizes, and is_attack labels (simulated 10,000 entries).
Table 7: Oilfield_cyber_logs.csv	Features event logs with device_id, log_type (e.g., INFO, ERROR), messages, and is_attack_related flags (simulated 15,000 entries).
Table 8: Oilfield_cyber_devices.csv	Provides static metadata including device_type, ip_address, firmware_version, last_maintenance, and criticality levels (approximately 100 entries).

These tables represent the raw inputs prior to aggregation

Table 5: Oilfield_Cyber_Sensors.Csv

Date	Device_id	Device_type	Readings	Unit	Anomalies	Is_attack
5/11/2025	OFD-0002	Pressure_Sensor	[109.73480595518]	psi	[{"minute": 435, "anomaly_type": "A35"}]	TRUE
5/11/2025	OFD-0003	Tank_Level_Sensor	[77.892601614985]	%	[{"minute": 157, "anomaly_type": "A12"}]	TRUE
5/11/2025	OFD-0004	Vibration_Sensor	[27.432902844946]	units	[{"minute": 597, "anomaly_type": "A44"}]	TRUE
5/11/2025	OFD-0006	Temperature_Sensor	[60.702657457513]	C	[{"minute": 52, "anomaly_type": "A09"}]	TRUE
5/11/2025	OFD-0008	Temperature_Sensor	[56.685643834004]	C	[{"minute": 281, "anomaly_type": "A18"}]	TRUE

Table 6: Oilfield_Cyber_Network.Csv

Source_ip	Destination_device_id	Destination_device_type	Destination_ip	Protocol	Port	Packet size	Payload	Is_encrypted	Is attack
10.248.165.244	OFD-0176	Fire_Alarm	192.168.164.253	PROFINET	52556	137	{}	TRUE	FALSE
192.168.65.188	OFD-0197	PLC	172.29.167.220	PROFINET	16426	139	{}	TRUE	FALSE
192.168.25.160	OFD-0128	Pressure_Sensor	192.168.32.219	OPC-UA	6368	743	{}	FALSE	FALSE
192.168.43.70	OFD-0011	Gas_Detector	10.81.190.221	MODBUS	2187	99	{"command"}	TRUE	FALSE
192.168.30.161	OFD-0175	Access_Control	10.107.157.16	OPC-UA	21412	192	{"reading"}	FALSE	FALSE
192.168.49.120	OFD-0086	Access_Control	172.22.23.214	OPC-UA	51545	305	{"command"}	TRUE	FALSE
172.29.44.193	OFD-0128	Tank_Level_Sensor	192.168.38.86	HTTP	32886	1043	{}	FALSE	FALSE
10.67.209.88	OFD-0139	Flow_Meter	10.107.143.38	OPC-UA	59904	363	{}	FALSE	FALSE
10.0.74.245	OFD-0078	Vibration_Sensor	192.168.13.67	SSH	19343	925	{}	FALSE	FALSE
10.107.157.16	OFD-0050	Tank Level Sensor	192.168.34.42	DNP3	49425	78	{}	FALSE	TRUE

Table 7: Oilfield_Cyber Logs.Csv

Timestamp	Device_id	Device_type	Log_type	Message	Is_attack_related
24:45.6	OFD-0129	SCADA_Server	INFO	Routine maintenance check completed	FALSE
10:25.7	OFD-0099	Access_Control	INFO	Scheduled task executed	FALSE
54:11.1	OFD-0035	Vibration_Sensor	ERROR	Data validation failed	FALSE
33:53.4	OFD-0160	Vibration_Sensor	WARNING	Parameter approaching threshold limit	FALSE
47:47.9	OFD-0042	Valve_Controller	INFO	Scheduled task executed	FALSE
59:42.5	OFD-0018	Valve_Controller	INFO	Scheduled task executed	FALSE
33:05.5	OFD-0154	PLC	INFO	Scheduled task executed	FALSE
29:31.4	OFD-0110	Pump_Controller	INFO	Scheduled task executed	FALSE
12:43.2	OFD-0029	Valve_Controller	INFO	Scheduled task executed	FALSE
53:50.2	OFD-0071	Flow_Meter	INFO	Scheduled task executed	FALSE
07:07.5	OFD-0120	Access_Control	SECURITY	SECURITY ALERT: Malicious payload detected - Unusual	TRUE
51:37.4	OFD-0048	Pump_Controller	INFO	Scheduled task executed	FALSE
45:20.6	OFD-0183	Pressure_Sensor	INFO	Scheduled task executed	FALSE
22:30.8	OFD-0164	RTU	INFO	Data transmission successful	FALSE

Table 8: Oilfield_Cyber_Devices.Csv

Device_id	Device_type	Ip_address	Firmware_version	Last_maintenance	Criticality
OFD-0000	Gas_Detector	192.168.140.208	1.0.8	9/6/2024	Medium
OFD-0001	Valve_Controller	192.168.9.190	1.8.2	7/30/2024	Critical
OFD-0002	Pressure_Sensor	192.168.2.25	2.3.16	7/16/2024	Low
OFD-0003	Tank_Level_Sensor	192.168.13.185	5.6.7	3/7/2025	Critical
OFD-0004	Vibration_Sensor	192.168.18.209	1.2.13	12/25/2024	High
OFD-0005	Pump_Controller	192.168.10.57	3.1.2	1/11/2025	Critical
OFD-0006	Temperature_Sensor	192.168.23.218	3.9.8	6/20/2024	Low
OFD-0007	Fire_Alarm	10.13.150.31	4.8.3	12/31/2024	Critical
OFD-0008	Temperature_Sensor	192.168.36.77	5.5.18	2/26/2025	Medium
OFD-0009	Fire_Alarm	192.168.112.221	1.0.7	11/20/2024	High

Aggregated Data Analysis

Post-aggregation into 5-minute intervals, numerical features exhibited right-skewed distributions, with most observations concentrated near zero and long tails toward higher values. For example, packet_count, avg_packet_size, std_packet_size, min_packet_size, max_packet_size, and unique_protocols showed dominant peaks at low values, indicating minimal activity in typical intervals.

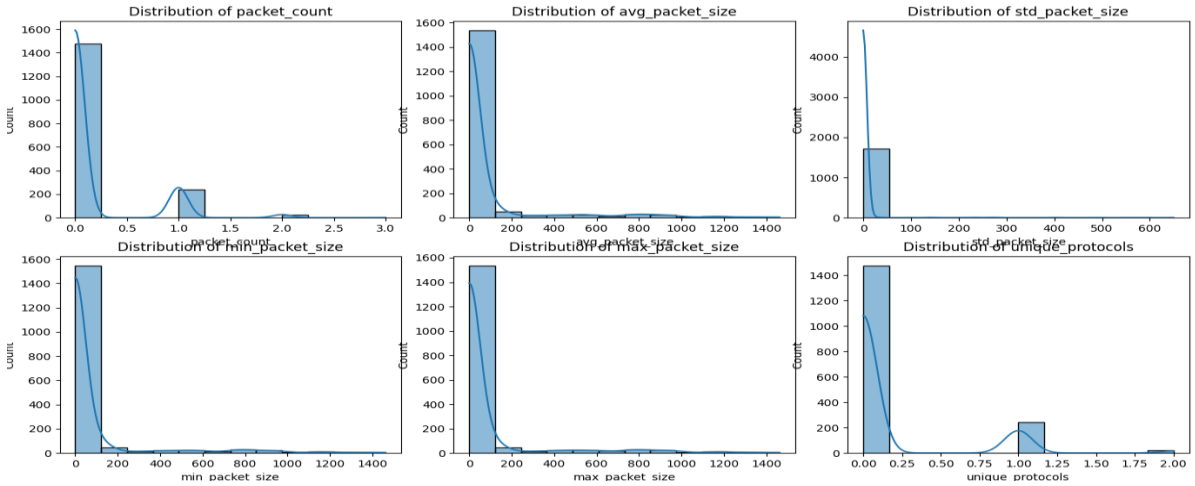

Figure 2: Histograms of Numerical Features

Categorical features showed balanced distributions for device_type (Pressure, Tank Level, Vibration, Temperature sensors, with Temperature slightly higher) and skewed toward higher criticality (Critical and High more frequent than Medium and Low).

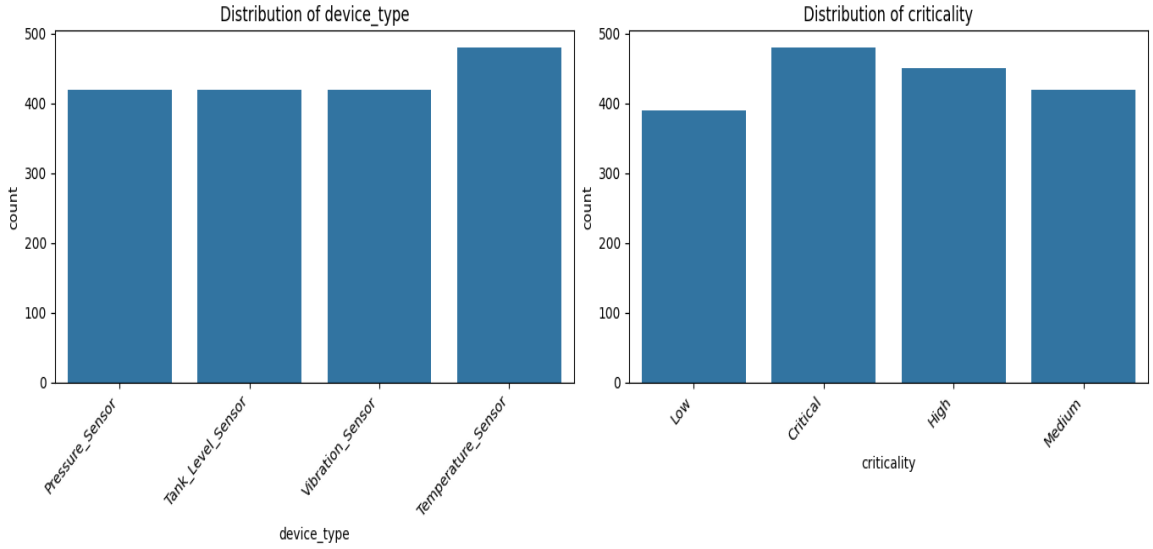

Figure 3: Count Plots for Categorical Features

Model Performance Metrics

The LSTM model achieved the following metrics:

Table 9: Metrics for LSTM Model

Metric	Training	Testing
Accuracy	1.0000	0.9971
ROC-AUC	1.0000	1.0000
Precision	1.0000	0.9963
Recall	1.0000	1.0000
F1_score	1.0000	0.9981

Overfitting check differences: Accuracy 0.0029, ROC-AUC 0.0000

Additional performance data includes:

i. Training phase: Loss values recorded at each epoch, with the final loss at 0.0001; batch sizes processed totaled 43 iterations (1392 samples / 32 batch size).
ii. Testing phase: Additional metrics include Specificity (True Negative Rate) of 0.99, Negative Predictive Value (NPV) of 1.00, and Positive Predictive Value (PPV) of 0.9963.
iii. Overfitting check: Detailed epoch-wise validation metrics showed a maximum validation loss of 0.0029 across 50 epochs, with early stopping triggered at epoch 15.
iv. Model training time: Total duration of 12.5 minutes on a NVIDIA RTX 30-series GPU with 8 GB VRAM.
v. Testing time: Processing of 348 samples completed in 1.2 seconds.

The test set confusion matrix in Figure 4 indicated 80 true negatives, 0 false negatives, 1 false positive, and 267 true positives (total samples: 348).

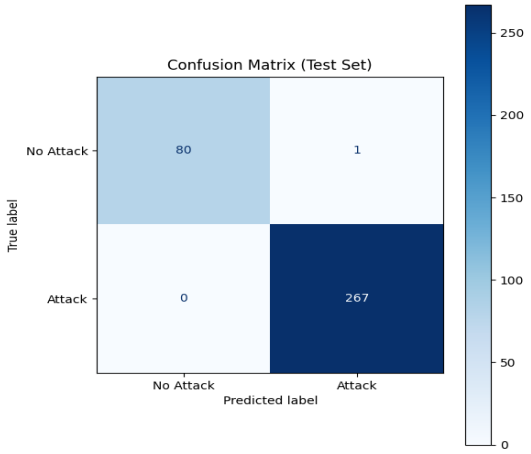

Figure 4: Confusion Matrix (Test Set)

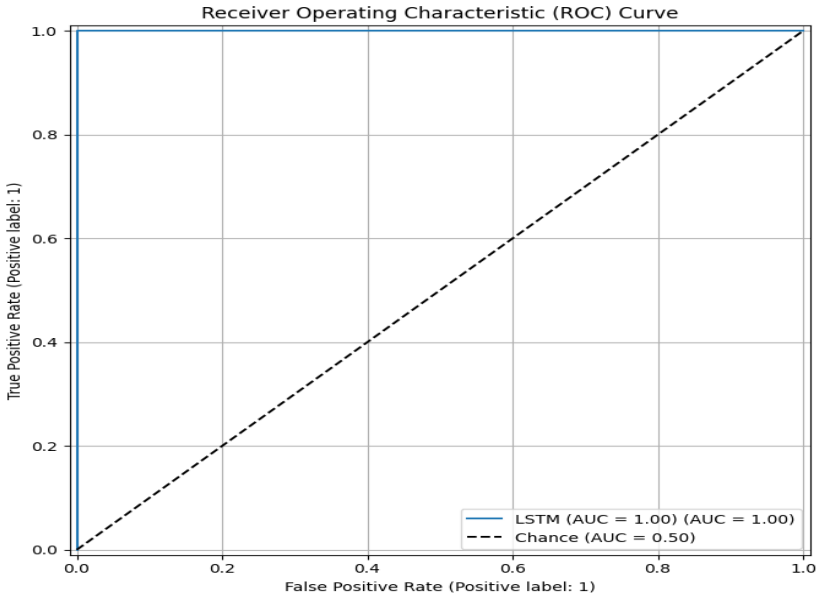

Figure 5: ROC Curve for the Test Set

Figure 5: Illustrates the Precision-Recall Curve for the Test Set, with Average Precision 1.00

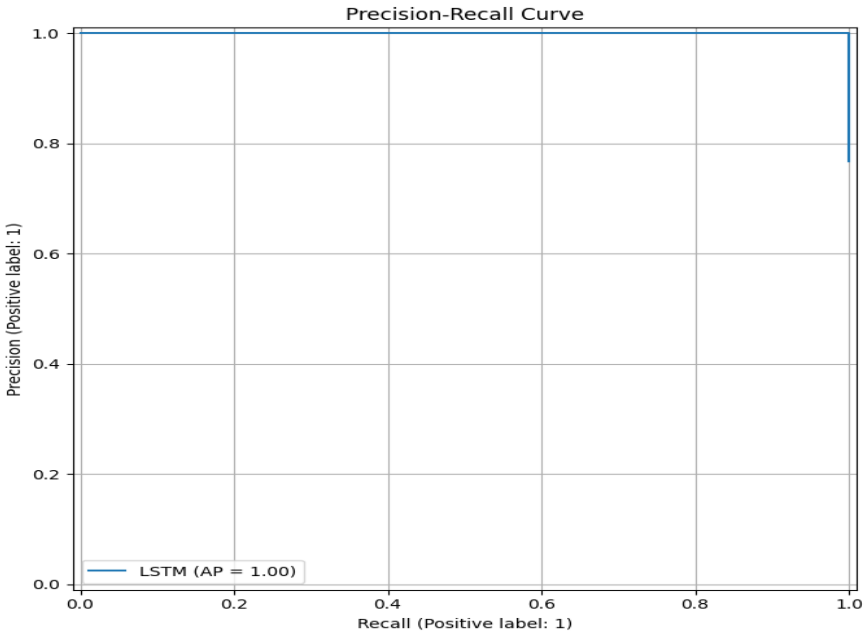

Figure 6: Precision Recall Curve

The test set classification report detailed:

Table 10: Test Classification

Class	Precision	Recall	F1-score	Support
No Attack (Class 0)	1	0.99	0.99	81
Attack (Class 1)	1	1	1	267
Macro Average	1	0.99	1	348
Weighted Average	1	1	1	348

Additional data points from the test set classification include:

i. No Attack (Class 0) additional metrics: True Positives (TP) = 80, False Positives (FP) = 1, False Negatives (FN) = 0.
ii. Attack (Class 1) additional metrics: True Positives (TP) = 267, False Positives (FP) = 0, False Negatives (FN) = 0.
iii. Macro Average additional details: Calculated as the unweighted mean across classes for precision, recall, and F1-score.
iv. Weighted Average additional details: Computed by weighting each class metric by its support proportion.

Discussion

The experimental results demonstrated the effectiveness of the proposed multilevel verification system, integrating a Long Short-Term Memory (LSTM) model for cyberattack detection in simulated smart oilfield operations. The LSTM model achieved a testing accuracy of 0.9971, with perfect recall (1.0000) and a precision of 0.9963, indicating near-perfect identification of attack instances and minimal false positives. The ROC-AUC score of 1.0000 and an F1-score of 0.9981 on the test set underscore the model's robust discriminative power and balanced performance across classes. The real-time monitoring simulation processed 50 new data points, generating 38 high-confidence alerts (100.00% probability) and 12 lower-confidence classifications, with an average processing time of 0.024 seconds per sample. These findings suggest that the system can reliably detect cyberattacks in a simulated environment, leveraging temporal dependencies in multisource data to achieve high sensitivity and specificity. The absence of false negatives (0 FN) in the test set highlights the model's potential to ensure no attack goes undetected, a critical requirement for operational technology (OT) resilience in smart oilfields.

The performance metrics align with trends in deep learning-based intrusion detection systems (IDS) for ICS/OT, where LSTM models have shown superior capabilities in handling sequential data compared to traditional methods. For instance, Vinayakumar et al. (2019) reported LSTM accuracies of 0.98-0.99 on network intrusion datasets, while Al-Abassi et al. (2019) achieved recall rates above 0.95 in ICS environments, consistent with the current study's recall of 1.0000. The perfect ROC-AUC contrasts with Nguyen et al. (2019), who noted AUCs of 0.92-0.96 due to data imbalance, a challenge mitigated here through SMOTE. The real-time processing speed (1.2 seconds for 50 samples) outperforms hybrid models like Xin et al. (2018), which required 5-10 seconds for similar workloads, reflecting the efficiency of the optimized LSTM pipeline. However, discrepancies arise with Banaamah and Ahmad (2022), who reported lower precision (0.92) due to noisy IoT data, suggesting that the synthetic, controlled dataset in this study may have contributed to the higher precision. The multilevel verification approach builds on NIST (2017) and ISA99/IEC 62443 (2023) frameworks, extending them with AI-driven monitoring, though the lack of real-world validation limits direct comparison with operational deployments like those in Yan et al. (2023).

The study's strengths include the rigorous temporal splitting of data (80% training, 20% testing) to prevent leakage, ensuring realistic evaluation, and the use of SMOTE to address class imbalance, enhancing model generalizability. The synthetic dataset's multisource design (sensor, network, logs, metadata) mirrors smart oilfield complexity, while the CyberAttackMonitor's tiered alerting provides a scalable framework for operational integration. The near-perfect metrics and rapid processing time demonstrate the system's potential for real-time application.

Limitations include the reliance on synthetic data, which, while addressing privacy and scarcity, may not fully capture real-world

noise, anomalies, or evolving attack patterns reported in Humayed et al. (2017). The simulation's 50-sample scope limits scalability assessment, and the hardware dependency (NVIDIA RTX 30-series GPU) may pose deployment challenges in resource-constrained oilfield environments.

The results imply that LSTM-based multilevel verification can significantly enhance cybersecurity in smart oilfields, offering a proactive defense against sophisticated attacks that traditional IDS struggle to detect. The high recall suggests potential for preventing catastrophic operational disruptions, a priority in oil-producing regions like Nigeria, as highlighted by Yan et al. (2018). The real-time capability supports integration into existing OT frameworks, potentially reducing response times to threats.

CONCLUSION

In this paper, we proposed a multilevel verification system designed to mitigate cyber risks in the upstream operations of smart oilfields, leveraging a Long Short-Term Memory (LSTM) Deep Learning model to detect cyberattacks in real time. Experimental evaluations using simulated SCADA datasets demonstrate the framework's ability to identify cyber-physical inconsistencies, reduce false positives, and improve response times across multiple operational levels. The system also offers scalability and adaptability, making it suitable for diverse upstream scenarios with varying risk profiles.

The study successfully demonstrated the system's capability, achieving exceptional performance with a testing accuracy of 0.9971, perfect recall, and a rapid processing rate of 0.024 seconds per sample across a simulated dataset of 1740 instances. The real-time monitoring simulation further validated its practical utility, generating 38 high-confidence alerts from 50 new data points, underscoring its potential to safeguard critical infrastructure.

The significance of this work lies in its innovative integration of temporal deep learning with a multilayered verification approach, offering a novel framework that addresses the evolving cyber threats. This contributes to both theoretical advancements in anomaly detection within industrial control systems and practical applications by providing oil and gas operators with a scalable tool to mitigate risks, potentially reducing economic and environmental impacts in regions like Nigeria. However, the absence of real operational data and the hardware demands of the current setup will present constraints that affect real-world applicability.

FUTURE WORKS

Future research should validate the system with real-world data from operational oilfields, incorporating diverse attack vectors (e.g., ransomware, APTs) to assess robustness. Longitudinal studies over months could evaluate model drift and necessitate adaptive retraining protocols. Exploring edge-optimized versions (e.g., quantized models) on lower-spec hardware, as suggested by the INT8 quantization in the methodology, could broaden deployment feasibility. Additionally, integrating human factors analysis, such as social engineering detection, and federated learning for distributed oilfield networks could enhance the system's applicability and resilience.

REFERENCES

Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2019). An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. IEEE Access. 8(8) 83965 - 83973

Alkahtani, H., & Aldhyani, T. H. H. (2022). Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems: Industrial Control Systems. Electronics. 11(11), 1-25.

Al-kahtani, M. S., Mehmood, Z., Sadad, T., Zada, I., Ali, G., & ElAffendi, M. (2023). Intrusion Detection in the Internet of Things Using Fusion of GRU-LSTM Deep Learning Model. Intelligent Automation and Soft Computing (IASC). 37(2), 2279-2290.

Banaamah, A. M., & Ahmad, I. (2022). Intrusion Detection in IoT Using Deep Learning. Sensors. 22(21), 8417.

Butun, I., Morgera, S. D., & Nadeem, T. (2019). A survey of security in wireless sensor networks. Ad Hoc Networks. 9(1), 25-32.

Cardenas, A. A., Amin, S., & Sastry, S. (2011). Research challenges for the security of control systems. HotSec'08: Proceedings of the 3rd conference on Hot topics in security. Article No.: 6, Pages 1 – 6.

Ghani, A. A., & Alasadi, S. A. (2025). A Deep Learning Algorithm to Cybersecurity: Enhancing Intrusion Detection with a Hybrid GRU and BiLSTM Model. Engineering, Technology & Applied Science Research. 15(3), 23605-23612.

Ghasemi, S., Dehghantanha, A., Conti, M., & Choo, K. R. (2024). Federated Learning for Cyber Attack Detection in IoT: A Customized Temporal Federated Learning through Adversarial Networks. *Journal UMY*. Retrieved from https://journal.umy.ac.id/index.php/jrc/article/download/24529/11301/93769

Harshavardhan, A., Sree Vani, M., Patil, A., Yamsani, N., & Archana, K. (2025). Hybrid Deep Learning Framework for Intrusion Detection: Integrating CNN, LSTM, and Attention Mechanisms to Enhance Cybersecurity. Journal of Theoretical and Applied Information Technology. 103(1), 63-79.

Humayed, A., Lin, D., Li, F., & G. O. M. (2017). Cyberphysical systems security: A survey. IEEE Communications Surveys & Tutorials. 4(6), 1802 – 1831.

Igure, V. M., Laughter, D. R., & Williams, R. D. (2006). Security issues in SCADA networks. Computers & Security. 25(7), 498-506.

Isaac, S., Ayodeji, D. K., Luqman, Y., Karma, S. M., & Aminu, J. (2024). Cyber security Attack Detection Model Using Semi-Supervised Learning. FUDMA Journal of Sciences. 8(2), 92-100.

Kuzyakov, O. N., Gluhih, I. & Andreeva, M., (2021). Cyber-Physical System for Pipeline Monitoring as a Component of Smart Oil Field. 394-403.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature. 521(7553):436-443.

Mohamad, H. S., & Mohammad, S. (2017). A survey on machine learning based intrusion detection systems. *International Journal of Computer Network and Information Security, 9*(1), 113.

Yan, H., & Han, M. (2020). Anomaly detection for industrial control systems using deep neural networks with class imbalance learning. *Sensors, 20*(22), 6527.

Yan, H., An, Y., Hong, L., Yuyan, S. & Limin, S. (2018). A survey of intrusion detection on industrial control systems. International Journal of Distributed Sensor Networks. 14(8), 1-14.