Cureus Journal of Computer Science
https://doi.org/10.7759/s44389-026-00076-0

Original Article

Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation

M. Agus Syamsul Arifin [1], Deris Stiawan [2, ✉], Susanto Susanto [3], Mohd Yazid Idris [4], Rahmat Budiarto [5]

1. *Informatics, Universitas Jenderal Soedirman, Banyumas, IDN*
2. *Computer System Engineering, Universitas Sriwijaya, Palembang, IDN*
3. *Information System, Universitas Pembangunan Nasional Veteran Jakarta, Jakarta, IDN*
4. *School of Computing, Universiti Teknologi Malaysia, Johor Bahru, MYS*
5. *Computer and Information Technology, Albaha University, Albaha, SAU*

Received: February 06, 2026 | Review began: February 23, 2026 | Review ended: April 15, 2026 | Published: May 15, 2026

Abstract

The increasing prevalence of cyber attacks targeting industrial control systems, particularly supervisory control and data acquisition (SCADA) networks based on the IEC 60870-5-104 protocol, necessitates the development of highly accurate and efficient intrusion detection systems. This study conducts a comprehensive comparative analysis of deep learning models, including Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Bidirectional LSTM, Convolutional Neural Networks (CNN)-LSTM, CNN-BiLSTM, LSTM-GRU, CNN-LSTM-GRU, and CNN-BiLSTM-GRU, to detect diverse network attacks in SCADA environments. The dataset used in this research was generated from a realistic SCADA IEC 60870-5-104 testbed and contains both benign traffic and multiple attack types, including bruteforce, Internet Control Message Protocol flood, IEC104 flood, port scan, SYN flood, and XMAS flood. Each model was trained and evaluated using a sequence-based learning approach, with performance assessed through accuracy, loss, precision, recall, and F1-score for both training and testing datasets. Confusion matrices were utilized to visualize classification performance per class, while training and validation curves provided insights into model convergence and generalization capabilities. The results demonstrate that sequence-based models, particularly BiLSTM and LSTM-GRU, achieve the highest and most consistent performance across all metrics, with near-perfect detection rates for most attack classes. In contrast, CNN-based hybrids exhibited reduced performance for certain attack types, such as Internet Control Message Protocol flood, despite maintaining high accuracy on others. These findings highlight the effectiveness of pure sequence-based deep learning architectures for intrusion detection in SCADA IEC 60870-5-104 networks and provide practical insights into selecting optimal intrusion detection system models for industrial control system cybersecurity.

Categories: Network Security, Cyber-Physical Systems, Deep Learning

Keywords: scada iec 60870-5-104, industrial control systems security, intrusion detection system (ids), hybrid deep learning, sequence modelling

How to cite this article:
Arifin M, Stiawan D, Susanto S, et al. (May 15, 2026) Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation. Cureus J Comput Sci 3 : es44389-026-00076-0. DOI https://doi.org/10.7759/s44389-026-00076-0

Introduction

Traditional supervisory control and data acquisition (SCADA) systems were originally designed to operate in isolated environments using closed networks [1,2], which limited exposure to external cyber threats. However, with the advancement of industrial automation, modern SCADA systems are increasingly integrated with external networks and communicate using standard protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP) [3,4]. While this integration improves operational efficiency and reduces monitoring and maintenance costs, it also significantly expands the attack surface and introduces new security vulnerabilities [5,6]. SCADA systems play a critical role in industrial control environments, including power grids, water treatment facilities, and transportation infrastructures, where reliability and real-time operation are essential. Cyberattacks targeting these systems can result in severe consequences, such as operational disruptions, financial losses, and safety hazards. In particular, modern SCADA protocols such as IEC 60870-5-104 (IEC 104) are widely deployed over TCP/IP networks to enable communication between control centers and substations [7,8]. The increasing complexity of SCADA communication and its exposure to network-based threats necessitate the deployment of effective intrusion detection systems (IDS). However, malicious activities in SCADA networks often mimic legitimate communication patterns, making detection particularly challenging. Conventional IDS designed for traditional IT networks are therefore insufficient for SCADA environments due to differences in protocol behavior, traffic characteristics, and real-time constraints. Accordingly, this study focuses on developing an intrusion detection approach based on machine learning to identify malicious activities in SCADA IEC 60870-5-104 networks.

In this study, we focus on intrusion detection in SCADA networks using the IEC 60870-5-104 protocol. We investigate the effectiveness of sequence-based deep learning models in detecting malicious activities within SCADA communication traffic. Recent advancements in machine learning and deep learning have demonstrated strong capabilities in intrusion detection, particularly in modeling complex and high-dimensional data. Sequence-based architectures, such as Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), are especially suitable for capturing temporal dependencies in network traffic, which is essential in SCADA environments where communication follows structured and time-dependent patterns. To explore the impact of different architectural designs, this study evaluates both standalone and hybrid deep learning models. Specifically, recurrent models such as LSTM and Bidirectional LSTM (BiLSTM) are combined with convolutional and gated mechanisms, including Convolutional Neural Networks (CNN) and GRU, to form hybrid architectures. In total, eight model configurations are examined, namely LSTM, LSTM-GRU, CNN-LSTM, CNN-LSTM-GRU, BiLSTM, BiLSTM-GRU, CNN-BiLSTM, and CNN-BiLSTM-GRU. The evaluation is conducted using a SCADA IEC 60870-5-104 dataset generated from a testbed environment designed to reflect realistic industrial network conditions [9]. The dataset includes both normal traffic and multiple categories of cyberattacks, such as brute force, Internet Control Message Protocol (ICMP) flood, IEC 104 flood, port scanning, SYN flood, and XMAS flood, enabling a comprehensive assessment of model performance in multi-class intrusion detection scenarios. This study makes the following contributions:

1. This study provides a comprehensive comparison of eight deep learning and hybrid architectures under consistent experimental conditions for intrusion detection in SCADA IEC 60870-5-104 networks.

2. This study applies sequence-based deep learning models to capture temporal dependencies in SCADA communication traffic.

3. This study utilizes a realistic SCADA IEC 60870-5-104 dataset generated from a testbed environment reflecting real-world industrial conditions.

4. This study performs a detailed multi-class evaluation of intrusion detection performance across various SCADA-specific attack scenarios.

Materials And Methods

Background and related work

SCADA IEC 60870-5-104 Protocol

How to cite this article:
Arifin M, Stiawan D, Susanto S, et al. (May 15, 2026) Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation. Cureus J Comput Sci 3 : es44389-026-00076-0. DOI https://doi.org/10.7759/s44389-026-00076-0

The IEC 60870-5-101 (IEC 101) standard has been modified to IEC 104 in order to operate on TCP/IP network for controlling and monitoring critical infrastructure through a more flexible network [10-12]. The IEC established IEC 104 to deliver IEC 101 packet data over the TCP protocol [13]. The IEC 101 packet has been encapsulated to IEC 104 application protocol data unit (APDU) and then delivered using TCP protocol. The application protocol control information (APCI) and application service data unit are part of APDU. The APDU may contain APCI only or APCI with application service data unit [13]. In SCADA IEC 104 protocol, there are three types of APCI frame formats, which are I (Information instruction), U (Unnumbered control frame), and S (Supervisory format) [14].

Malicious Activity on SCADA Network

The opening of external connections on the SCADA network led to many cyberattacks on the SCADA system, including command injection [15]. Industrial control systems face persistent challenges in detecting malicious activities. While network traffic monitoring schemes are commonly employed, they can be fooled by anomalies that closely resemble normal system behavior, leading to ineffective anomaly detection [16]. Research conducted by Radoglou-Grammatikis et al. [7] simulates cyberattacks on SCADA networks by carrying out several attack scenarios on SCADA IEC 104 networks. Research conducted by Hareesh et al. [10] investigates attacks against a protocol used for clock synchronization called network time protocol. Network time protocol on the SCADA system can be manipulated to get time stamps to affect control loops and processes in SCADA.2.1.3. IDS on SCADA network.

IDS in SCADA networks can be broadly categorized into host-based and network-based approaches. Host-based IDS monitors and analyzes event logs from individual devices to detect suspicious activities [17,18], whereas network-based IDS inspects traffic flowing across the network to identify potential threats [19].

Traditional IDS approaches in SCADA environments are generally classified into signature-based and anomaly-based methods. Signature-based IDS relies on predefined rules or known attack patterns to detect malicious activity [20]. For example, Radoglou-Grammatikis et al. [13] proposed a whitelist-based approach to filter suspicious packets in SCADA IEC 60870-5-104 networks, while Asad and Gashi [21] compared signature-based IDS tools such as Snort and Suricata for detecting malicious traffic. However, these approaches are limited in their ability to detect unknown or evolving attacks.

To address these limitations, anomaly-based IDS leveraging machine learning techniques have been widely explored [22,23]. Conventional machine learning algorithms, such as Decision Trees, Support Vector Machines, and Naïve Bayes, have demonstrated promising performance in distinguishing between normal and malicious traffic [24]. Nevertheless, these methods often struggle to capture complex and temporal dependencies in network behavior, which are critical in SCADA systems.

Recent studies have increasingly focused on applying machine learning techniques to SCADA-specific environments. For instance, Grammatikis et al. [25] investigated anomaly detection using One-Class Support Vector Machines, Local Outlier Factor, and Isolation Forest on IEC 60870-5-104 communication data. While their approach enables detection without labeled attack data, it is limited to binary classification and does not provide detailed insights into specific attack types. Similarly, Egger et al. [26] conducted a comparative study of supervised, semi-supervised, and unsupervised methods for intrusion detection. However, their work primarily focuses on general network traffic and does not explicitly model SCADA-specific communication characteristics or temporal dependencies.

More recently, advances in deep learning have introduced sequence-based models, such as LSTM [27] and GRU [28], which are capable of capturing temporal dependencies in sequential data. These models are particularly suitable for SCADA systems, where communication patterns are inherently time-dependent. In addition, hybrid architectures that combine CNN with recurrent models have been proposed to enhance feature extraction and improve detection performance.

Despite these advancements, several challenges remain in the development of IDS for SCADA systems. Many existing studies rely on binary classification, limiting their ability to distinguish between different attack types. Additionally, the use of generalized or non-SCADA datasets reduces the applicability of these models to real-world industrial environments. Furthermore, there is still a lack of comprehensive evaluations comparing multiple deep learning

architectures under consistent experimental settings. These limitations highlight the need for more systematic and SCADA-specific investigations, which motivates the approach adopted in this study. Table *1* presents a comparison between the proposed work and previous studies on IDS in SCADA systems.

How to cite this article:
Arifin M, Stiawan D, Susanto S, et al. (May 15, 2026) Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation. Cureus J Comput Sci 3 : es44389-026-00076-0. DOI https://doi.org/10.7759/s44389-026-00076-0

Reference	Threats	Method	Number of class	Pros and cons
Grammatikis et al. [25]	Anomaly	OS-SVM, LOF, Isolation Forest	2-Class (Normal and Attack)	Low dimension, but TPR and F1-score should still be able to be improved, and no discussion of attack patterns.
Egger et al. [26]	Port scan, DoS	Supervised, Semi-Supervised, Unsupervised	2-Class (Normal and Attack)	Provides a comprehensive comparison of methods for building an IDS, but no discussion of attack patterns.
Arifin et al. [29]	DoS	DT, GNB, SVM	2-Class (Normal and Attack)	The performance of the IDS model is good; there is a discussion of DoS attack patterns on SCADA networks, but there are no specific attacks for SCADA IEC 104.
Arifin et al. [30]	DoS, Port Scan, and Brutefore	GB, DT, RF	7-class (Multi-class)	In this study, data balancing techniques were employed due to the imbalanced class distribution in the dataset, resulting in very good performance for the evaluated machine learning models. However, since the data used was synthetic as a result of oversampling and SMOTE, there is an indication that the models' performance may be less accurate. Furthermore, with the undersampling technique, there is a possibility of losing important features that represent key attack patterns.

Balla et al. [31]	Anomaly	CNN-LSTM	2-Class (Normal and Attack)	This study achieved good model performance using CNN-LSTM, with an accuracy of up to 95%. However, the dataset used was based on general computer network traffic, which does not fully reflect the real conditions of a SCADA network.
Hamdi [32]	MiTM, DoS, and Spoofing	HL and FLMC	7-Class (Multi-class)	This study compares the HL method with its federated counterpart (FLMC) model. The HL method achieved higher accuracy than FLMC, reaching 90% when testing the model on each client. However, this performance is still insufficient for an IDS model in SCADA systems, where modern attacks occur more rapidly and pose greater threats.
Our work (2026)	DoS, Port Scan, and Bruteforce	LSTM, LSTM-GRU, CNN-LSTM CNN-LSTM-GRU, BiLSTM, BiLSTM-GRU, CNN-BiLSTM CNN-BiLSTM-GRU	7-Class (Multi-class)	Our study comprehensively compares eight hybrid deep learning methods to identify the most effective model for detecting attacks in SCADA networks using the IEC 104 protocol. The performance of each algorithm was measured in detail to produce a model that is truly relevant for IDS deployment in SCADA IEC 104 environments.

TABLE 1: Comparison with other works

BiLSTM, Bidirectional Long Short-Term Memory; CNN, Convolutional Neural Network; DT, Decision Tree; GB, Gradient Boosting; GNB, Gaussian Naive Bayes; GRU, Gated Recurrent Unit; HL, Hybrid Learning; IDS, Intrusion Detection System; LSTM, Long Short-Term Memory; LOF, Local Outlier Factor; OS-SVM, One-Class Support Vector Machine; RF, Random Forest; SCADA, Supervisory Control and Data Acquisition; SMOTE, Synthetic Minority Over-sampling Technique; SVM, Support Vector Machine; TPR, True Positive Rate

Table *1* illustrates several limitations in existing research on intrusion detection for SCADA systems. First, many prior studies rely on binary classification (normal vs attack), which limits the ability to distinguish between different types of cyberattacks. Second, a number of studies utilize generalized or non-SCADA datasets, reducing their applicability to real-world SCADA IEC 60870-5-104 environments. Third, although some works have explored hybrid and deep learning approaches, there is still a lack of comprehensive comparisons across multiple architectures under consistent experimental conditions. In addition, limited attention has been given to modeling temporal dependencies in SCADA communication traffic.

Despite these advancements, existing studies remain constrained by the use of generalized datasets, binary classification approaches, and insufficient modeling of temporal dependencies. Therefore, this study addresses these gaps by utilizing a realistic SCADA IEC 60870-5-104 dataset and conducting a systematic multi-class evaluation of eight sequence-based and hybrid deep learning architectures. This approach provides a more rigorous foundation for developing IDS that are not only accurate but also aligned with the operational characteristics of modern SCADA systems.

Design and method

Proposed Method

The experimental evaluation employs a SCADA intrusion detection dataset specifically developed for the IEC 60870-5-104 protocol [9], which is widely used in electric power grid control systems. The captured traffic reflects realistic protocol behavior, including supervisory control messages, telemetry exchanges, and control commands. The dataset represents network communication within a simulated industrial control environment and includes both normal operational traffic and multiple categories of cyberattacks targeting SCADA communication such as bruteforce, SYN flood, ICMP flood, XMAS flood, IEC104 flood, and port scan attacks. The SCADA-specific characteristics of the dataset make it particularly suitable for evaluating sequence-aware models, as temporal dependencies in industrial communication differ significantly from conventional IT network traffic.

Following the data acquisition phase, a series of pre-processing steps were applied to ensure the dataset's suitability for deep learning. These steps involved feature extraction and selection, data labeling, and the application of sequence-based techniques. The latter was considered particularly important, as SCADA traffic inherently exhibits temporal dependencies that sequence-aware learning models can effectively exploit. After pre-processing, the dataset contained a total of 1,048,564 records. To facilitate model training and evaluation, the dataset was divided into training and testing subsets using a 70:30 ratio, resulting in 733,994 records for training and 314,570 records for testing. This split ratio was chosen based on established practices in machine learning research, balancing the need for robust model training with reliable performance evaluation.

The overall methodological workflow, encompassing data generation, pre-processing, and preparation for model training and evaluation, is illustrated in Figure *1*.

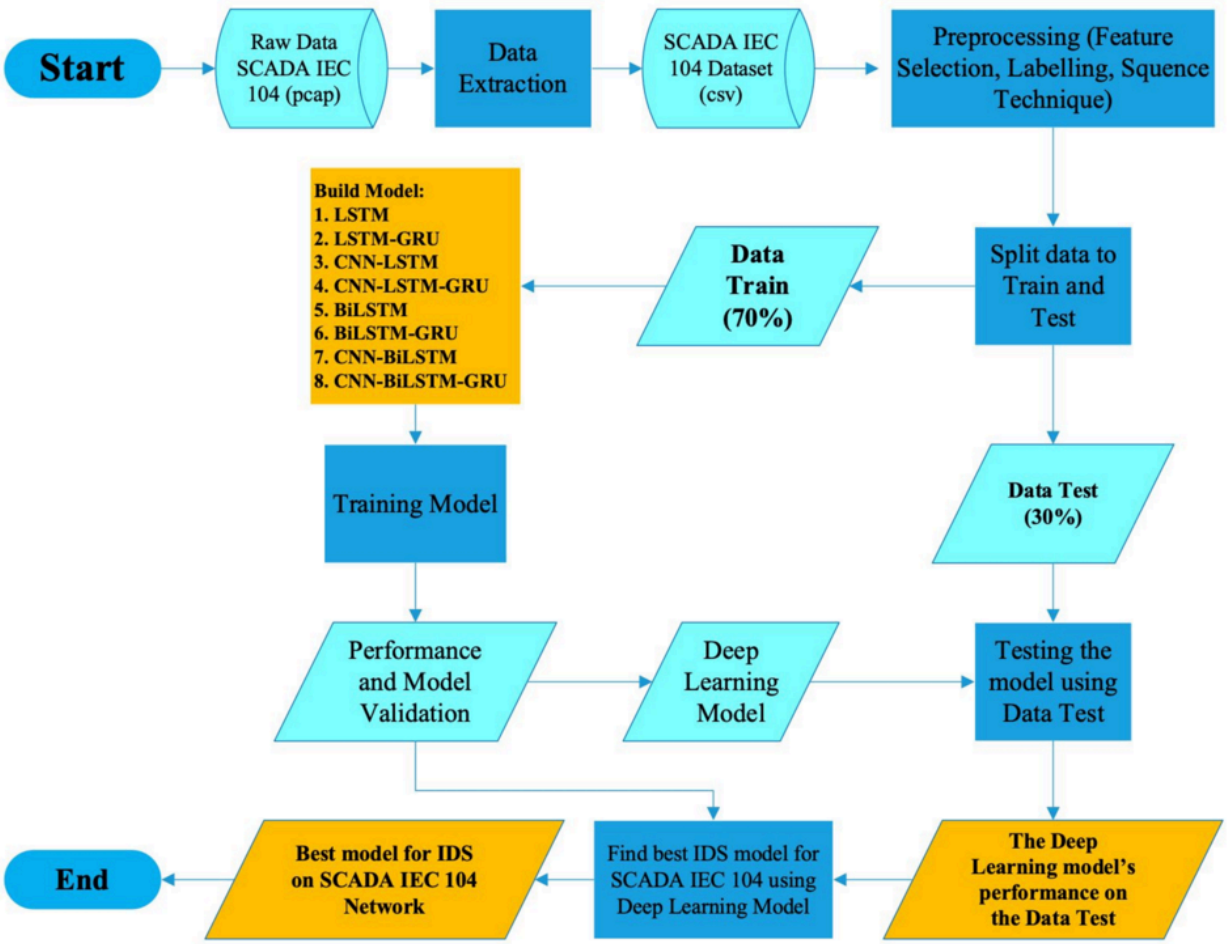

FIGURE 1: Proposed method to find the best algorithm for the IDS model

BiLSTM, Bidirectional Long Short-Term Memory; CNN, Convolutional Neural Network; GRU, Gated Recurrent Unit; IDS, Intrusion Detection System; LSTM, Long Short-Term Memory; SCADA, Supervisory Control and Data Acquisition

Temporal Sequence Construction

Since SCADA network communication exhibits time-dependent behavior [33-35], a sliding window approach was employed to construct sequential inputs for the deep learning models [36-38]. In this approach, consecutive records were grouped into fixed-length sequences to preserve temporal context. Let T denote the predefined sequence length. For each window, T consecutive observations were aggregated to form a single sequence sample, and the window was shifted step-by-step across the dataset to generate overlapping sequences. As a result, the dataset was transformed from a two-dimensional tabular structure into a three-dimensional tensor representation:

$$InputShape = (N, T, F)$$

where N represents the number of generated sequences, T denotes the sequence length (number of time steps), and F corresponds to the number of input features.

This transformation enables the recurrent and hybrid deep learning architectures to model temporal dependencies in IEC 60870-5-104 traffic, allowing the networks to learn evolving communication patterns rather than isolated packet characteristics.

Hybrid Deep Learning Model

Research on hybrid deep learning models for IDS has been widely explored in recent years. Several studies have employed CNN-LSTM architectures to detect malicious activities in network environments, demonstrating strong performance in capturing both spatial and temporal features [31,39,40]. Similar approaches have also been applied in IoT and critical infrastructure networks, showing promising detection capabilities under complex traffic conditions [41,42].

In addition, CNN-BiLSTM-based models have been investigated to further enhance temporal feature representation through bidirectional sequence learning [43-45]. Hybrid architectures combining GRU and BiLSTM have also been proposed to improve detection accuracy while maintaining computational efficiency, particularly in IoT environments [28,46]. Other variants, such as transfer learning-based BiLSTM (TL-BiLSTM), have demonstrated effectiveness in improving model generalization across different network scenarios [47].

More complex hybrid architectures integrating CNN, LSTM, and GRU have also been developed for intrusion detection tasks. For instance, a study in [48] reported high performance using combined deep learning models on benchmark datasets such as TON_IoT and CICIDS2017, achieving up to 100% accuracy for binary classification and 97% for multi-class classification. Similar hybrid approaches have also been applied in IoT-based electric vehicle charging station networks and other network environments, further confirming the effectiveness of multi-architecture deep learning models in intrusion detection [49,50].

Despite these advancements, most existing studies focus on general-purpose or IoT-based datasets, with limited attention to SCADA specific communication protocols such as IEC 60870-5-104. Moreover, comprehensive comparisons across multiple hybrid architectures under consistent experimental conditions remain scarce.

Therefore, this study conducts a systematic comparative analysis of eight deep learning and hybrid architectures using a realistic SCADA IEC 60870-5-104 dataset. The complete framework of the proposed models is presented in Figure *2*.

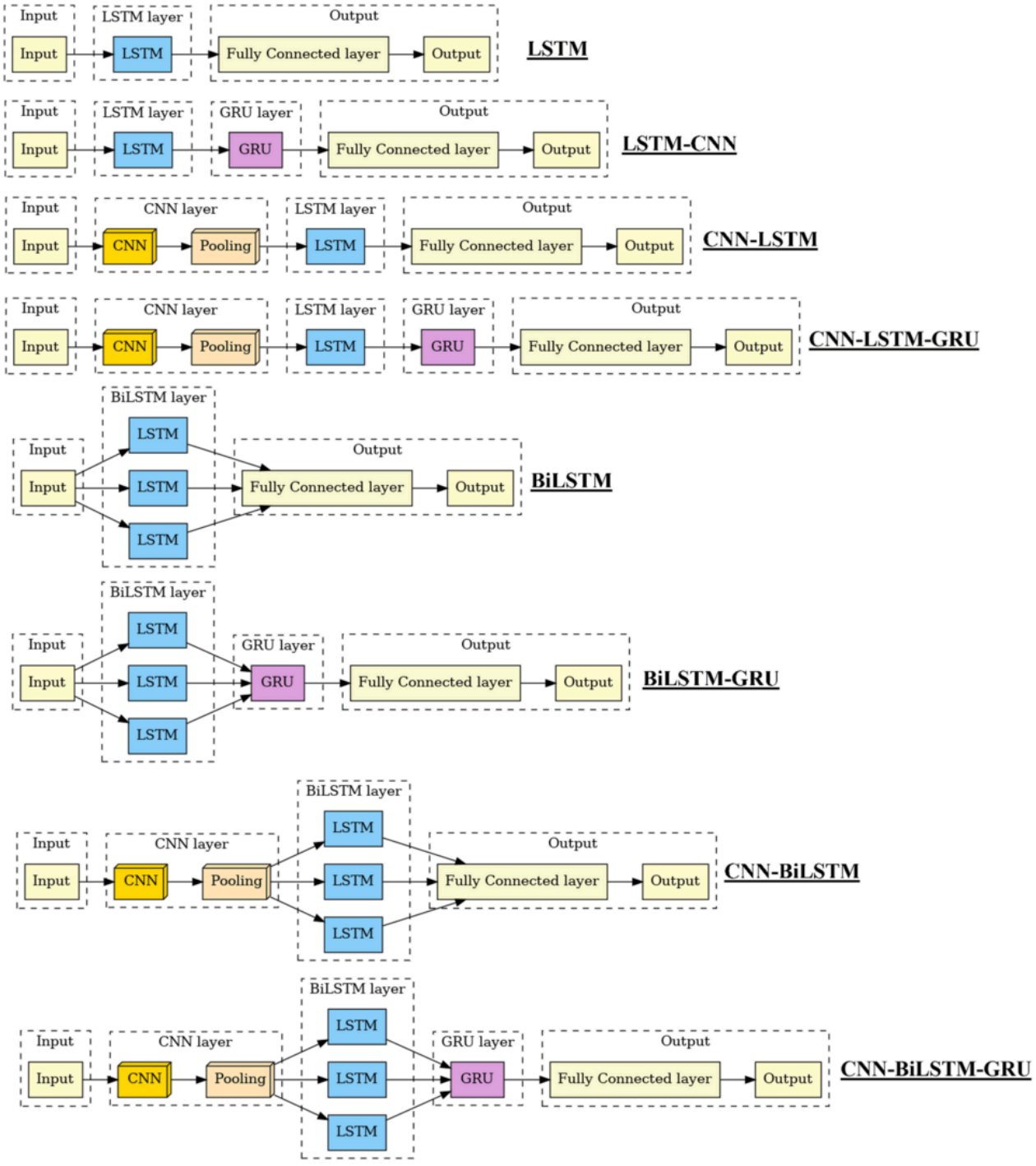

FIGURE 2: Framework structure of each evaluated model

BiLSTM, Bidirectional Long Short-Term Memory; CNN, Convolutional Neural Network; GRU, Gated Recurrent Unit; LSTM, Long Short-Term Memory

All proposed models are implemented using the Sequential API in TensorFlow/Keras and operate on three-dimensional input tensors with the shape (samples,timesteps,features)(samples, timesteps, features)(samples,timesteps,features), where the timesteps and feature dimensions correspond to the preprocessed SCADA IEC 60870-5-104 traffic sequences.

The recurrent-based architectures employ LSTM layers with 128 hidden units as the primary temporal feature extractor, followed in certain configurations by either an additional LSTM layer with 64 units or a GRU layer with 64 units. For bidirectional models, a bidirectional wrapper is applied to the LSTM layer with 128 units to capture forward and backward temporal dependencies. In hybrid configurations, a one-dimensional convolutional layer with 64 filters and a kernel size of 3 is applied prior to recurrent layers to extract local feature patterns, followed by a MaxPooling1D layer to reduce sequence dimensionality.

Across all models, Dropout layers with a rate of 0.3 are inserted after convolutional and recurrent layers to reduce overfitting. Each architecture includes a fully connected Dense layer with 32 neurons and ReLU activation before the final output layer. The classification layer consists of a Dense layer with a Softmax activation function, where the number of output neurons corresponds to the number of traffic classes in the dataset.

All models are compiled using the categorical cross-entropy loss function and optimized with the Adam optimizer. Model performance is evaluated using accuracy as the primary metric. For training consistency and fair comparison, all architectures are trained under identical experimental settings with 50 epochs, a batch size of 64, and a validation split of 0.2 applied to the training data.

The first model evaluated in this study is the LSTM architecture. This model utilizes stacked LSTM layers to capture long-term temporal dependencies in IEC 104 traffic sequences. The first LSTM layer processes the sequential input and retains the temporal structure, while the subsequent LSTM layer further abstracts higher-level temporal representations. The extracted features are then passed to a fully connected layer before being classified through the output layer. The use of LSTM enables the model to preserve relevant historical information while mitigating the vanishing gradient problem. The second architecture is the LSTM-GRU model, which combines the memory capability of LSTM with the computational efficiency of GRU. In this configuration, the LSTM layer first extracts temporal features from the input sequence. The resulting sequence representation is then refined by a GRU layer, which applies gating mechanisms to selectively retain important information while reducing parameter complexity. The final representation is forwarded to a fully connected layer for classification. Since the GRU configuration is consistent across models, it maintains the same gating structure and hidden unit size to ensure fair comparison. The third model is the CNN-LSTM architecture. In this hybrid configuration, a one-dimensional convolutional layer is first applied to extract local spatial patterns from the input sequence, particularly short-term correlations between adjacent features. A pooling layer is used to reduce dimensionality and computational complexity. The resulting feature maps are then processed by the LSTM layer to capture longer temporal dependencies before being classified by the fully connected and output layers. The CNN configuration used in this study remains consistent across all hybrid CNN-based models to maintain experimental fairness.

The fourth model, CNN-LSTM-GRU, extends the previous architecture by introducing a GRU layer after the LSTM layer. In this structure, the CNN extracts spatial features, the LSTM models intermediate temporal relationships, and the GRU further refines the sequential representation before final classification. This stacked hybrid design aims to improve representational depth while maintaining computational efficiency. The fifth architecture is the BiLSTM model, which employs bidirectional LSTM layers to process the sequence in both forward and backward directions. Unlike standard LSTM, BiLSTM can capture contextual information from past and future time steps simultaneously, providing richer sequence representation. The bidirectional outputs are combined and then forwarded to the fully connected layer for classification. The internal LSTM configuration in the BiLSTM models is kept consistent with that of the unidirectional LSTM to ensure comparability. The sixth model is the BiLSTM-GRU architecture. In this design, the bidirectional LSTM first extracts forward and backward temporal features, which are subsequently refined by a GRU layer. The GRU layer consolidates the bidirectional representations and reduces redundancy before classification. As in the previous models, the GRU configuration remains identical to maintain controlled experimental conditions. The seventh model, CNN-BiLSTM, integrates convolutional feature extraction with bidirectional temporal modeling. The CNN and pooling layers capture local traffic characteristics, which are then processed by the BiLSTM layer to learn bidirectional sequence dependencies. The resulting representation is passed through a fully connected layer to generate the final classification output.

Finally, the CNN-BiLSTM-GRU architecture combines convolutional feature extraction with bidirectional and gated recurrent layers. The CNN extracts local feature patterns, the BiLSTM captures forward and backward temporal dependencies, and the GRU consolidates the sequential representation prior to classification. Overall, the eight evaluated architectures were implemented under the same experimental conditions to enable a systematic comparison of recurrent and convolutional-recurrent deep learning approaches for intrusion detection in SCADA IEC 60870-5-104 networks.

Results And Discussion

IDS models performance and validation

All experiments were conducted on a workstation equipped with an Intel Core i7-9750H processor, 64 GB DDR4 RAM, and an NVIDIA GeForce GTX 1660 Ti GPU (6 GB) running Ubuntu Linux. The models were implemented using Python with the TensorFlow framework and Keras API. The dataset was split into 70% training data and 30% testing data. From the training portion, 20% was allocated for validation during model training. All architectures were trained under identical conditions to ensure fair comparison, using 50 epochs, a batch size of 64, the Adam optimizer, and categorical cross-entropy as the loss function. Accuracy was used as the primary evaluation metric during training.

The experimental results are summarized through multiple tables and figures to comprehensively evaluate model performance. Table *2* presents the training and testing accuracy, loss, and total training time for 50 epochs, highlighting the trade-offs between predictive performance and computational cost for each architecture. Table *3* details the precision, recall, and F1-score for each attack class and the benign class across all evaluated models on both training and testing datasets, providing a fine-grained view of classification effectiveness for specific SCADA IEC 60870-5-104 attack types.

How to cite this article:
Arifin M, Stiawan D, Susanto S, et al. (May 15, 2026) Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation. Cureus J Comput Sci 3 : es44389-026-00076-0. DOI https://doi.org/10.7759/s44389-026-00076-0

Models	Accuracy (%)		Loss (%)		Training time (50 epochs) (minutes)
	Train	Test	Train	Test	
LSTM	99.96	99.92	0.18	0.34	170
LSTM-GRU	99.95	99.93	0.20	0.32	173
CNN-LSTM	98.49	98.45	0.25	0.26	36
CNN-LSTM-GRU	98.45	98.39	0.26	0.28	68
BiLSTM	99.97	99.93	0.17	0.37	171
BiLSTM-GRU	99.94	99.92	0.24	0.35	221
CNN-BiLSTM	98.46	98.35	0.24	0.27	135
CNN-BiLSTM-GRU	98.51	98.47	0.24	0.26	124

TABLE 2: Comparison of IDS models' accuracy and loss

BiLSTM, Bidirectional Long Short-Term Memory; CNN, Convolutional Neural Network; GRU, Gated Recurrent Unit; IDS, Intrusion Detection System; LSTM, Long Short-Term Memory

How to cite this article:
Arifin M, Stiawan D, Susanto S, et al. (May 15, 2026) Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation. Cureus J Comput Sci 3 : es44389-026-00076-0. DOI https://doi.org/10.7759/s44389-026-00076-0

Models	Class	Train (%)			Test (%)		
		Precision	Recall	F1-Score	Precision	Recall	F1-Score
LSTM	bf	99.15	98.45	98.88	98.38	98.19	98.28
	icmpf	100	100	100	100	100	100
	iec104f	100	100	100	100	100	100
	normal	99.95	99.96	99.95	99.93	99.93	99.93
	ps	99.81	99.84	99.83	99.68	99.69	99.68
	synf	99.99	99.98	99.99	99.99	99.98	99.98
	xmas	100	100	100	100	100	100
LSTM-GRU	bf	98.50	99.84	99.16	97.55	99.12	98.33
	icmpf	100	100	100	100	100	100
	iec104f	100	100	100	100	100	100
	normal	99.97	99.9	99.95	99.96	99.91	99.94
	ps	99.72	99.84	99.79	99.59	99.75	99.67
	synf	99.99	99.99	99.99	99.99	99.99	99.99
	xmas	100	100	100	100	100	100
CNN-LSTM	bf	95.38	90.25	92.75	95.40	90.31	92.78
	icmpf	69.82	100	82.23	69.87	99.99	82.26
	iec104f	99.99	99.98	99.99	99.97	99.92	99.95
	normal	99.88	97.41	99.88	99.85	97.36	98.59
	ps	98.68	99.35	99.01	98.47	99.29	98.88
	synf	99.76	99.96	99.86	99.71	99.93	99.82
	xmas	100	100	100	100	100	100
CNN-LSTM-GRU	bf	98.44	83.84	90.55	97.99	81.67	89.09
	icmpf	69.74	99.99	82.17	69.76	99.99	82.19

	iec104f	99.98	99.99	99.99	99.97	99.95	99.96
	normal	99.84	97.39	98.59	99.80	97.32	98.54
	ps	98.88	99.35	99.11	98.57	99.19	98.88
	synf	99.62	99.99	99.80	99.54	99.97	99.76
	xmas	99.99	100	99.99	99.96	100	99.98
BiLSTM	bf	99.73	98.59	99.16	99.25	98.01	98.62
	icmpf	100	100	100	100	100	100
	iec104f	100	100	100	100	100	100
	normal	99.96	99.98	99.97	99.92	99.96	99.94
	ps	99.90	99.86	99.88	99.76	99.65	99.70
	synf	99.99	99.99	99.99	99.99	99.99	99.99
	xmas	100	100	100	100	100	100
BiLSTM-GRU	bf	98.99	97.09	98.04	98.36	97.02	97.69
	icmpf	99.99	100	99.99	100	99.98	99.99
	iec104f	100	100	100	100	100	100
	normal	99.94	99.95	99.95	99.92	99.94	99.92
	ps	99.78	99.78	99.78	99.72	99.65	99.69
	synf	99.99	99.99	99.99	99.99	99.99	99.99
	xmas	100	100	100	100	100	100
CNN-BiLSTM	bf	94.72	91.77	93.22	94.17	88.25	91.11
	icmpf	1.000000	54.33	70.41	100	53.84	69.99
	iec104f	99.94	99.97	99.96	99.95	99.95	99.95
	normal	97.50	99.78	98.63	97.43	99.69	98.54
	ps	98.99	99.39	99.19	98.42	99.24	98.83
	synf	99.82	99.93	99.87	99.77	99.87	99.82
	xmas	100	100	100	100	100	100

CNN-BiLSTM-GRU	bf	97.55	92.25	94.83	96.50	90.93	93.63
	icmpf	69.77	100	82.19	69.80	99.99	82.22
	iec104f	99.91	99.99	99.95	99.95	99.99	99.97
	normal	99.73	97.56	98.64	99.71	97.52	98.60
	ps	99.04	99.33	99.18	98.77	99.16	98.96
	synf	99.97	99.71	99.84	99.96	99.72	99.84
	xmas	100	100	100	99.98	100	99.99

TABLE 3: The performance comparison

BiLSTM, Bidirectional Long Short-Term Memory; CNN, Convolutional Neural Network; GRU, Gated Recurrent Unit; LSTM, Long Short-Term Memory

Figure *3* illustrates the confusion matrix for the training datasets, while Figure *4* shows the confusion matrix for the test datasets, offering visual insights into correct and incorrect predictions as well as model generalization capability. Finally, Figure *5* depicts the accuracy and loss curves over 50 epochs for both training and validation sets, revealing the convergence patterns, stability, and potential overfitting or underfitting behaviors of the evaluated deep learning and hybrid models.

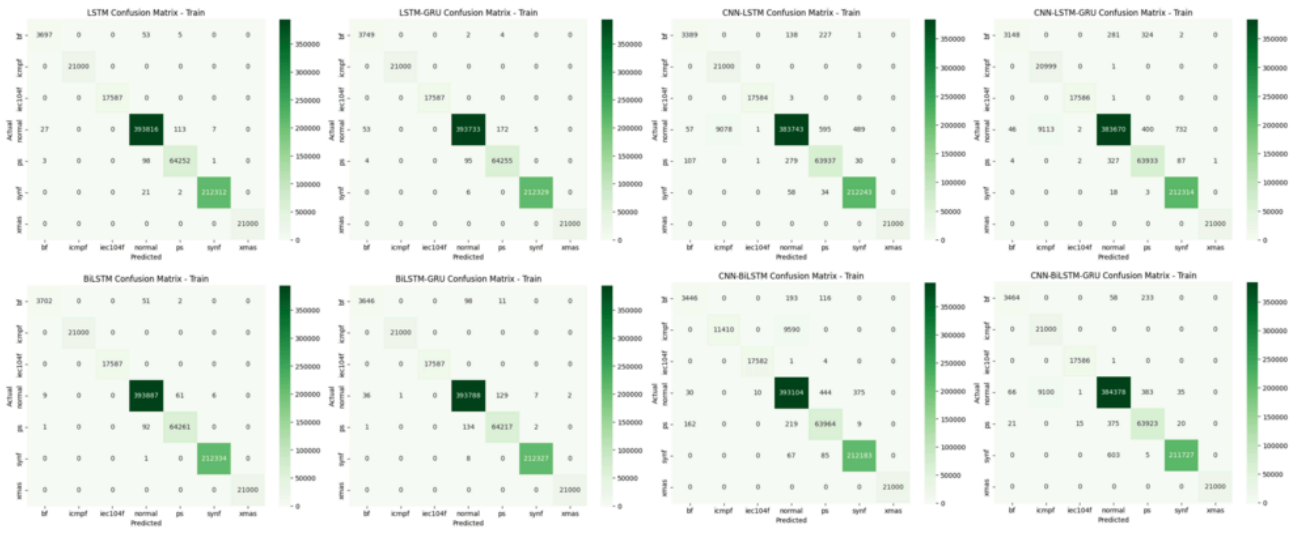

FIGURE 3: Confusion matrices of training datasets for all evaluated models

BiLSTM, Bidirectional Long Short-Term Memory; CNN, Convolutional Neural Network; GRU, Gated Recurrent Unit; LSTM, Long Short-Term Memory

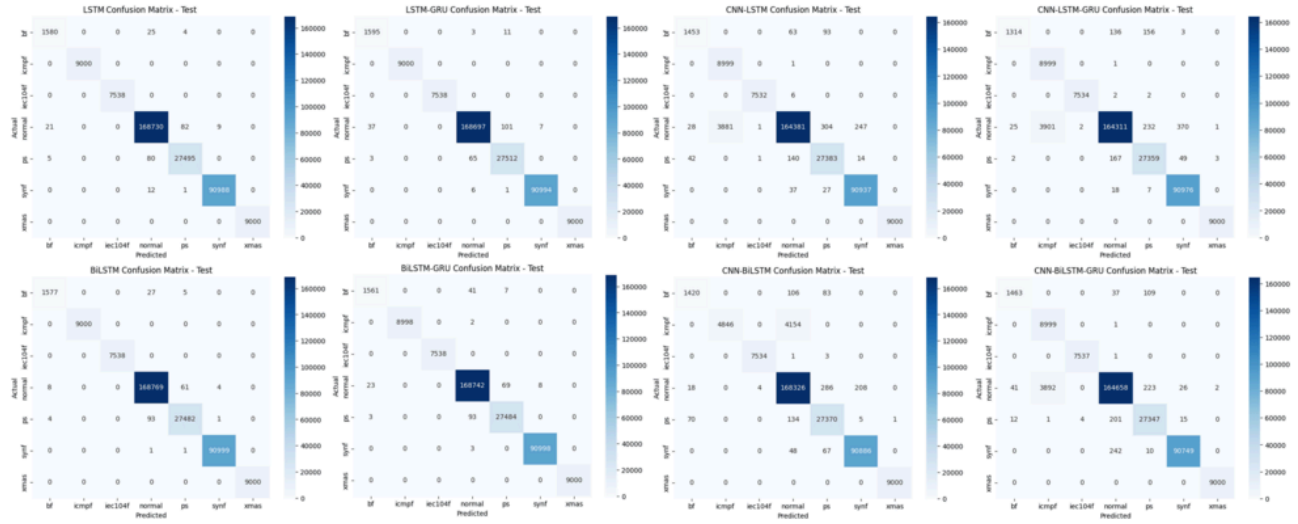

FIGURE 4: Confusion matrices of testing datasets for all evaluated models

BiLSTM, Bidirectional Long Short-Term Memory; CNN, Convolutional Neural Network; GRU, Gated Recurrent Unit; LSTM, Long Short-Term Memory

How to cite this article:
Arifin M, Stiawan D, Susanto S, et al. (May 15, 2026) Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation. Cureus J Comput Sci 3 : es44389-026-00076-0. DOI https://doi.org/10.7759/s44389-026-00076-0

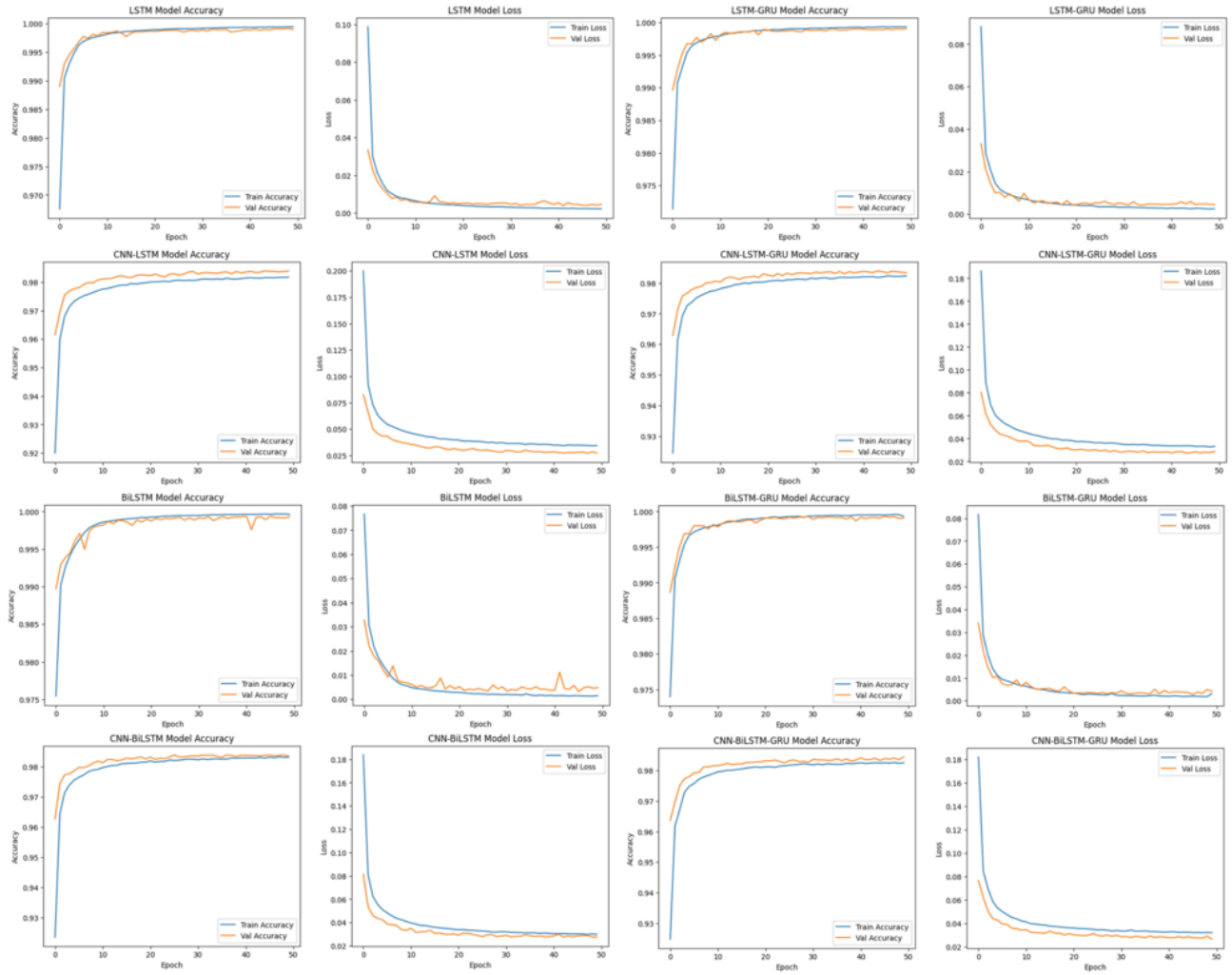

FIGURE 5: Training and validation accuracy and loss curves over 50 epochs for all evaluated models

BiLSTM, Bidirectional Long Short-Term Memory; CNN, Convolutional Neural Network; GRU, Gated Recurrent Unit; LSTM, Long Short-Term Memory

Analysis and discussion

Although the dataset used in this study was generated from a realistic SCADA IEC 60870-5-104 testbed, several limitations should be acknowledged. First, the dataset is collected in a controlled experimental environment, which may not fully capture the complexity and variability of real-world industrial deployments. As a result, certain network conditions, background traffic variations, and unexpected operational behaviors may not be entirely represented.

Second, there is a potential class imbalance in the dataset, where some attack types may have fewer samples compared to others. This imbalance can influence the learning process and may lead to biased model performance toward more dominant classes.

Third, the dataset includes a predefined set of attack scenarios, such as brute force, flooding-based attacks, and port scanning. While these attacks represent common threats in SCADA networks, other advanced or stealthy attack types may not be covered, which limits the generalization of the models to unseen attack patterns.

Despite these limitations, the dataset provides a realistic and SCADA-specific representation of IEC 60870-5-104 communication, making it suitable for evaluating sequence-based intrusion detection models under controlled and reproducible conditions. These limitations should be considered when interpreting the experimental results, as they may partially influence the observed performance differences across models and attack types.

The evaluation results show that the LSTM and BiLSTM models are the most consistent and accurate in detecting attacks on the SCADA IEC 60870-5-104 network. Both models achieved approximately 99.9% accuracy on both training and test datasets, with very low loss values (0.17-0.34). The accuracy curves indicate rapid convergence within the first 10 epochs, and the loss curves remain stable without significant signs of overfitting. The confusion matrices reveal that almost all classes - including bf, icmpf, iec104f, and xmas - are correctly classified, with only minor misclassifications in the bf and ps classes. BiLSTM in particular demonstrates superior performance because it captures bidirectional temporal dependencies, which are especially important in SCADA traffic where attacks often exhibit repetitive and overlapping temporal patterns.

LSTM-GRU and BiLSTM-GRU also deliver strong results, with accuracy close to LSTM/BiLSTM. Although the training time, especially for BiLSTM-GRU (221 minutes), is longer due to the added complexity, their performance remains robust, with F1-scores approaching 1.0 for almost all classes. The accuracy curves for these models follow a pattern similar to the pure LSTM but show slightly more fluctuation in later epochs, indicating small variations in generalization. The advantage of GRU in these hybrids lies in its simpler gating mechanism, which improves computational efficiency and makes them more attractive for real-time IDS deployment.

CNN-based models such as CNN-LSTM and CNN-BiLSTM show a drop in performance, with test accuracy in the range of 98.3-98.4% and lower F1-scores for certain classes, particularly icmpf and bf. The confusion matrices reveal notable misclassifications between normal traffic and icmpf, indicating that CNN-based feature extraction is less effective in capturing the temporal characteristics of certain attack patterns. This discrepancy can be explained by the nature of ICMP flood attacks, which exhibit highly repetitive and time-dependent behavior rather than localized feature structures. While convolutional layers are effective at extracting spatial or local patterns, they may not optimally preserve long-range temporal dependencies, especially when combined with pooling operations that can reduce sequential resolution. As a result, important temporal relationships may be partially lost, leading to reduced detection performance for flooding-based attacks.

In contrast, sequence-based models such as LSTM and BiLSTM are specifically designed to capture temporal dependencies in sequential data, allowing them to better model the continuous and repetitive patterns of ICMP flood traffic. This explains the superior performance observed in these models across most evaluation metrics. From a practical perspective, these findings suggest that model selection for intrusion detection in SCADA environments should consider the dominant characteristics of network traffic. For scenarios where attacks exhibit strong temporal dependencies, sequence-based architectures are more suitable, whereas CNN-based hybrid models may still be beneficial when both spatial and temporal features are present.

Three-stage hybrid models like CNN-LSTM-GRU and CNN-BiLSTM-GRU show a similar trend to other CNN-based variants, with slight improvements in some classes. While their accuracy and loss metrics outperform CNN-only architectures, the icmpf and bf classes still exhibit misclassifications in the confusion matrices. Their accuracy curves also display a small but consistent gap between training and validation, suggesting reasonable but not optimal generalization. However, these models provide a good balance by combining CNN's spatial feature extraction, BiLSTM's bidirectional sequence learning, and GRU's efficiency making them relevant for scenarios where both accuracy and computational constraints must be considered.

Overall, the results indicate that sequence-based architectures, particularly BiLSTM and LSTM, demonstrate superior performance under the experimental conditions of this study. CNN-based hybrid models, while slightly less effective for purely sequential SCADA traffic, remain relevant in scenarios where both spatial and temporal features are present. These findings highlight the importance of selecting model architectures based on the underlying characteristics of network traffic.

Conclusions

This study presented a comprehensive comparative analysis of deep learning and hybrid deep learning architectures for intrusion detection in SCADA networks operating under the IEC 60870-5-104 protocol. Eight models - LSTM, GRU, BiLSTM, CNN-LSTM, CNN-BiLSTM, LSTM-GRU, CNN-LSTM-GRU, and CNN-BiLSTM-GRU - were evaluated using a realistic dataset containing both benign traffic and multiple attack types, including bruteforce, ICMP flood, IEC104 flood, port scan, SYN flood, and XMAS flood. The evaluation employed sequence-based learning, with performance assessed through accuracy, loss, precision, recall, F1-score, confusion matrix analysis, and convergence behavior. The findings reveal that sequence-oriented architectures, particularly BiLSTM and LSTM-GRU, achieved the most consistent and superior performance, maintaining accuracy close to 99.9% and demonstrating strong generalization on unseen traffic. BiLSTM, in particular, proved highly effective at capturing bidirectional temporal dependencies, while LSTM-GRU offered a balance between accuracy and computational efficiency. In contrast, CNN-based hybrid models performed competitively in most scenarios but showed noticeable degradation in detecting certain attack types such as ICMP flood, indicating that convolutional layers are less optimal for modeling purely temporal patterns in SCADA traffic. Overall, the results suggest that pure sequence-based architectures remain the most suitable for intrusion detection in SCADA IEC 60870-5-104 environments, where temporal dependencies.

Future research will focus on expanding the dataset to include more diverse attack scenarios, integrating attention mechanisms to enhance feature representation, and exploring lightweight yet robust model architectures for deployment in resource-constrained industrial environments.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: M. Agus Syamsul Arifin, Deris Stiawan, Susanto Susanto, Mohd Yazid Idris, Rahmat Budiarto

Acquisition, analysis, or interpretation of data: M. Agus Syamsul Arifin, Deris Stiawan, Susanto Susanto, Mohd Yazid Idris, Rahmat Budiarto

Drafting of the manuscript: M. Agus Syamsul Arifin, Deris Stiawan, Susanto Susanto, Mohd Yazid Idris, Rahmat Budiarto

Critical review of the manuscript for important intellectual content: M. Agus Syamsul Arifin, Deris Stiawan, Susanto Susanto, Mohd Yazid Idris, Rahmat Budiarto

Supervision: M. Agus Syamsul Arifin, Deris Stiawan, Susanto Susanto, Mohd Yazid Idris, Rahmat Budiarto

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

Data Availability Statements

De-identified and/or licensed data are available via controlled access from Zenodo; see https://zenodo.org/records/7034534 for access criteria.

References

1. Yadav G, Paul K: Architecture and security of SCADA systems: A review. International Journal of Critical Infrastructure Protection. 2021, 34:100433. 10.1016/j.ijcip.2021.100433
2. Sverko M, Grbac TG, Mikuc M: SCADA systems with focus on continuous manufacturing and steel industry: a survey on architectures, standards, challenges and Industry 5.0. IEEE Access. 2022, 10:109395-109430. 10.1109/access.2022.3211288
3. Suaboot J, Fahad A, Tari Z, et al.: A taxonomy of supervised learning for IDSs in SCADA environments. ACM Computing Surveys. 2020, 53:1-37. 10.1145/3379499
4. Mondal S, Prudhvi B, Khare P, Bharata Reddy MJ: Real-time analysis of cyber attacks in SCADA based power system. Australian Journal of Electrical and Electronics Engineering. 2025, 1-25. 10.1080/1448837X.2025.2531694
5. Alimi OA, Ouahada K, Abu-Mahfouz AM, Rimer S, Alimi KOA: A review of research works on supervised learning algorithms for SCADA intrusion detection and classification. Sustainability. 2021, 13:9597. 10.3390/su13179597
6. Wali S, Farrukh YA, Khan I, Hamilton JA: Covert penetrations: Analyzing and defending SCADA systems from stealth and Hijacking attacks. Computers & Security. 2025, 156:104449. 10.1016/j.cose.2025.104449
7. Radoglou-Grammatikis P, Sarigiannidis P, Giannoulakis I, Kafetzakis E, Panaousis E: Attacking IEC-60870-5-104 SCADA systems. 2019 IEEE World Congress on Services (SERVICES), Milan, Italy. 2019, 41-46. 10.1109/services.2019.00022
8. Mai K, Qin X, Ortiz Silva N, Cardenas AA: IEC 60870-5-104 network characterization of a large-scale operational power grid. 2019 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA. 2019, 236-241. 10.1109/SPW.2019.00051
9. Arifin MAS, Stiawan D, Suprapto BY, et al.: A novel dataset for experimentation with intrusion detection systems in SCADA networks using IEC 60870-5-104 standard. IEEE Access. 2024, 12:170553-170569. 10.1109/access.2024.3473895
10. Hareesh R, Kalluri R, Mahendra L, Senthil Kumar RK, Bindhumadhava BS: Passive security monitoring for IEC-60870-5-104 based SCADA systems. International Journal of Industrial Control Systems Security (IJICSS). 2020, 3:90-99. 10.20533/ijicss.9781.9083.20346.2020.0010
11. Baiocco A, Wolthusen SD: Causality re-ordering attacks on the IEC 60870-5-104 protocol. 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, USA. 2018, 1-5. 10.1109/PESGM.2018.8586010
12. Pliatsios D, Sarigiannidis P, Lagkas T, Sarigiannidis AG: A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Communications Surveys & Tutorials. 2020, 22:1942-1976. 10.1109/comst.2020.2987688
13. Radoglou-Grammatikis P, Rompolos K, Sarigiannidis P: Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach. IEEE Transactions on Industrial Informatics. 2021, 18:2041-2052. 10.1109/tii.2021.3093905
14. Lin CY, Nadjm-Tehrani S: Understanding IEC-60870-5-104 traffic patterns in SCADA networks. CPSS '18: Proceedings of the 4th ACM Workshop on Cyber-Physical System Security. 2018, 51-60. 10.1145/3198458.3198460
15. Negi R, Dutta A, Handa A, Ayyangar U, Shukla SK: Intrusion detection & prevention in programmable logic controllers: a model-driven approach. 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS), Tampere, Finland. 2020, 215-222. 10.1109/ICPS48405.2020.9274765
16. Zhao X, Zhang L, Cao Y, Jin K, Hou Y: Anomaly detection approach in industrial control systems based on measurement data. Information. 2022, 13:450. 10.3390/info13100450
17. Upadhyay D, Manero J, Zaman M, Sampalli S: Intrusion detection in SCADA based power grids: recursive feature elimination model with majority vote ensemble algorithm. IEEE Transactions on Network Science and Engineering. 2021, 8:2559-2574. 10.1109/tnse.2021.3099371
18. Saranya T, Sridevi S, Deisy C, Chung TD, Ahamed Khan MKA: Performance analysis of machine learning algorithms in intrusion detection system: a review. Procedia Computer Science. 2020, 171:1251-1260. 10.1016/j.procs.2020.04.133
19. Rashid A, Siddique MJ, Ahmed SM: Machine and deep learning based comparative analysis using hybrid approaches for intrusion detection system. 2020 3rd International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan. 2020, 1-9. 10.1109/ICACS47775.2020.9055946
20. Oliveira N, Praça I, Maia E, Sousa O: Intelligent cyber attack detection and classification for network-based intrusion detection systems. Applied Sciences. 2021, 11:1674. 10.3390/app11041674

How to cite this article:
Arifin M, Stiawan D, Susanto S, et al. (May 15, 2026) Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation. Cureus J Comput Sci 3 : es44389-026-00076-0. DOI https://doi.org/10.7759/s44389-026-00076-0

21. Asad H, Gashi I: Dynamical analysis of diversity in rule-based open source network intrusion detection systems. Empirical Software Engineering. 2022, 27:4. 10.1007/s10664-021-10046-w

22. Liu H, Lang B: Machine learning and deep learning methods for intrusion detection systems: A survey. Applied Sciences. 2019, 9:4396. 10.3390/app9204396

23. Rakas SVB, Stojanović MD, Marković-Petrović JD: A review of research work on network-based SCADA intrusion detection systems. IEEE Access. 2020, 8:93083-93108. 10.1109/access.2020.2994961

24. Waagsnes H, Ulltveit-Moe N: Intrusion detection system test framework for SCADA systems. Proceedings of the 4th International Conference on Information Systems Security and Privacy - ICISSP. 2018, 1:275-285. 10.5220/0006588202750285

25. Grammatikis PR, Sarigiannidis P, Sarigiannidis A, Margounakis D, Tsiakalos A, Efstathopoulos G: An anomaly detection mechanism for IEC 60870-5-104. 2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST), Bremen, Germany. 2020, 1-4. 10.1109/MOCAST49295.2020.9200285

26. Egger M, Eibl G, Engel D: Comparison of approaches for intrusion detection in substations using the IEC 60870-5-104 protocol. Energy Informatics. 2020, 3:15. 10.1186/s42162-020-00118-4

27. Altunay HC, Albayrak Z, Özalp AN, Çakmak M: Analysis of anomaly detection approaches performed through deep learning methods in SCADA systems. 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey. 2021, 3:1-6. 10.1109/HORA52670.2021.9461273

28. Ghani AA, Alasadi SA: A deep learning algorithm to cybersecurity: enhancing intrusion detection with a hybrid GRU and BiLSTM model. Engineering, Technology & Applied Science Research. 2025, 15:23605-23612. 10.48084/etasr.10666

29. Arifin MAS, Stiawan D, Susanto, Rejito J, Idris MY, Budiarto R: Denial of service attacks detection on SCADA network IEC 60870-5-104 using machine learning. 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Semarang, Indonesia. 2021, 228-232. 10.23919/eecsi53397.2021.9624255

30. Agus Syamsul Arifin M, Stiawan D, Suprapto BY, Susanto S, Salim T, Idris MY, Budiarto R: Oversampling and undersampling for intrusion detection system in the supervisory control and data acquisition IEC 60870-5-104. IET Cyber-Physical Systems: Theory & Applications. 2024, 9:282-292. 10.1049/cps2.12085

31. Balla A, Habaebi MH, Elsheikh EAA, Islam MR, Suliman FEM, Mubarak S: Enhanced CNN-LSTM deep learning for SCADA IDS featuring Hurst parameter self-similarity. IEEE Access. 2024, 12:6100-6116. 10.1109/access.2024.3350978

32. Hamdi N: A hybrid learning technique for intrusion detection system for smart grid. Sustainable Computing: Informatics and Systems. 2025, 46:101102. 10.1016/j.suscom.2025.101102

33. Barsha NK, Hubballi N: Anomaly detection in SCADA systems: a state transition modeling. IEEE Transactions on Network and Service Management. 2024, 21:3511-3521. 10.1109/tnsm.2024.3373881

34. Choudhary N, Khaitan V: Dependability analysis of cloud-based VoIP under an advanced persistent threat attack: a semi-Markov approach. Transactions on Emerging Telecommunications Technologies. 2026, 37:e70353. 10.1002/ett.70353

35. Bakhsh SA, Khan MS, Saidani O, Alasbali N, Abbas SQ, Khan MA, Ahmad J: Enhancing security in DNP3 communication for smart grids: a segmented neural network approach. IEEE Access. 2025, 13:110436-110456. 10.1109/access.2025.3580507

36. Farheen, Kumar R: Sliding window-based anomaly detection. Procedia Computer Science. 2025, 258:2520-2529. 10.1016/j.procs.2025.04.514

37. Chaudhari A, Gohil B, Rao UP: A novel hybrid framework for Cloud Intrusion Detection System using system call sequence analysis. Cluster Computing. 2023, 27:3753-3769. 10.1007/s10586-023-04162-z

38. Huan S, Zhang X, Shang W, Cao H, Li H, Yang Y, Liu W: T-shaped CAN feature integration with lightweight deep learning model for in-vehicle network intrusion detection. IEEE Transactions on Intelligent Transportation Systems. 2024, 25:21183-21196. 10.1109/tits.2024.3478371

39. Halbouni A, Gunawan TS, Habaebi MH, Halbouni M, Kartiwi M, Ahmad R: CNN-LSTM: hybrid deep neural network for network intrusion detection system. IEEE Access. 2022, 10:99837-99849. 10.1109/access.2022.3206425

40. Hariharan S, Annie Jerusha Y, Suganeshwari G, Syed Ibrahim SP, Tupakula U, Varadharajan V: A hybrid deep learning model for network intrusion detection system using Seq2Seq and ConvLSTM-subnets. IEEE Access. 2025, 13:30705-30721. 10.1109/access.2025.3541399

How to cite this article:
Arifin M, Stiawan D, Susanto S, et al. (May 15, 2026) Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation. Cureus J Comput Sci 3 : es44389-026-00076-0. DOI https://doi.org/10.7759/s44389-026-00076-0

41. Yaras S, Dener M: IoT-based intrusion detection system using new hybrid deep learning algorithm. Electronics. 2024, 13:1053. 10.3390/electronics13061053

42. Bamber SS, Reddy Katkuri AV, Sharma S, Angurala M: A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system. Computers & Security. 2025, 148:104146. 10.1016/j.cose.2024.104146

43. Ben Said R, Sabir Z, Askerzade I: CNN-BiLSTM: a hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection. IEEE Access. 2023, 11:138732-138747. 10.1109/access.2023.3340142

44. Dai W, Li X, Ji W, He S: Network intrusion detection method based on CNN-BiLSTM-attention model. IEEE Access. 2024, 12:53099-53111. 10.1109/access.2024.3384528

45. Zhang C, Li J, Wang N, Zhang D: Research on intrusion detection method based on transformer and CNN-BiLSTM in Internet of Things. Sensors. 2025, 25:2725. 10.3390/s25092725

46. Hnamte V, Hussain J: DCNNBiLSTM: an efficient hybrid deep learning-based intrusion detection system. Telematics and Informatics Reports. 2023, 10:100053. 10.1016/j.teler.2023.100053

47. Nandanwar H, Katarya R: TL-BILSTM IoT: transfer learning model for prediction of intrusion detection system in IoT environment. International Journal of Information Security. 2024, 23:1251-1277. 10.1007/s10207-023-00787-8

48. Afraji DMAA, Lloret J, Peñalver L: An integrated hybrid deep learning framework for intrusion detection in IoT and IIoT networks using CNN-LSTM-GRU architecture. Computation. 2025, 13:222. 10.3390/computation13090222

49. Kilichev D, Turimov D, Kim W: Next-generation intrusion detection for IoT EVCS: integrating CNN, LSTM, and GRU models. Mathematics. 2024, 12:571. 10.3390/math12040571

50. Pradeep M, Gopalakrishnan S: Enhancing intrusion detection systems in IoT networks: a hybrid approach using CNN, ANN, LSTM, GRU for improved security. 2024 8th International Conference on Inventive Systems and Control (ICISC), Coimbatore, India. 2024, 487-492. 10.1109/ICISC62624.2024.00087

How to cite this article:
Arifin M, Stiawan D, Susanto S, et al. (May 15, 2026) Performance Enhancement of Supervisory Control and Data Acquisition (SCADA) IEC 60870-5-104 Intrusion Detection Using Sequence-Aware and Hybrid Deep Learning Models: A Comparative Evaluation. Cureus J Comput Sci 3 : es44389-026-00076-0. DOI https://doi.org/10.7759/s44389-026-00076-0