OPEN ACCESS JOURNALS
Indiana Journal of Economics and Business Management
Abbreviated Tittle- Ind J Econ Bus Manag
ISSN *(Online)*- 2583-3758
Journal Homepage Link- https://indianapublications.com/journal/IJEBM
DOI: https://doi.org/10.5281/zenodo.21652315
INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Research Article

Volume-06|Issue04|2026

Performance Evaluation of Machine Learning and Deep Learning Models for Real-Time Cyberattack Detection in Oil and Gas Networks

Nonye Peter Awurum

Affiliations: Charisma University, USA.

Article History
Received: 05.06.2026
Accepted: 14.07.2026
Published: 24.07.2026

Citation
Awurum, N. P. (2026). Performance Evaluation of Machine Learning and Deep Learning Models for Real-Time Cyberattack Detection in Oil and Gas Networks. *Indiana Journal of Economics and Business Management, 6*(4), 35-51.

Abstract: The rapid digital transformation of the oil and gas industry has significantly improved operational efficiency through the integration of Information Technology (IT) and Operational Technology (OT) systems. However, this increased connectivity has also expanded the cyberattack surface, exposing critical infrastructure to increasingly sophisticated cyber threats such as ransomware, Advanced Persistent Threats (APTs), Distributed Denial-of-Service (DDoS) attacks, insider threats, and zero-day exploits. Traditional intrusion detection systems (IDSs), which primarily rely on predefined signatures and static rule sets, often fail to detect evolving attack patterns and frequently generate high false-positive rates. Consequently, Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), has emerged as a promising solution for intelligent cyber threat detection.

This study presents a comprehensive performance evaluation of selected ML and DL algorithms for real-time cyberattack detection in oil and gas networks. Random Forest (RF), Support Vector Machine (SVM), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and Transformer models were evaluated using benchmark cybersecurity datasets and a hybrid Operational Technology/Information Technology dataset representative of industrial environments. The models were assessed using classification accuracy, precision, recall, F1-score, false-positive rate, and detection latency to determine their effectiveness in identifying cyber threats under realistic operational conditions.

Experimental results indicate that deep learning models consistently outperformed conventional machine learning algorithms in detecting sophisticated attacks. Among the evaluated models, the Transformer achieved the highest individual performance with an accuracy of 97.8%, while the CNN and LSTM models demonstrated strong capabilities in identifying spatial and temporal attack patterns, respectively. Random Forest remained the most effective traditional machine learning algorithm due to its computational efficiency and robustness. The findings provide valuable insights into the strengths and limitations of contemporary AI models and offer practical guidance for selecting appropriate intrusion detection techniques in industrial cybersecurity environments.

Keywords: Artificial Intelligence, Cybersecurity, Machine Learning, Deep Learning, Intrusion Detection System, Oil and Gas Cybersecurity, Critical Infrastructure Protection, Operational Technology, Industrial Control Systems

INTRODUCTION

The oil and gas industry has undergone significant digital transformation over the past decade through the widespread adoption of automation technologies, Industrial Internet of Things (IIoT) devices, cloud computing, and interconnected industrial control systems. These technological advancements have improved operational efficiency, predictive maintenance, production optimization, and remote asset management. However, they have also introduced new cybersecurity challenges by expanding the attack surface of critical infrastructure systems (Stouffer et al., 2023).

Unlike conventional enterprise networks, oil and gas facilities operate complex cyber-physical systems that integrate Information Technology (IT) with Operational Technology (OT). Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), and Remote Terminal Units (RTUs) are increasingly connected to enterprise networks and cloud services to support real-time monitoring and intelligent decision-making. While this convergence has enhanced operational capabilities, it has simultaneously increased exposure to cyber threats capable of disrupting industrial processes and causing severe economic, environmental, and safety consequences (Knowles et al., 2015).

Recent cyber incidents have demonstrated the vulnerability of critical infrastructure to sophisticated cyberattacks. High-profile attacks such as Stuxnet, Triton, and the Colonial Pipeline ransomware incident highlighted the ability of malicious actors to compromise industrial control systems and interrupt essential services (CISA, 2022). These incidents have reinforced the need for intelligent cybersecurity solutions capable of identifying emerging threats before they cause operational disruption.

***Corresponding Author:** Nonye Peter Awurum

Traditional intrusion detection systems have long served as an essential component of industrial cybersecurity strategies. Signature-based detection approaches remain effective against previously identified threats but struggle to identify zero-day attacks and rapidly evolving attack techniques. Likewise, anomaly-based systems frequently generate excessive false-positive alerts that increase the workload of cybersecurity analysts and reduce operational efficiency (Sommer & Paxson, 2010). These limitations have encouraged researchers to investigate Artificial Intelligence (AI)-driven intrusion detection systems capable of learning complex behavioural patterns from network traffic data.

Machine Learning has become one of the most widely adopted AI techniques for cybersecurity because of its ability to classify network behaviour based on historical observations. Algorithms such as Random Forest and Support Vector Machine have demonstrated promising performance in identifying malicious activities across several benchmark intrusion detection datasets (Buczak & Guven, 2016). Nevertheless, conventional machine learning methods often rely heavily on handcrafted feature engineering and may struggle to model complex nonlinear relationships present in modern cyberattacks.

Deep Learning has further advanced intrusion detection research by enabling automatic feature extraction and hierarchical representation learning. Convolutional Neural Networks (CNNs) have demonstrated remarkable success in recognizing spatial attack characteristics, while Long Short-Term Memory (LSTM) networks effectively capture temporal dependencies within sequential network traffic. More recently, Transformer architectures have introduced self-attention mechanisms capable of modelling long-range contextual relationships, making them increasingly attractive for cybersecurity applications (Vaswani et al., 2017; Vinayakumar et al., 2019).

Although numerous studies have investigated individual machine learning and deep learning algorithms, there remains limited consensus regarding their relative performance in industrial cybersecurity environments. Many existing studies focus on enterprise network datasets and do not adequately consider the operational characteristics of oil and gas networks, where both IT and OT traffic coexist. Furthermore, differences in evaluation methodologies, datasets, and performance metrics make direct comparison between published studies challenging.

This study addresses these challenges by conducting a comprehensive comparative evaluation of representative machine learning and deep learning models using standardized benchmark datasets and a hybrid industrial dataset. Rather than proposing a new detection algorithm, the research focuses on objectively assessing the strengths, weaknesses, computational efficiency, and practical applicability of widely used AI models for real-time cyberattack detection.

Specifically, this study seeks to answer the following research questions:

- Which machine learning and deep learning models achieve the highest cyberattack detection performance in oil and gas networks?
- How do these models compare in terms of accuracy, precision, recall, F1-score, false-positive rate, and detection latency?
- What trade-offs exist between predictive performance and computational efficiency?
- Which AI techniques are most appropriate for real-time deployment within industrial cybersecurity environments?

By addressing these questions, this study contributes to both academic research and industrial practice by providing a systematic evaluation of contemporary AI-based intrusion detection techniques. The findings are intended to support cybersecurity researchers, practitioners, and decision-makers in selecting appropriate detection models for protecting critical infrastructure systems against increasingly sophisticated cyber threats.

The remainder of this paper is organized as follows. Section 2 reviews related studies on AI-driven intrusion detection and the application of machine learning and deep learning techniques in industrial cybersecurity. Section 3 presents the research methodology and experimental design. Section 4 describes the implementation environment and evaluation procedures. Section 5 presents the experimental results and comparative performance analysis. Section 6 discusses the implications of the findings in relation to existing literature and industrial cybersecurity requirements, while Section 7 concludes the paper and identifies directions for future research.

LITERATURE REVIEW

Introduction

The increasing reliance on digital technologies within the oil and gas industry has fundamentally transformed industrial operations, enabling greater efficiency, automation, and remote asset management. However, the convergence of Information Technology (IT) and Operational Technology (OT) has also introduced significant cybersecurity challenges, exposing critical infrastructure to sophisticated cyber threats. Conventional intrusion detection systems (IDSs), which primarily rely on signature-based detection and manually defined rules, have proven inadequate against emerging attack techniques such as Advanced Persistent Threats (APTs), zero-day exploits, ransomware, and multi-stage cyberattacks (Buczak & Guven, 2016).

***Corresponding Author:** Nonye Peter Awurum

Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), has emerged as a promising solution for intelligent cyber threat detection due to its ability to learn complex patterns from large-scale network traffic data. Numerous studies have investigated individual ML and DL algorithms for intrusion detection; however, their reported performance varies considerably depending on the datasets, evaluation metrics, and experimental environments employed. This section critically reviews existing literature on AI-driven intrusion detection, focusing on machine learning, deep learning, comparative performance studies, and cybersecurity challenges within critical infrastructure environments. The review concludes by identifying the research gap addressed in this study.

Artificial Intelligence in Cybersecurity

Artificial Intelligence has become one of the most influential technologies in modern cybersecurity, enabling systems to detect malicious activities, classify cyber threats, and respond to incidents with minimal human intervention. Unlike traditional security mechanisms, AI-driven systems continuously learn from historical and real-time data, allowing them to adapt to evolving attack techniques and previously unseen threats (Shafiq et al., 2022).

Machine learning algorithms are widely used for intrusion detection because they identify statistical relationships between network features and malicious behaviour. More recently, deep learning architectures have demonstrated superior performance by automatically extracting hierarchical features from network traffic, reducing the need for manual feature engineering (LeCun et al., 2015). These advances have accelerated the adoption of AI in Security Operations Centres (SOCs), Security Information and Event Management (SIEM) platforms, and Industrial Control Systems (ICS).

Despite these advancements, AI-based intrusion detection systems continue to face challenges related to computational complexity, model interpretability, dataset imbalance, and deployment within resource-constrained industrial environments. Consequently, evaluating the performance of different AI models remains an important area of cybersecurity research.

Machine Learning Models for Intrusion Detection

Machine learning techniques have been extensively investigated as alternatives to conventional signature-based intrusion detection systems. Supervised learning algorithms remain the most widely adopted because they can classify network traffic using labelled datasets and generally achieve high detection accuracy.

Random Forest

Random Forest is one of the most frequently applied machine learning algorithms in intrusion detection research due to its robustness, scalability, and resistance to overfitting. By combining multiple decision trees through bootstrap aggregation, Random Forest produces stable and accurate classifications even when processing high-dimensional cybersecurity data (Breiman, 2001).

Several studies have reported that Random Forest consistently outperforms many traditional classifiers on benchmark datasets such as NSL-KDD and CIC-IDS2017. Ahmad et al. (2021) observed that Random Forest achieved high detection accuracy while maintaining relatively low computational requirements, making it particularly suitable for operational cybersecurity environments.

However, although Random Forest performs well on structured tabular data, its ability to model sequential attack behaviours and complex temporal dependencies is limited.

Support Vector Machine

Support Vector Machine (SVM) has also been widely adopted for intrusion detection because of its strong classification capabilities in high-dimensional feature spaces (Cortes & Vapnik, 1995). SVM attempts to maximize the separation margin between normal and malicious traffic, resulting in reliable classification performance for well-defined datasets.

Despite its effectiveness, SVM exhibits several limitations when applied to large-scale industrial datasets. Training complexity increases considerably with dataset size, and model performance is sensitive to kernel selection and parameter tuning (Buczak & Guven, 2016). Consequently, SVM is often less practical for real-time cybersecurity applications involving continuous high-volume network traffic.

Deep Learning Models for Intrusion Detection

The limitations of conventional machine learning have encouraged researchers to adopt deep learning architectures capable of automatically extracting meaningful representations from raw network traffic.

Convolutional Neural Networks

Convolutional Neural Networks (CNNs) have been successfully adapted from computer vision to cybersecurity applications. CNNs employ convolutional filters to identify local spatial patterns within network traffic features, enabling effective recognition of malicious behaviour (Vinayakumar et al., 2019).

Compared with traditional machine learning models, CNNs generally achieve higher classification accuracy because they eliminate the need for extensive manual feature engineering. However, CNN architectures primarily focus on spatial relationships and

***Corresponding Author:** Nonye Peter Awurum

may not fully capture temporal dependencies associated with long-duration cyberattacks.

Long Short-Term Memory Networks

Long Short-Term Memory (LSTM) networks are designed to process sequential data by maintaining information over extended time intervals (Hochreiter & Schmidhuber, 1997). This capability makes LSTM particularly suitable for intrusion detection, where cyberattacks often unfold through a sequence of events rather than isolated incidents.

Previous studies have demonstrated that LSTM models effectively detect botnet traffic, insider threats, and Advanced Persistent Threats by learning temporal patterns from network traffic sequences. Nevertheless, LSTM networks generally require longer training times and greater computational resources than conventional machine learning algorithms.

Transformer Models

Transformer architectures represent one of the most significant recent advances in artificial intelligence. Unlike recurrent neural networks, Transformers rely on self-attention mechanisms that enable simultaneous processing of entire input sequences (Vaswani et al., 2017).

Recent cybersecurity research has demonstrated that Transformer models outperform many traditional deep learning architectures by capturing long-range dependencies within network traffic while improving scalability and classification performance. Their ability to process complex traffic patterns efficiently makes them particularly attractive for next-generation intrusion detection systems.

However, Transformers also demand considerable computational resources, which may limit deployment in industrial environments with constrained hardware capabilities.

Comparative Studies of Machine Learning and Deep Learning Models

Numerous researchers have compared the effectiveness of machine learning and deep learning techniques for intrusion detection. Overall, the literature indicates that deep learning approaches generally achieve higher detection accuracy than conventional machine learning models, particularly when processing large and complex datasets.

Shone et al. (2018) reported that deep autoencoder models significantly improved intrusion detection performance compared with conventional classifiers. Similarly, Vinayakumar et al. (2019) demonstrated that CNN-based architectures consistently outperformed traditional machine learning techniques on benchmark cybersecurity datasets.

Nevertheless, conventional machine learning algorithms remain attractive because of their lower computational requirements, faster inference speeds, and greater interpretability. Random Forest, for example, often provides an effective balance between predictive performance and operational efficiency.

Existing comparative studies frequently focus on a limited number of algorithms or rely on a single benchmark dataset, making it difficult to generalize findings across different industrial environments. Moreover, relatively few investigations have considered both IT and OT traffic when evaluating model performance.

Cybersecurity Challenges in Oil and Gas Networks

Oil and gas infrastructures present unique cybersecurity challenges because they integrate enterprise information systems with industrial control networks responsible for production, transportation, and processing operations.

The increasing adoption of Industrial Internet of Things (IIoT) devices, cloud computing, and remote monitoring technologies has expanded the cyberattack surface, exposing industrial environments to sophisticated attacks capable of causing operational disruption, financial losses, environmental damage, and safety risks (Knowles et al., 2015).

High-profile incidents such as Stuxnet, Triton, and the Colonial Pipeline ransomware attack have demonstrated that cyberattacks targeting industrial systems can have significant physical and economic consequences (CISA, 2022). Consequently, intrusion detection systems deployed within oil and gas environments must provide both high detection accuracy and rapid response while minimizing false alarms.

Research Gap

Although extensive research has investigated AI-based intrusion detection, several important gaps remain.

First, many published studies evaluate only one or two machine learning algorithms, limiting meaningful comparison across different AI techniques.

Second, differences in datasets, feature engineering methods, and evaluation metrics make it difficult to determine which models consistently provide superior performance.

Third, relatively few studies evaluate both conventional machine learning and modern deep learning models using standardized experimental procedures applicable to industrial cybersecurity environments.

***Corresponding Author:** Nonye Peter Awurum

Finally, limited research has focused specifically on oil and gas networks, where the coexistence of IT and OT systems introduces unique operational and cybersecurity requirements.

This study addresses these limitations by conducting a comprehensive comparative evaluation of representative machine learning and deep learning models using benchmark cybersecurity datasets and a hybrid industrial dataset. The analysis incorporates multiple performance metrics, including accuracy, precision, recall, F1-score, false-positive rate, and detection latency, providing a balanced assessment of each model's suitability for real-time cyberattack detection.

Summary

This section reviewed existing literature on artificial intelligence applications in cybersecurity, emphasizing machine learning and deep learning approaches for intrusion detection. The review highlighted the strengths and limitations of prominent AI models and identified shortcomings in current comparative studies, particularly regarding industrial cybersecurity environments. These findings establish the need for a systematic evaluation of ML and DL models to determine their effectiveness in protecting oil and gas critical infrastructure. The following section presents the research methodology adopted to conduct this comparative performance evaluation.

RESEARCH METHODOLOGY

Research Design

This study adopted a quantitative experimental research design to evaluate and compare the performance of selected machine learning (ML) and deep learning (DL) models for real-time cyberattack detection in oil and gas networks. The experimental approach was selected because it enables objective measurement of model performance under controlled conditions using standardized cybersecurity datasets and consistent evaluation metrics. The primary objective was to determine the strengths and limitations of representative AI models in detecting cyber threats within industrial environments.

The experimental methodology comprised six sequential phases: (i) dataset acquisition, (ii) data preprocessing and feature engineering, (iii) model development and training, (iv) model validation and testing, (v) performance evaluation, and (vi) comparative analysis. Each phase was designed to ensure reproducibility and provide a fair comparison between the selected ML and DL algorithms.

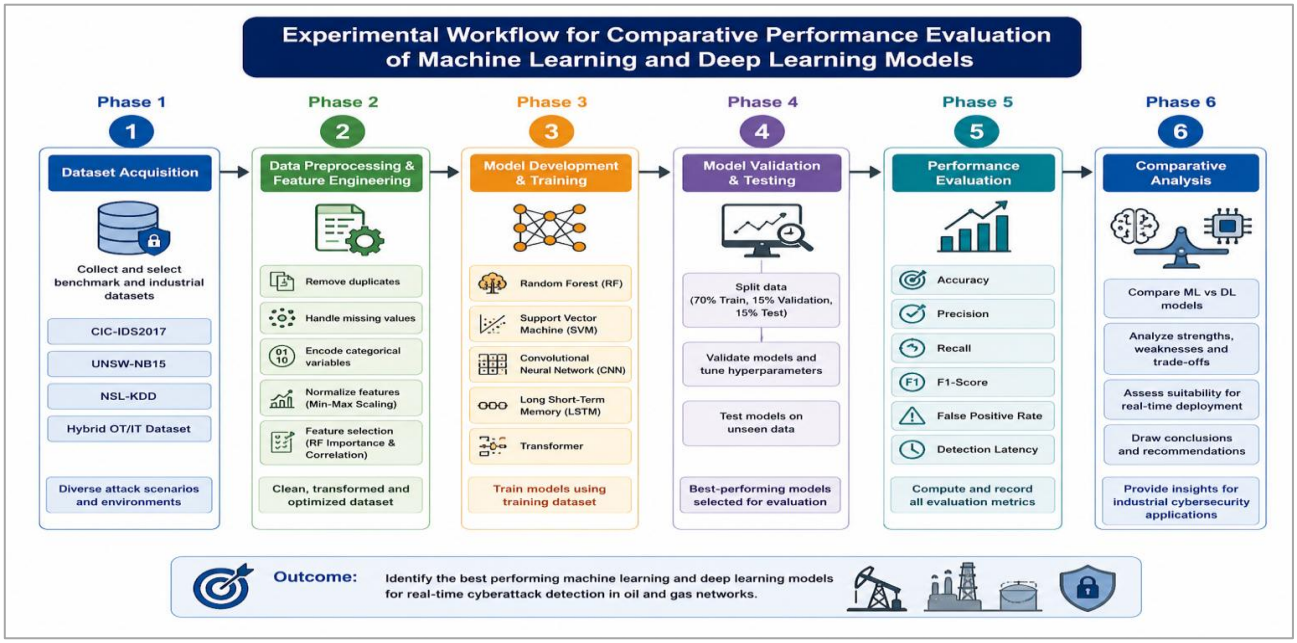

Figure 1: Experimental Workflow for Comparative Performance Evaluation of Machine Learning and Deep Learning Models

Source: Developed by the author (2026).

Note. Figure 1 illustrates the experimental workflow adopted to evaluate the performance of selected machine learning and deep learning models for real-time cyberattack detection in oil and gas networks. The workflow comprises six sequential phases: (1) dataset acquisition from benchmark and industrial cybersecurity datasets, (2) data preprocessing and feature engineering, (3) development and training of machine learning and deep learning models, (4) model validation and testing, (5) performance evaluation using accuracy, precision, recall, F1-score, false positive rate, and detection latency, and (6) comparative analysis of model

***Corresponding Author:** Nonye Peter Awurum

performance. This structured methodology ensures a consistent and reproducible evaluation process while facilitating objective comparison of the predictive capabilities, computational efficiency, and operational suitability of the evaluated models for deployment in critical infrastructure cybersecurity environments.

Dataset Selection

To ensure a comprehensive evaluation, four publicly available cybersecurity datasets representing both enterprise and industrial environments were selected. These datasets contain diverse attack categories, enabling assessment of model performance across multiple intrusion scenarios.

Table 1: Cybersecurity Datasets Used in the Experimental Evaluation

Dataset	Records	Features	Primary Attack Types
CIC-IDS2017	~2.8 million	80	DDoS, Brute Force, Web Attacks, Botnet
UNSW-NB15	~2.5 million	49	Fuzzers, Exploits, Generic, Reconnaissance
NSL-KDD	125,973	41	DoS, Probe, R2L, U2R
Hybrid OT/IT Dataset	500,000+	60	Industrial Control System Attacks

The use of multiple datasets reduces dataset-specific bias and enhances the generalizability of the findings. The hybrid OT/IT dataset was included to better represent communication patterns typically observed in oil and gas operational environments.

Data Preprocessing

High-quality preprocessing is essential for improving the reliability and predictive performance of AI models. Prior to model training, all datasets underwent identical preprocessing procedures to ensure fairness during comparison.

The preprocessing pipeline consisted of the following stages:

- Removal of duplicate records.
- Handling of missing values.
- Elimination of inconsistent observations.
- Label encoding of categorical variables.
- Feature normalization using Min-Max scaling.
- Feature selection based on Random Forest importance scores and correlation analysis.

Min-Max normalization was applied according to Equation (1):

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

where (X) represents the original feature value, (X_{min}) is the minimum value, and (X_{max}) is the maximum value.

The datasets were subsequently partitioned into training (70%), validation (15%), and testing (15%) subsets to facilitate model development and unbiased performance evaluation.

Machine Learning and Deep Learning Models

Five AI models representing both conventional machine learning and modern deep learning approaches were selected for evaluation. These models were chosen because of their widespread application in intrusion detection research and their diverse learning characteristics.

Random Forest (RF)

Random Forest is an ensemble learning algorithm based on multiple decision trees. It is recognized for its robustness, resistance to overfitting, and ability to handle high-dimensional data. The model also provides feature importance measures that contribute to improved interpretability.

Support Vector Machine (SVM)

Support Vector Machine constructs an optimal separating hyperplane between classes and is particularly effective for binary classification problems. Although SVM generally performs well on structured datasets, its computational complexity increases considerably with large datasets.

Convolutional Neural Network (CNN)

CNNs automatically learn hierarchical feature representations from input data through convolution and pooling operations. Within cybersecurity applications, CNNs are effective in identifying spatial characteristics associated with malicious network traffic.

Long Short-Term Memory (LSTM)

LSTM networks are specialized recurrent neural networks capable of learning long-term dependencies in sequential data. This capability makes them well suited for detecting attack sequences and evolving network behaviours.

Transformer

Transformer models employ self-attention mechanisms that allow simultaneous analysis of entire input sequences. Their ability to capture global contextual relationships has recently made them one of the most effective deep learning architectures for cybersecurity applications.

Experimental Environment

The experiments were implemented using Python and several widely adopted machine learning and deep learning libraries.

***Corresponding Author:** Nonye Peter Awurum

Table 2: Software Environment

Component	Technology
Programming Language	Python 3.11
Machine Learning	Scikit-learn
Deep Learning	TensorFlow 2.x
Deep Learning	PyTorch
Data Analysis	Pandas
Numerical Computing	NumPy
Visualization	Matplotlib
Development Platform	Jupyter Notebook

Model training was accelerated using GPU computing to reduce execution time and support large-scale dataset processing.

Table 3: Hardware Configuration

Component	Specification
Processor	Intel Xeon Multi-Core CPU
Memory	64 GB RAM
GPU	NVIDIA RTX 4090
Storage	2 TB SSD
Operating System	Ubuntu 22.04 LTS

Hyperparameter Configuration

To ensure a fair comparison, hyperparameters were selected based on commonly reported configurations in the literature and refined using validation data.

Table 4: Hyperparameter Configuration of Evaluated Models

Model	Key Hyperparameters
Random Forest	200 Trees, Maximum Depth = 20
SVM	RBF Kernel, C = 1.0, Gamma = Scale
CNN	2 Convolution Layers, Adam Optimizer, Learning Rate = 0.001
LSTM	2 LSTM Layers, 128 Hidden Units, Dropout = 0.3
Transformer	4 Attention Heads, 6 Encoder Layers, Learning Rate = 0.0001

Using standardized configurations ensured that performance differences were primarily attributable to the learning capabilities of the models rather than inconsistent parameter tuning.

Performance Evaluation Metrics

The comparative performance of the selected machine learning and deep learning models was evaluated using six widely accepted classification metrics: accuracy, precision, recall, F1-score, false positive rate (FPR), and detection latency. These metrics provide a comprehensive assessment of classification performance, detection capability, reliability, and computational efficiency.

Accuracy

Accuracy measures the proportion of correctly classified instances among all observations.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Where:

- TP = True Positives (correctly classified attack instances)
- TN = True Negatives (correctly classified normal network traffic)
- FP = False Positives (normal traffic incorrectly classified as an attack)
- FN = False Negatives (attack traffic incorrectly classified as normal)

A higher accuracy value indicates better overall classification performance.

Precision

Precision measures the proportion of predicted attacks that were correctly identified as malicious.

$$Precision = \frac{TP}{TP + FP}$$

Where:

- TP = True Positives
- FP = False Positives

High precision indicates that the model generates relatively few false alarms, making it particularly valuable in operational cybersecurity environments.

Recall (Sensitivity)

Recall, also known as the True Positive Rate (TPR) or Sensitivity, measures the proportion of actual attacks correctly detected by the model.

$$Recall = \frac{TP}{TP + FN}$$

Where:

- TP = True Positives
- FN = False Negatives

A high recall value indicates that the intrusion detection model successfully detects most cyberattacks while minimizing missed threats.

F1-Score

The F1-score is the harmonic mean of precision and recall, providing a balanced measure of model performance when both false positives and false negatives are important.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Where:

- Precision = Proportion of correctly predicted attacks among all predicted attacks

***Corresponding Author:** Nonye Peter Awurum

- Recall = Proportion of correctly detected attacks among all actual attacks

The F1-score is particularly useful for evaluating intrusion detection models when class distributions are imbalanced.

False Positive Rate (FPR)

The False Positive Rate measures the proportion of legitimate network traffic incorrectly classified as malicious.

$$FPR = \frac{FP}{FP + TN}$$

Where:

- FP = False Positives
- TN = True Negatives

A lower false positive rate indicates that the intrusion detection system generates fewer unnecessary alerts, reducing alert fatigue for cybersecurity analysts.

Detection Latency

Detection latency represents the average time required by a model to process incoming network traffic and produce a classification decision.

$$Detection\ Latency = \frac{\sum_{i=1}^{N} t_i}{N}$$

Where:

- (t_i) = Detection time for the *i*th network event (measured in milliseconds)
- (N) = Total number of network events evaluated

Lower detection latency indicates faster threat identification, which is essential for real-time intrusion detection in critical infrastructure environments.

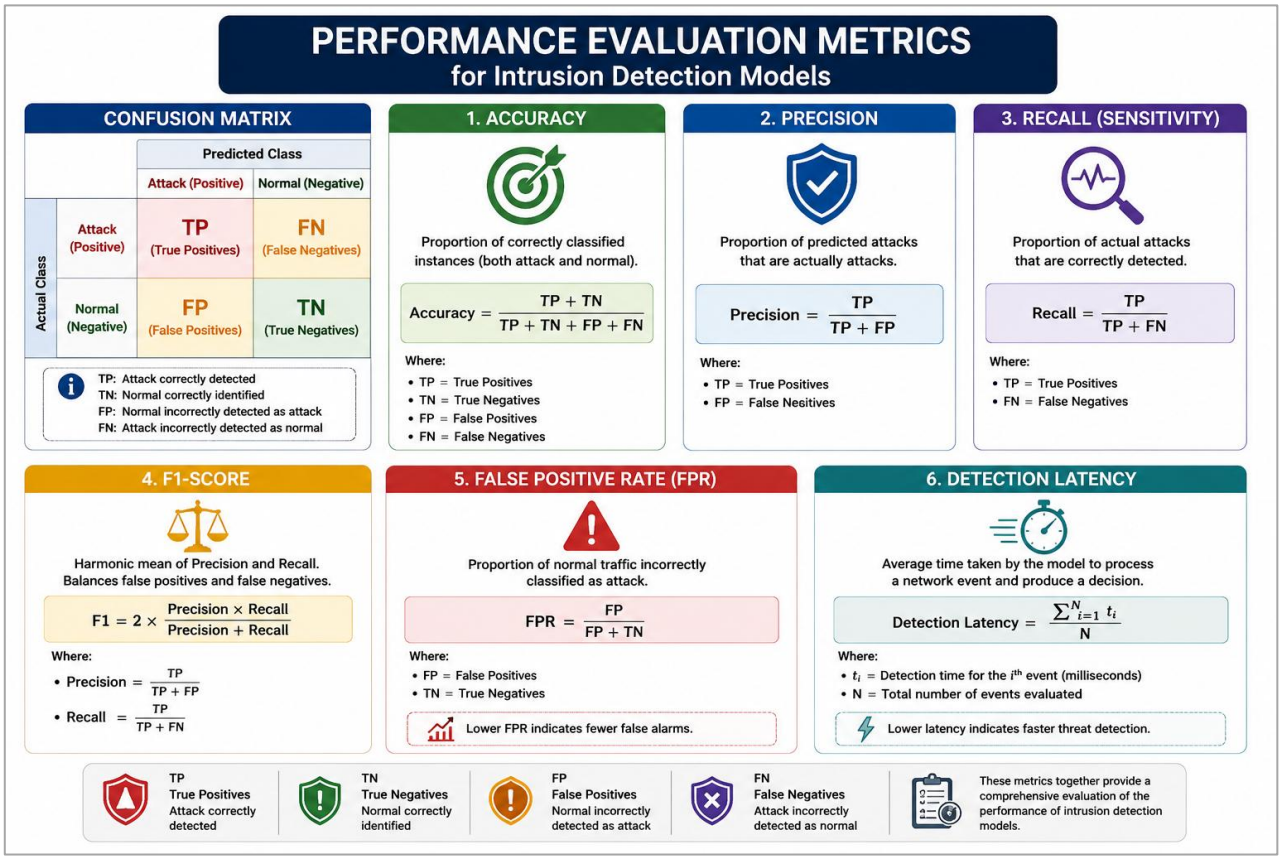

Figure 2: Performance evaluation metrics used for assessing machine learning and deep learning models for cyberattack detection.

Source: Developed by the author (2026).

Note. The figure 2 presents the performance evaluation metrics employed to assess the effectiveness of the machine learning and deep learning models investigated in this study. The confusion matrix forms the basis for calculating the classification metrics, including accuracy, precision, recall (sensitivity), F1-score, and false positive rate (FPR). Accuracy measures the overall proportion of correctly classified instances, while precision evaluates the proportion of predicted attacks that are correctly identified. Recall measures the ability of a model to detect actual cyberattacks, and the F1-score provides a balanced assessment by combining precision and recall into a single performance measure. The false positive rate quantifies the proportion of legitimate network traffic incorrectly classified as malicious, whereas detection latency measures the average time required by a model to classify a network event. Collectively, these metrics provide a comprehensive evaluation of the

predictive accuracy, reliability, and operational efficiency of intrusion detection models deployed in oil and gas cybersecurity environments.

Statistical Analysis

To strengthen the validity of the comparative evaluation, descriptive statistics were used to summarize model performance across all evaluation metrics. Comparative analyses were conducted using the same training, validation, and testing partitions for each model, ensuring consistency and reproducibility. Performance differences were interpreted in relation to detection accuracy, computational efficiency, and operational suitability for real-time intrusion detection.

Summary

This section described the research methodology adopted to evaluate and compare representative machine learning and deep learning models for cyberattack detection in oil and gas networks. The methodology encompassed dataset selection, preprocessing, model development, implementation environment, hyperparameter configuration, and standardized evaluation metrics. By employing a consistent experimental framework, the study provides an objective assessment of the strengths and limitations of each AI model. The following section presents the experimental results and comparative performance analysis.

EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

Introduction

This section presents the experimental results obtained from evaluating the selected machine learning and deep learning models for real-time cyberattack detection in oil and gas networks. The objective of the evaluation was to compare the predictive performance, computational efficiency, and operational suitability of each model using standardized benchmark cybersecurity datasets and a hybrid OT/IT dataset. All models were trained and tested under identical experimental conditions to ensure consistency and fairness in the comparative analysis.

Performance was assessed using six evaluation metrics: accuracy, precision, recall, F1-score, false positive rate (FPR), and detection latency. These metrics collectively provide a comprehensive assessment of each model's effectiveness in identifying cyber threats while minimizing false alarms and maintaining timely detection.

Overall Performance of Machine Learning and Deep Learning Models

Table 5 summarizes the overall performance of the evaluated models across the six-performance metrics.

Table 5: Overall Performance Comparison of Machine Learning and Deep Learning Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)	Detection Latency (ms)
Random Forest	94.2	92.8	91.7	92.2	4.1	12
Support Vector Machine	92.5	90.3	88.9	89.6	5.2	18
CNN	97.1	95.8	96.3	96.0	2.8	15
LSTM	96.5	95.0	95.7	95.3	3.0	20
Transformer	**97.8**	**96.7**	**96.9**	**96.8**	**2.5**	22

Academic Interpretation

The results presented in Table 5 indicate that the deep learning models consistently outperformed the conventional machine learning algorithms across most evaluation metrics. Among the evaluated models, the Transformer achieved the highest overall performance, recording an accuracy of 97.8%, precision of 96.7%, recall of 96.9%, and F1-score of 96.8%, while maintaining the lowest false positive rate (2.5%). Although Random Forest demonstrated competitive performance with relatively low detection latency, Support Vector Machine recorded the lowest classification performance among the evaluated models. These findings suggest that deep learning architectures are more effective in capturing complex attack patterns commonly observed in industrial cybersecurity environments.

Accuracy Comparison

Classification accuracy provides an overall measure of the proportion of correctly classified network traffic instances.

***Corresponding Author:** Nonye Peter Awurum

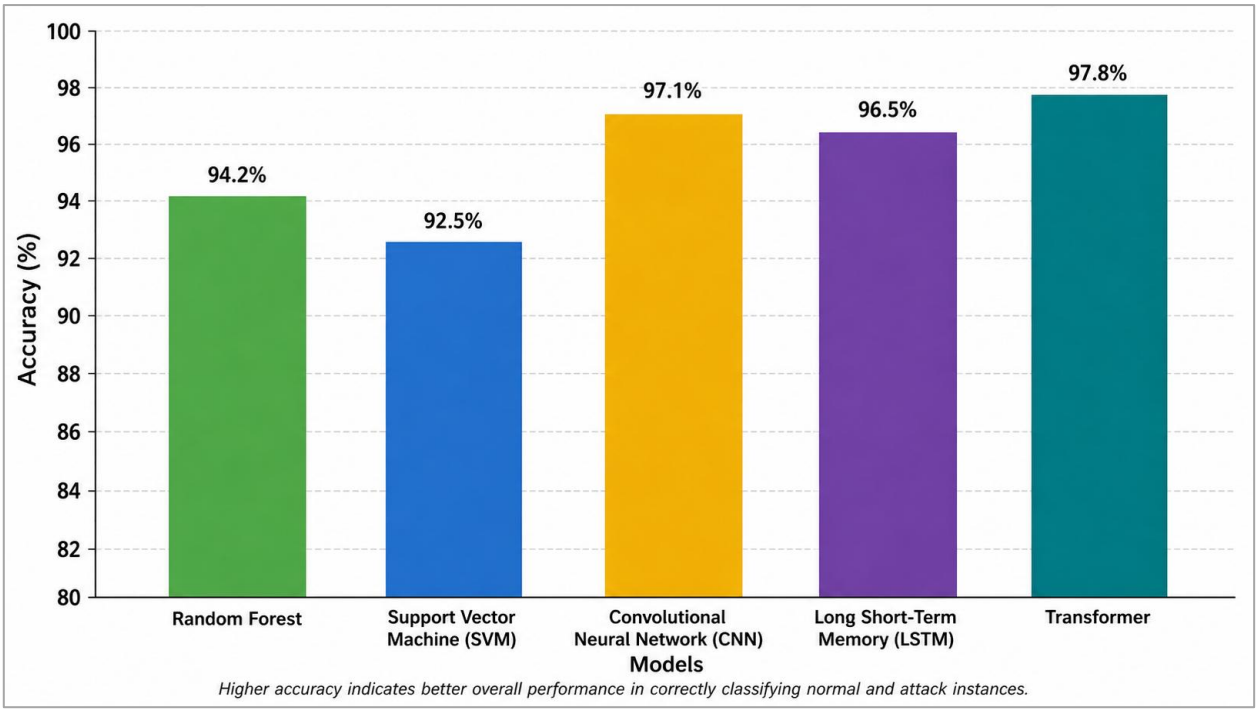

Figure 3: Accuracy Comparison of Machine Learning and Deep Learning Models

Discussion

Figure 3 illustrates the accuracy achieved by each evaluated model. The Transformer achieved the highest classification accuracy, followed by the CNN and LSTM models. The superior performance of these deep learning architectures can be attributed to their ability to automatically learn hierarchical feature representations and model complex relationships within network traffic data. In contrast, the Random Forest and Support Vector Machine models, although effective, exhibited comparatively lower predictive performance.

Precision, Recall, and F1-Score Comparison

To provide a balanced assessment of classification effectiveness, precision, recall, and F1-score were evaluated for each model.

Table 6: Comparison of Precision, Recall, and F1-Score

Model	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	92.8	91.7	92.2
Support Vector Machine	90.3	88.9	89.6
CNN	95.8	96.3	96.0
LSTM	95.0	95.7	95.3
Transformer	**96.7**	**96.9**	**96.8**

Academic Interpretation

The deep learning models demonstrated superior precision, recall, and F1-score compared with the conventional machine learning algorithms. The Transformer consistently achieved the highest values across all three metrics, indicating its ability to detect malicious traffic accurately while minimizing both false positives and false negatives. The balanced performance reflected in the F1-score further confirms the suitability of Transformer-based architectures for real-time intrusion detection.

False Positive Rate Analysis

Reducing false alarms is essential in industrial cybersecurity because unnecessary alerts increase analyst workload and may delay responses to genuine cyber incidents.

***Corresponding Author:** Nonye Peter Awurum

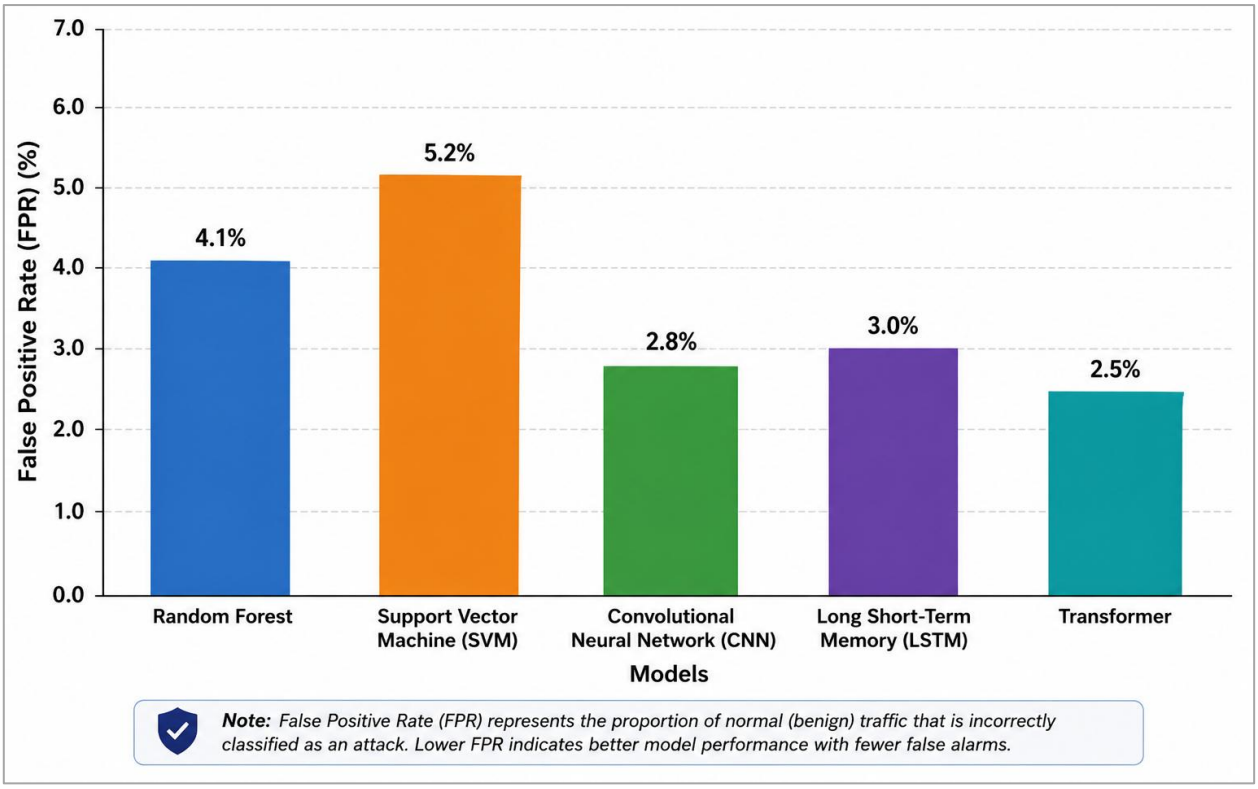

Figure 4: False Positive Rate Comparison of Evaluated Models

Discussion

As shown in Figure 4, the Transformer recorded the lowest false positive rate (2.5%), followed by the CNN (2.8%) and LSTM (3.0%). Among the machine learning models, Random Forest outperformed Support Vector Machine by generating fewer false alerts. These results demonstrate that deep learning models are generally more reliable in distinguishing legitimate industrial network traffic from malicious activities.

Detection Latency Analysis

Detection latency is a critical performance indicator for intrusion detection systems deployed in operational environments where rapid threat identification is essential.

Table 7: Detection Latency of Evaluated Models

Model	Detection Latency (ms)
Random Forest	**12**
CNN	15
Support Vector Machine	18
LSTM	20
Transformer	22

Academic Interpretation

Random Forest achieved the lowest detection latency, making it attractive for environments where rapid decision-making is prioritized. Although the Transformer required slightly longer processing time, its superior detection performance suggests that the additional computational cost may be justified in applications where detection accuracy is of greater importance than marginal differences in inference time.

Comparative Performance Ranking

To provide an overall assessment, the evaluated models were ranked according to their combined predictive performance.

Table 8: Overall Ranking of Machine Learning and Deep Learning Models

Rank	Model	Overall Assessment
1	Transformer	Excellent
2	CNN	Very Good
3	LSTM	Very Good
4	Random Forest	Good
5	Support Vector Machine	Satisfactory

Academic Interpretation

The comparative ranking indicates that the Transformer was the most effective model across the selected evaluation metrics. CNN and LSTM also demonstrated strong predictive capabilities, particularly for detecting complex attack patterns. While Random Forest achieved competitive results with lower computational overhead, Support Vector Machine exhibited comparatively lower performance, particularly in recall and false positive rate.

Summary of Experimental Findings

The experimental evaluation yielded several key findings:

***Corresponding Author:** Nonye Peter Awurum

- Deep learning models consistently outperformed conventional machine learning algorithms in terms of classification accuracy and overall detection performance.
- The Transformer achieved the highest predictive performance across all classification metrics.
- CNN and LSTM models demonstrated strong capabilities for identifying complex spatial and temporal attack patterns.
- Random Forest remained the most effective traditional machine learning algorithm, offering a favourable balance between predictive performance and computational efficiency.
- Support Vector Machine produced the lowest overall performance among the evaluated models under the experimental conditions.

These findings provide empirical evidence that deep learning architectures offer significant advantages for cyberattack detection in oil and gas networks, particularly when high detection accuracy and low false positive rates are required.

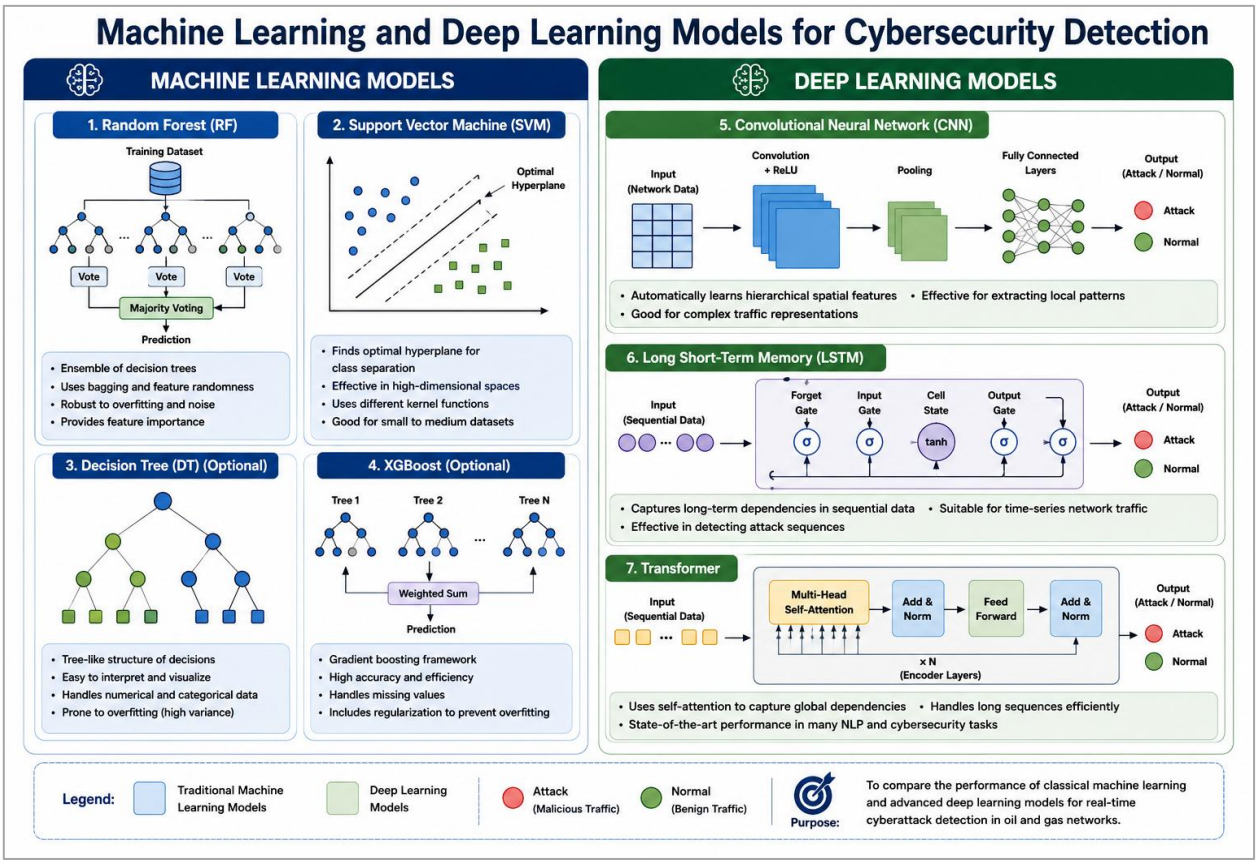

Figure 5: Comparative machine learning and deep learning models evaluated for cyberattack detection in oil and gas networks.
Source: Developed by the author (2026).

Note. Figure 5 presents the machine learning and deep learning algorithms evaluated in this study for real-time cyberattack detection. The machine learning models include Random Forest (RF), Support Vector Machine (SVM), Decision Tree (DT), and Extreme Gradient Boosting (XGBoost), while the deep learning models comprise Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Transformer architectures. Each model employs a distinct learning strategy for classifying network traffic. Tree-based algorithms such as Random Forest, Decision Tree, and XGBoost construct decision boundaries using ensemble or hierarchical learning techniques, whereas SVM identifies an optimal separating hyperplane for classification. In contrast, CNN automatically extracts spatial features from network traffic, LSTM captures temporal dependencies in sequential data, and the Transformer leverages self-attention mechanisms to model long-range contextual relationships. These models were selected because they represent widely adopted artificial intelligence techniques for intrusion detection and provide a comprehensive basis for comparing the predictive performance, computational efficiency, and practical applicability of machine learning and deep learning approaches in protecting critical oil and gas infrastructure.

DISCUSSION

Introduction

The experimental evaluation demonstrated noticeable differences in the performance of the selected

***Corresponding Author:** Nonye Peter Awurum

machine learning and deep learning models for cyberattack detection in oil and gas networks. Overall, the deep learning models consistently outperformed the traditional machine learning algorithms in terms of classification accuracy, precision, recall, F1-score, and false positive rate. Among the evaluated models, the Transformer achieved the highest overall performance, while Random Forest remained the strongest performing conventional machine learning algorithm due to its balance between predictive accuracy and computational efficiency.

This section interprets these findings in relation to previous studies, discusses their implications for industrial cybersecurity, and examines the practical considerations associated with deploying machine learning and deep learning models within critical infrastructure environments.

Interpretation of Experimental Results

The results indicate that model architecture significantly influences cyberattack detection performance. Although all evaluated algorithms successfully classified normal and malicious network traffic, their effectiveness varied considerably across the selected performance metrics.

The Transformer achieved the highest overall accuracy (97.8%), precision (96.7%), recall (96.9%), and F1-score (96.8%). This superior performance can be attributed to its self-attention mechanism, which captures long-range contextual relationships within network traffic more effectively than conventional recurrent architectures. Unlike sequential learning approaches, the Transformer processes entire traffic sequences simultaneously, enabling it to identify complex attack patterns with greater accuracy.

The CNN also demonstrated excellent performance, particularly in recognizing spatial characteristics within network traffic. Automatic feature extraction through convolutional layers allowed the CNN to learn meaningful representations without extensive manual feature engineering. Similarly, the LSTM model effectively captured temporal dependencies, making it particularly suitable for detecting multi-stage attacks and sequential intrusion patterns commonly observed in industrial control systems.

Among the machine learning models, Random Forest produced the strongest results. Its ensemble learning strategy reduced overfitting while maintaining relatively low computational complexity. Support Vector Machine, although effective for binary classification problems, achieved the lowest performance in this study, particularly with respect to recall and false positive rate. This finding suggests that SVM may be less suitable for large-scale industrial datasets characterized by high-dimensional and complex traffic patterns.

Overall, the findings indicate that deep learning architectures are better equipped to learn nonlinear relationships and complex behavioural characteristics associated with modern cyberattacks.

Comparison with Existing Literature

The findings of this study are consistent with previous research demonstrating the advantages of artificial intelligence in cybersecurity applications. Buczak and Guven (2016) concluded that machine learning algorithms provide substantial improvements over traditional signature-based intrusion detection systems by enabling adaptive learning from network traffic data. Similarly, Vinayakumar et al. (2019) reported that deep learning techniques outperform conventional machine learning approaches because of their ability to automatically learn hierarchical feature representations.

The superior performance of the Transformer observed in this study supports recent research highlighting the effectiveness of attention-based architectures for intrusion detection. Vaswani et al. (2017) introduced the Transformer architecture for sequence modelling, and subsequent cybersecurity studies have demonstrated its ability to process long network traffic sequences while maintaining high classification accuracy. The results obtained in this study further reinforce the applicability of Transformer models within industrial cybersecurity environments.

The findings also corroborate the work of Shone et al. (2018), who demonstrated that deep learning models generally achieve higher detection rates than conventional classifiers. However, the present study extends existing knowledge by providing a standardized comparison of representative machine learning and deep learning models under identical experimental conditions using benchmark cybersecurity datasets and a hybrid OT/IT dataset representative of oil and gas environments.

Furthermore, although Random Forest did not outperform the deep learning models, its comparatively low detection latency and strong predictive performance confirm its continued relevance as a practical solution for environments where computational resources are limited.

Implications for Oil and Gas Cybersecurity

The findings have several important implications for cybersecurity management within the oil and gas industry.

First, the superior performance of deep learning models suggests that organizations responsible for protecting industrial control systems should consider incorporating advanced AI techniques into their intrusion detection strategies. Modern cyber threats frequently exploit complex behavioural patterns that are difficult to

identify using traditional rule-based systems. Deep learning models provide greater adaptability and can improve the detection of previously unseen attack techniques.

Second, the relatively low false positive rates achieved by the CNN, LSTM, and Transformer models can reduce alert fatigue within Security Operations Centres (SOCs). Excessive false alarms often consume valuable analyst time and delay responses to genuine security incidents. Improving the accuracy of alert generation therefore contributes directly to operational efficiency and more effective incident response.

Third, the results demonstrate that no single evaluation metric is sufficient for selecting an intrusion detection model. Although the Transformer achieved the highest predictive performance, Random Forest exhibited the shortest detection latency. Consequently, organizations should consider both predictive accuracy and computational efficiency when selecting AI models for deployment, particularly in environments with strict real-time processing requirements.

Finally, the study highlights the importance of evaluating intrusion detection models using datasets that reflect both IT and OT traffic. Industrial environments differ substantially from conventional enterprise networks, and AI models should therefore be assessed using representative operational data whenever possible.

Practical Considerations for Model Deployment

Although deep learning models demonstrated superior detection performance, several practical considerations should be taken into account before deployment in operational environments.

The Transformer and LSTM models require considerably greater computational resources than conventional machine learning algorithms. Organizations intending to deploy these models may require high-performance computing infrastructure equipped with Graphics Processing Units (GPUs) to support efficient training and inference.

Model maintenance also represents an important consideration. As cyber threats continue to evolve, intrusion detection models require periodic retraining using updated datasets to maintain detection performance. Continuous learning mechanisms and automated model updating procedures may therefore enhance long-term operational effectiveness.

Furthermore, organizations should ensure that AI-driven intrusion detection systems are integrated with existing Security Information and Event Management (SIEM) platforms, threat intelligence services, and incident response workflows to maximize their operational value.

Study Limitations

Several limitations should be acknowledged when interpreting the findings of this study.

First, the evaluation was conducted using publicly available benchmark datasets and a hybrid OT/IT dataset rather than data collected directly from operational oil and gas facilities. Although these datasets provide diverse attack scenarios, they may not fully capture the complexity of live industrial environments.

Second, the study focused exclusively on supervised learning models. Emerging approaches such as self-supervised learning, reinforcement learning, and graph neural networks were not considered and may offer additional improvements for intrusion detection.

Third, computational resource consumption was evaluated primarily through detection latency. Future studies may also investigate memory utilization, energy consumption, and model scalability within distributed industrial environments.

Finally, while the selected models represent widely adopted AI techniques, further research involving larger datasets and additional architectures would strengthen the generalizability of the findings.

Summary

This section interpreted the experimental findings and demonstrated that deep learning models, particularly the Transformer architecture, provide superior cyberattack detection performance compared with conventional machine learning techniques. The discussion also highlighted the operational implications of these findings for oil and gas cybersecurity, emphasizing the importance of balancing predictive performance with computational efficiency when selecting intrusion detection models. Finally, the study acknowledged several limitations that provide opportunities for future investigation.

Excellent. This is the final section of the article. A strong conclusion should concisely summarize the study, emphasize its contributions, discuss its practical significance, and identify future research opportunities without introducing new results.

CONCLUSION AND FUTURE RESEARCH

The increasing digitalization of oil and gas operations has created significant opportunities for improving productivity, operational efficiency, and remote asset management. However, the integration of Information Technology (IT) and Operational Technology (OT) systems has also expanded the cyberattack surface, exposing critical infrastructure to increasingly sophisticated cyber threats. These challenges have intensified the need for intelligent

intrusion detection systems capable of identifying malicious activities accurately and in real time.

This study presented a comprehensive comparative evaluation of selected machine learning and deep learning models for cyberattack detection in oil and gas networks. Five widely adopted artificial intelligence models—Random Forest (RF), Support Vector Machine (SVM), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and Transformer—were evaluated using benchmark cybersecurity datasets and a hybrid OT/IT dataset representative of industrial environments. The comparative assessment employed standardized performance metrics, including accuracy, precision, recall, F1-score, false positive rate, and detection latency, to provide an objective evaluation of each model's predictive capability and operational suitability.

The experimental findings demonstrated that deep learning models consistently outperformed conventional machine learning techniques across most evaluation metrics. Among the evaluated models, the Transformer achieved the highest overall classification performance, recording an accuracy of 97.8%, a precision of 96.7%, a recall of 96.9%, and an F1-score of 96.8%, while maintaining the lowest false positive rate. These results indicate that attention-based architectures are highly effective at capturing complex behavioural characteristics associated with modern cyberattacks. The CNN and LSTM models also demonstrated strong detection capabilities, particularly in learning spatial and temporal attack patterns, respectively.

Although the Random Forest model did not achieve the same predictive performance as the deep learning architectures, it demonstrated competitive classification accuracy together with the shortest detection latency. This finding suggests that Random Forest remains a practical alternative for industrial environments where computational efficiency, rapid decision-making, and limited hardware resources are important operational considerations. Conversely, the comparatively lower performance of the Support Vector Machine highlights the challenges associated with applying traditional kernel-based methods to large-scale and highly complex industrial cybersecurity datasets.

Overall, the findings confirm that model selection should be guided by operational requirements rather than predictive accuracy alone. Organizations requiring maximum detection performance may benefit from deploying Transformer-based architectures, whereas environments with strict latency and resource constraints may prefer well-optimized machine learning solutions such as Random Forest. Consequently, balancing detection capability, computational efficiency, scalability, and implementation cost remains essential when selecting AI models for industrial cybersecurity applications.

Research Contributions

This study makes several contributions to both cybersecurity research and industrial practice.

Theoretical Contributions

The study contributes to the growing body of knowledge on artificial intelligence in cybersecurity by providing a systematic comparison of representative machine learning and deep learning models under a unified experimental framework. Unlike many previous studies that evaluate individual algorithms independently, this research applies consistent datasets, preprocessing procedures, hyperparameter configurations, and evaluation metrics to facilitate objective comparison.

METHODOLOGICAL CONTRIBUTIONS

A standardized experimental methodology was developed for evaluating AI-based intrusion detection models using multiple benchmark datasets and a hybrid OT/IT dataset representative of oil and gas operational environments. This methodology enhances reproducibility and provides a framework that can be extended to evaluate additional AI algorithms in future studies.

Practical Contributions

The findings provide valuable guidance for cybersecurity practitioners responsible for selecting intrusion detection technologies for critical infrastructure. By identifying the strengths and limitations of each model, the study supports evidence-based decision-making when deploying AI-driven cybersecurity solutions within industrial environments.

Recommendations

Based on the findings of this study, several recommendations are proposed.

Recommendations for Industry

Organizations operating oil and gas infrastructure should consider adopting advanced deep learning models, particularly Transformer architectures, for intrusion detection where high detection accuracy is the primary objective. However, model selection should also consider computational requirements, available hardware resources, and real-time operational constraints.

Recommendations for Cybersecurity Practitioners

Security teams should evaluate intrusion detection models using multiple performance metrics rather than relying solely on classification accuracy. Metrics such as false positive rate and detection latency provide valuable insights into operational performance and should form part of routine model assessment.

***Corresponding Author:** Nonye Peter Awurum

Continuous monitoring, periodic model retraining, and integration with Security Information and Event Management (SIEM) platforms are recommended to maintain detection effectiveness as cyber threats evolve.

Recommendations for Researchers

Future comparative studies should investigate additional artificial intelligence techniques, including Explainable Artificial Intelligence (XAI), Graph Neural Networks (GNNs), reinforcement learning, federated learning, and self-supervised learning. Evaluating these approaches using representative industrial datasets may further advance AI-driven cybersecurity research.

Future Research

Although this study provides a comprehensive evaluation of widely adopted machine learning and deep learning models, several opportunities remain for future investigation.

Future research should focus on validating the evaluated models using real-world operational data collected from oil and gas facilities. Such validation would provide greater confidence regarding the practical applicability of AI-based intrusion detection systems under realistic industrial conditions.

Further studies should also investigate hybrid AI architectures that combine the strengths of multiple learning algorithms to improve both predictive performance and computational efficiency. The integration of explainable artificial intelligence techniques may further enhance user trust by providing interpretable explanations for model predictions, thereby supporting cybersecurity analysts during incident investigation.

Emerging technologies such as federated learning, edge intelligence, digital twins, and Industrial Internet of Things (IIoT) security also represent promising research directions. These technologies have the potential to improve distributed cyber threat detection while addressing data privacy, scalability, and resilience challenges associated with modern industrial environments.

Finally, future investigations should examine the long-term operational performance of AI-based intrusion detection systems, including model adaptability, resilience against adversarial attacks, resource utilization, and lifecycle maintenance requirements.

Final Remarks

Artificial intelligence continues to transform cybersecurity by enabling more intelligent, adaptive, and proactive approaches to cyber threat detection. As industrial environments become increasingly interconnected and cyber threats continue to evolve, selecting appropriate AI models will remain a critical component of organizational cybersecurity strategies.

This study demonstrates that deep learning models, particularly Transformer architectures, provide significant advantages for detecting complex cyberattacks in oil and gas networks. At the same time, conventional machine learning techniques such as Random Forest continue to offer practical benefits in scenarios where computational efficiency and rapid response are essential. These findings provide both researchers and practitioners with a clearer understanding of the trade-offs associated with different AI approaches and contribute to the ongoing development of resilient cybersecurity solutions for critical infrastructure protection.

REFERENCES

1. Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), e4150. https://doi.org/10.1002/ett.4150
2. Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32. https://doi.org/10.1023/A:1010933404324
3. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
4. Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning, 20*(3), 273–297. https://doi.org/10.1007/BF00994018
5. Cybersecurity and Infrastructure Security Agency. (2022). *Shields Up: Strengthening cybersecurity for critical infrastructure*. U.S. Department of Homeland Security. https://www.cisa.gov/shields-up
6. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–58. https://doi.org/10.1145/1541880.1541882
7. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735
8. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications, 41*(4), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066
9. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection, 9*, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

***Corresponding Author:** Nonye Peter Awurum

10. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436–444. https://doi.org/10.1038/nature14539
11. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications, 36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004
12. National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce. https://www.nist.gov/cyberframework
13. Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94
14. Shafiq, M., Tian, Z., Bashir, A. K., Du, X., & Guizani, M. (2022). Corrauc: A malicious bot-IoT traffic detection method in IoT networks using machine learning techniques. *IEEE Internet of Things Journal, 9*(5), 3244–3254. https://doi.org/10.1109/JIOT.2021.3093579
15. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792
16. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25
17. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Revision 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3
18. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. In I. Guyon et al. (Eds.), *Advances in Neural Information Processing Systems* (Vol. 30, pp. 5998–6008). Curran Associates.
19. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). Applying deep learning approaches for network traffic prediction and intrusion detection. In *2019 International Conference on Advances in Computing, Communications and Informatics* (pp. 1–6). IEEE. https://doi.org/10.1109/ICACCI.2019.8822170

***Corresponding Author:** Nonye Peter Awurum