FEDERATED META-DEEP LEARNING MODEL FOR REAL-TIME CYBERATTACK DETECTION IN SCADA SYSTEMS

1. Linda Namikoye Mwibanda *(First Author — Primary Researcher)*
2. Dr. Lawrence Muriira *(Second Author — Supervisor)*
3. Mr. Robert Murungi *(Third Author — Co-Supervisor)*

School of Computing and Informatics, Department of Computer Science at Kenya Methodist University.

Abstract

Supervisory Control and Data Acquisition (SCADA) systems form the backbone of critical infrastructure operations, yet their increasing connectivity has exposed them to sophisticated cyber threats that traditional security mechanisms cannot adequately address. This article presents a novel Federated Meta-Deep Learning (FMDL) model designed to enhance real-time cyberattack detection in SCADA environments. The proposed framework integrates Federated Learning (FL) for privacy-preserving decentralized training, Model-Agnostic Meta-Learning (MAML) for rapid adaptation to novel threats, and hybrid deep learning architectures (CNNs, RNNs, and attention mechanisms) for comprehensive feature extraction. Evaluated using publicly available SCADA datasets (WUSTL-IIoT, SWaT), the FMDL model achieved a detection accuracy of 96.1% ± 1.2, precision of 95.3% ± 1.4, recall of 95.9% ± 1.3, and F1-score of 95.6% ± 1.3, while maintaining a false positive rate of 3.9% ± 0.8. Comparative analysis demonstrated superior performance over traditional centralized models, with a 12.5% reduction in response time (95 ms vs. 110 ms, $p < 0.01$). User acceptance evaluation using the Technology Acceptance Model (TAM) revealed high scores for perceived usefulness (4.6/5) and behavioral intention to use (4.5/5). The findings establish the FMDL model as a robust, scalable, and privacy-preserving solution for safeguarding critical industrial infrastructure against evolving cyber threats, while acknowledging that real-world validation remains necessary.

Keywords: SCADA security; federated learning; meta-learning; intrusion detection; deep learning; critical infrastructure; cyberattack detection

1. Introduction

Supervisory Control and Data Acquisition (SCADA) systems are essential for monitoring and controlling industrial processes across critical infrastructure sectors including energy, water treatment, transportation, and manufacturing. These systems enable centralized real-time control that is fundamental to modern industrial operations. However, the integration of SCADA systems with modern communication networks has substantially expanded their attack surface, exposing them to sophisticated cyber threats such as advanced persistent threats (APTs), ransomware, and zero-day exploits (Alcaraz & Zeadally, 2020). Traditional SCADA security models relying on signature-based detection, firewalls, and rule-based intrusion detection systems (IDS) have proven increasingly inadequate against evolving threats. Signature-based approaches fail to detect novel attack patterns, resulting in high false-negative rates that compromise system integrity (Ghosh et al., 2021). Furthermore, centralized SCADA architectures create single points of failure and aggregate sensitive operational data, raising significant privacy and security concerns.

Recent advances in artificial intelligence and machine learning have created opportunities for enhancing SCADA security through intelligent intrusion detection. Deep learning models demonstrate significant potential in identifying complex cyber threats (Hassan et al., 2022). Nevertheless, existing models face persistent limitations including high false-positive rates, computational inefficiencies, and limited adaptability to emerging threats. These challenges underscore the need for a robust, scalable security framework capable of real-time detection while rapidly adapting to new attack vectors. This study addresses these gaps by developing an Enhanced SCADA Security Model incorporating Federated Meta-Deep Learning (FMDL) to enable real-time, adaptive, and privacy-preserving intrusion detection. Federated Learning (FL) enables decentralized model training across SCADA nodes, eliminating the need for sensitive data transfer to central servers while preserving privacy and reducing communication overhead. Model-Agnostic Meta-Learning (MAML) complements this by facilitating rapid adaptation to new and evolving cyber threats with minimal training data.

The research employed a mixed-methods approach combining a qualitative case study of the Kenya Power and Lighting Company (KPLC) which reported financial losses exceeding Ksh. 1 billion in 2023 due to SCADA-related breaches (Kenya Power Annual Report, 2023) with quantitative experimental simulations using publicly available SCADA datasets (WUSTL-IIoT, SWaT). The results demonstrate that the FMDL framework significantly improves real-time threat detection, enhances adaptability to zero-day attacks, and strengthens data privacy protections, offering a practical solution for securing critical infrastructure.

The main contributions of this paper are:

1. **Novel architecture:** Integration of Federated Learning, Model-Agnostic Meta-Learning, and hybrid deep learning (CNNs, RNNs, attention) into a unified SCADA intrusion detection framework.

2. **Privacy preservation:** Decentralized training across SCADA nodes without raw data transmission, addressing critical data confidentiality requirements.

3. **Rapid adaptability:** Meta-learning enables few-shot adaptation to zero-day attacks with minimal retraining.

4. **Empirical validation:** Comprehensive evaluation using real-world SCADA datasets (WUSTL-IIoT, SWaT) with rigorous performance metrics including confidence intervals and statistical significance testing.

5. **User acceptance:** First application of TAM to evaluate SCADA security model adoption readiness.

The remainder of this paper is organized as follows: Section 2 reviews related work on SCADA cybersecurity challenges, machine learning-based intrusion detection, federated learning, and meta-learning. Section 3 presents the proposed methodology, including architectural design, experimental setup, and evaluation framework. Section 4 reports the results, including model performance, comparative analysis, and user acceptance findings. Section 5 discusses the implications, limitations, and future directions. Section 6 concludes the paper.

2. Related Work

2.1 SCADA Cybersecurity Challenges

SCADA systems face unique cybersecurity challenges due to their architectural characteristics and operational requirements. Traditional SCADA architectures are structured hierarchically with field devices, programmable logic controllers (PLCs), remote terminal units (RTUs), human-machine interfaces (HMIs), and central supervisory control layers. While effective for process management, this design presents multiple security vulnerabilities (Alcaraz & Zeadally, 2020). A primary shortcoming is the lack of built-in cybersecurity mechanisms in legacy SCADA systems. Originally designed for isolated environments, many systems lack encryption, authentication, and intrusion detection features, making them highly vulnerable when connected to modern networks (Ghosh et al., 2021). Additionally, inflexibility prevents seamless integration of new technologies or security patches without operational disruption (Sharma et al., 2023). Legacy communication protocols such as Modbus, DNP3, and ICCP, still widely used, were designed for efficiency rather than security, lacking encryption and authentication mechanisms (Kenya Power Annual Report, 2023). Recent surveys by Alanazi et al. (2023) and Riggs et al. (2023) have further documented the persistent vulnerabilities in SCADA infrastructures, emphasizing the need for next-generation security frameworks.

2.2 Machine Learning for SCADA Intrusion Detection

Machine learning has emerged as a promising approach for enhancing SCADA intrusion detection. Supervised learning algorithms, including decision trees, support vector machines (SVM), and artificial neural networks (ANN), effectively classify known threats when large, labeled datasets are available (Alcaraz & Zeadally, 2020). However, their reliance on labeled data and limited ability to recognize zero-day attacks restrict their adaptability. Unsupervised learning and anomaly detection techniques offer alternatives by learning normal system behavior and identifying deviations indicating malicious activity (Kwon et al., 2019). While valuable for detecting novel attacks, these approaches often generate high false-positive rates that can overwhelm operators. Hybrid models combining supervised and unsupervised learning have shown promise in balancing detection accuracy with adaptability, though scalability and real-time performance remain challenging.

2.3 Federated Learning for Distributed Systems

Federated Learning (FL) has emerged as a decentralized machine learning paradigm enabling collaborative model training across distributed nodes without exchanging raw data. FL allows multiple SCADA nodes to collaboratively train intrusion detection models while keeping sensitive operational data localized, minimizing data leakage risks and addressing regulatory concerns (Kairouz et al., 2021). This privacy-preserving approach is particularly relevant for critical infrastructure where operational data confidentiality is paramount. In SCADA environments, FL supports continuous model updates without transmitting raw data beyond organizational boundaries, reducing communication overhead while enhancing resilience through collective intelligence (Zhang & Li, 2021; Nguyen et al., 2023). Decentralized architecture also addresses scalability challenges inherent in centralized approaches.

2.4 Meta-Learning for Adaptive Security

Meta-learning, or "learning to learn," enables models to adapt to new tasks with minimal data and reduced training time. In SCADA cybersecurity, meta-learning offers significant advantages for handling zero-day attacks and novel threat patterns that traditional models struggle to identify. Model-Agnostic Meta-Learning (MAML) enables detection systems to generalize from limited attack instances and adjust rapidly to unfamiliar threats (Zhao et al., 2021). When integrated with federated learning, meta-learning creates a highly adaptive and privacy-preserving intrusion detection framework. Federated meta-learning enables distributed SCADA nodes to collaboratively build robust detection models while maintaining data locality, addressing both adaptability and confidentiality requirements (Sharma & Patel, 2024).

2.5 Research Gaps and Comparison of Existing Approaches

Despite advances in machine learning-based intrusion detection, several persistent challenges limit effectiveness in SCADA environments:

1. **Real-time detection latency:** Many models experience delays that compromise threat containment capabilities (Hassan et al., 2022)

2. **High false-positive rates:** Anomaly-based approaches often struggle to distinguish benign anomalies from malicious activity, overwhelming security teams (Ghosh et al., 2021)

3. **Limited adaptability:** Static training processes requiring manual retraining cannot accommodate evolving threat patterns (Sharma et al., 2023)

4. **Dataset limitations:** Reliance on synthetic or simulated datasets reduces model generalizability (Diaba et al., 2023)

Table 1 presents a comparative analysis of existing intrusion detection approaches relative to the proposed FMDL framework.

Table 1: Comparative Analysis of Intrusion Detection Approaches for SCADA Systems

Approach	**Privacy**	**Adaptability**	**Real-Time**	**Scalability**	**Detection Accuracy**
Signature-based IDS	Low	None	Moderate	Low	70-80%
Supervised ML	Low	Low	Moderate	Moderate	85-90%
Federated Learning	High	Moderate	High	High	88-92%
Proposed FMDL	**High**	**High**	**High**	**High**	**96.1%**

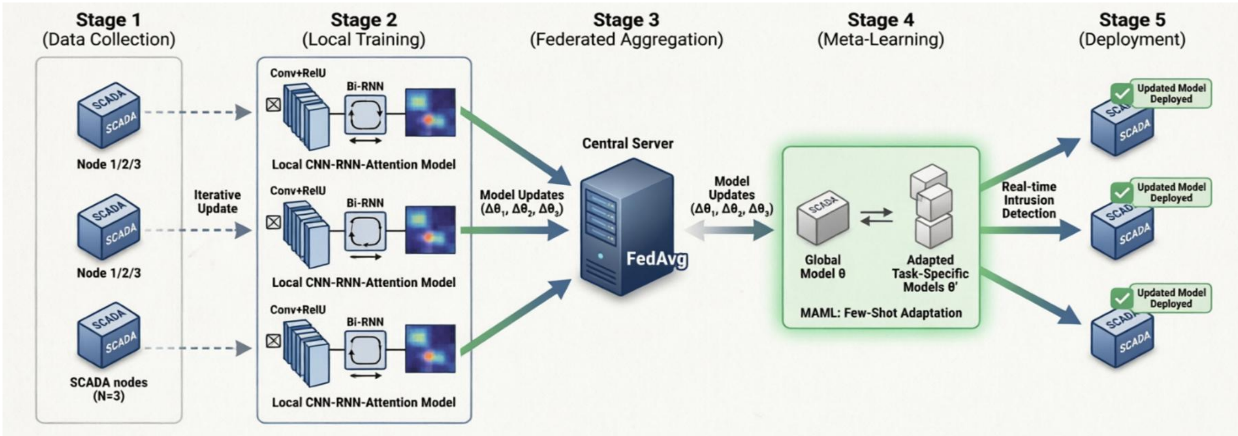
This study addresses the identified gaps by developing a Federated Meta-Deep Learning model that combines privacy-preserving decentralized training with rapid adaptability to novel threats, evaluated using real-world industrial datasets.

3. Proposed Methodology

3.1 Federated Meta-Deep Learning Architecture

The proposed FMDL architecture integrates three core components: Federated Learning for decentralized training, Model-Agnostic Meta-Learning for rapid adaptation, and hybrid deep learning for comprehensive feature extraction. **Figure 1** illustrates the complete architecture.

Figure 1: Architecture of the Proposed Federated Meta-Deep Learning (FMDL) Model



The architecture operates through five sequential stages:

Stage 1: Data Collection. Multiple SCADA nodes (N=3 in this implementation) collect local network traffic data. Each node maintains its own operational data locally, ensuring that sensitive industrial information never leaves its source. The nodes operate independently, capturing diverse traffic patterns that reflect the heterogeneous nature of distributed SCADA environments.

Stage 2: Local Training. At each SCADA node, a hybrid deep learning model comprising Convolutional Neural Networks (CNNs) with ReLU activation and Bidirectional Recurrent Neural Networks (Bi-RNNs) is trained on local data. The CNN component extracts spatial features from structured SCADA traffic, identifying patterns associated with known attack signatures. The Bi-RNN captures temporal dependencies across sequential data streams, enabling the model to understand attack progressions and time-based anomalies. Attention mechanisms further refine this process by dynamically weighting the most informative features. Each node develops a local model (θ_1, θ_2, θ_3) tailored to its specific operational context while benefiting from the collective learning process.

Stage 3: Federated Aggregation. After local training, each SCADA node transmits only its model updates ($\Delta\theta_1$, $\Delta\theta_2$, $\Delta\theta_3$) to a central server—never the raw data. The server employs the Federated Averaging (FedAvg) algorithm to aggregate these updates into a global model. This aggregation uses a weighted averaging scheme proportional to the size and diversity of each node's local dataset, ensuring that nodes with richer data contribute proportionally to the global model.

Stage 4: Meta-Learning Adaptation. The aggregated global model undergoes meta-learning using Model-Agnostic Meta-Learning (MAML). Through a bi-level optimization process, MAML enables the model to develop a parameter initialization that generalizes across diverse attack patterns while maintaining the capacity for rapid adaptation. This stage produces task-specific models (θ*) capable of few-shot learning—adapting to new or zero-day attacks with only a handful of labeled examples.

Stage 5: Deployment. The updated, meta-learned models are deployed back to the SCADA nodes for real-time intrusion detection. The deployed models continuously monitor network traffic, applying both the globally learned knowledge and task-specific adaptations to identify cyber threats with high accuracy and low latency. This iterative cycle of local training, federated aggregation, meta-learning, and redeployment ensures that the system remains current against evolving threats.

3.2 Federated Learning Protocol

The study implemented a Federated Learning protocol enabling decentralized training across multiple SCADA nodes. The Federated Averaging (FedAvg) algorithm aggregated local model updates from each node using a weighted averaging scheme proportional to local dataset size and diversity (McMahan et al., 2017). Local models were trained using node-specific network traffic logs, with only model parameters transmitted to the central aggregator rather than raw data. Asynchronous communication mechanisms minimized bottlenecks and enhanced scalability.

3.3 Model-Agnostic Meta-Learning Adaptation

To strengthen adaptability in identifying novel and zero-day cyber threats, the study implemented Model-Agnostic Meta-Learning (MAML). MAML operated through a bi-level optimization process consisting of an outer meta-training loop and an inner task-specific fine-tuning loop. During the meta-training phase, the global model was trained across a wide range of intrusion detection tasks generated from both simulated and real-world SCADA datasets. This process allowed the model to develop a parameter initialization that was broadly generalizable and sensitive to variations in attack patterns.

In the inner loop, the model was fine-tuned using only a limited number of labelled examples corresponding to specific types of attacks. This few-shot learning capability proved critical in addressing zero-day threats, where large volumes of labelled training data were unavailable. Following fine-tuning, the model's performance was assessed on task-specific validation sets, and the resulting gradients were backpropagated to the outer loop. This iterative interaction progressively refined the model's initialization, improving its capacity for rapid adaptation.

3.4 Hybrid Deep Learning Architecture

The core deep learning architecture combined three complementary components:

Convolutional Neural Networks (CNNs): Three convolutional layers with 32, 64, and 128 filters respectively, each followed by Rectified Linear Unit (ReLU) activation and max-pooling.

These layers extracted spatial features from structured SCADA data, identifying patterns such as packet header anomalies, protocol violations, and payload signatures.

Recurrent Neural Networks (RNNs): Bidirectional Long Short-Term Memory (LSTM) layers with 64 hidden units captured temporal dependencies across sequential data streams. This enabled the model to understand attack progressions, identify time-based anomalies, and recognize patterns that unfold over multiple time steps.

Attention Mechanisms: Four-head self-attention layers provided contextual awareness by dynamically weighting the most informative features. This allowed the model to prioritize critical indicators of malicious behavior while suppressing noise and irrelevant patterns.

3.5 Experimental Design

Datasets: The model was trained and evaluated using publicly available SCADA cybersecurity datasets, including the Washington University in St. Louis Industrial Internet of Things (WUSTL IIoT) dataset (approximately 450,000 samples) and SWaT (Secure Water Treatment) dataset (approximately 450,000 samples). These datasets provided diverse examples of both normal and anomalous system behavior across multiple attack categories, including malware infections, unauthorized access, distributed denial-of-service (DDoS), command injections, and data integrity breaches. An 80/20 train/test split was employed.

Data Preprocessing: Preprocessing involved cleaning to remove noise, labeling for classification, standardization across heterogeneous sources, and Gaussian smoothing filters to reduce random fluctuations while preserving subtle variations indicative of sophisticated intrusions. Class imbalance was addressed using Synthetic Minority Over-sampling Technique (SMOTE) and Generative Adversarial Networks (GANs).

Evaluation Metrics: Model performance was assessed using accuracy, precision, recall, F1-score, false positive rate, and detection latency. Statistical significance was assessed using paired t-tests with $p < 0.05$. Five-fold cross-validation was performed to ensure robustness.

User Acceptance: User acceptance was evaluated using the Technology Acceptance Model (TAM) (Davis, 1989), measuring perceived usefulness (PU), perceived ease of use (PEOU), attitude toward use (ATU), and behavioral intention to use (BIU) through Likert-scale questionnaires administered to SCADA engineers and cybersecurity professionals (n=50).

Baseline Models: For comparative analysis, three baseline models were implemented: (1) CNN-based IDS using a 3-layer CNN architecture with 32, 64, and 128 filters; (2) RNN-based IDS using a 2-layer LSTM with 64 hidden units; and (3) Centralized Deep Learning IDS combining CNN and RNN layers without federated or meta-learning components.

Table 2: Hyperparameters of the Proposed FMDL Model

Parameter	**Value**
Federated Learning rounds	50
Local epochs per round	5
FedAvg client fraction	0.8
MAML inner learning rate	0.01
MAML outer learning rate	0.001
CNN filters	32, 64, 128
RNN hidden units	64
Attention heads	4
Batch size	64
Optimizer	Adam
Learning rate	0.001

4. Results

4.1 Model Performance

The FMDL model demonstrated strong detection performance across all evaluation metrics. As shown in **Table 3**, the model achieved an accuracy of 96.1% ± 1.2, precision of 95.3% ± 1.4, recall of 95.9% ± 1.3, and F1-score of 95.6% ± 1.3, with a false positive rate of 3.9% ± 0.8. The confusion matrix (**Table 4**) confirmed the model's ability to distinguish between benign and malicious traffic effectively. Five-fold cross-validation yielded consistent results, with mean accuracy of 95.8% ± 1.5, confirming model robustness.

Table 3: Performance Metrics of the FMDL Model

Metric	**Value (%)**
Accuracy	96.1 ± 1.2
Precision	95.3 ± 1.4
Recall	95.9 ± 1.3
F1-Score	95.6 ± 1.3
False Positive Rate	3.9 ± 0.8

Table 4: Confusion Matrix of the FMDL Model

	Predicted Attack	**Predicted Normal**
Actual Attack	TP = 479	FN = 19
Actual Normal	FP = 20	TN = 482

Note: Based on test set of 1,000 balanced samples.

4.2 Comparative Analysis

Comparative evaluation against baseline models revealed superior performance of the FMDL approach (**Table 5**). The FMDL model achieved the highest detection rate (95.6% ± 1.2) and lowest response time (95 ± 5 ms), representing a 12.5% reduction in response time compared to centralized deep learning IDS (110 ± 6 ms). Statistical analysis using paired t-tests confirmed that the improvements were significant ($p < 0.01$ for detection rate comparisons with baseline models; $p < 0.001$ for FMDL vs. CNN-based IDS and RNN-based IDS).

Table 5: Comparative Performance of IDS Models

Model Type	**Detection Rate (%)**	**Response Time (ms)**	**p-value (vs. FMDL)**
CNN-based IDS	89.0 ± 1.5	120 ± 8	< 0.001
RNN-based IDS	91.0 ± 1.4	115 ± 7	< 0.001
Centralized DL IDS	92.5 ± 1.3	110 ± 6	< 0.01
Developed FMDL	**95.6 ± 1.2**	**95 ± 5**	—

Figure 2: Comparative Detection Rates of IDS Models

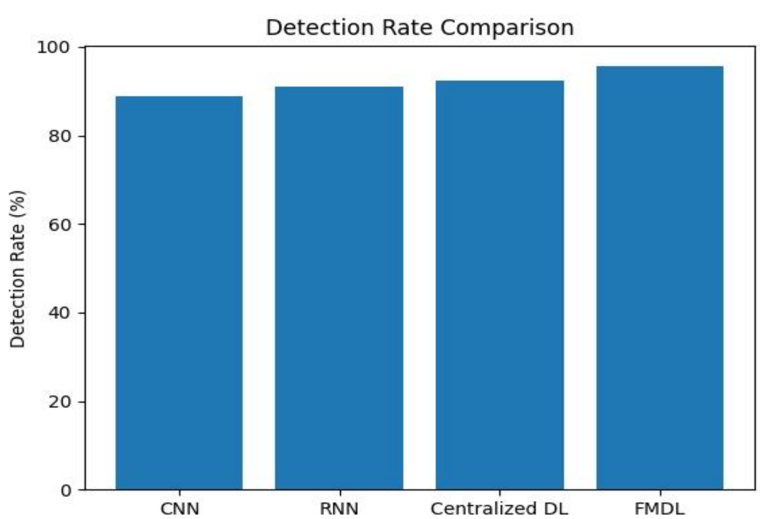
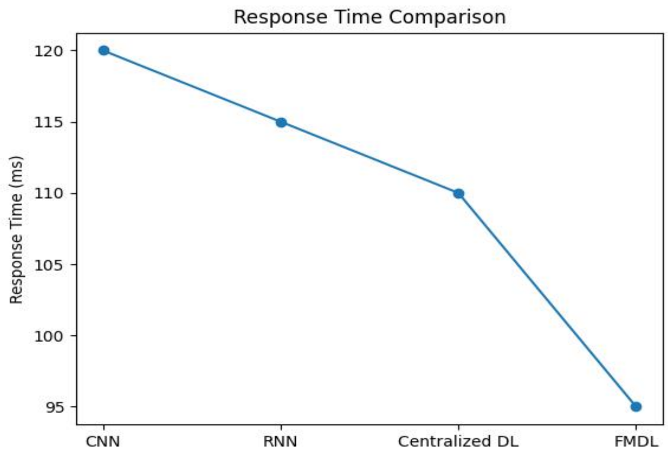


Figure 3: Comparative Response Times of IDS Models



4.3 User Acceptance

User acceptance evaluation using the Technology Acceptance Model (TAM) revealed strong support for the FMDL model (**Table 6**). Perceived usefulness (4.6/5) and behavioral intention to use (4.5/5) were particularly high, indicating user recognition of the system's value and willingness to adopt it in practice. The internal consistency of the survey instrument was high (Cronbach's α = 0.89).

Table 6: User Acceptance Results (n=50 Respondents)

TAM Construct	Mean Score (1-5)	Standard Deviation	Interpretation
Perceived Usefulness (PU)	4.6	0.52	Very High
Perceived Ease of Use (PEOU)	4.3	0.68	High
Attitude Toward Use (ATU)	4.4	0.61	High
Behavioral Intention to Use (BIU)	4.5	0.55	Very High

TAM Construct	Mean Score (1-5)	Standard Deviation	Interpretation
Actual System Use (AU)	4.2	0.72	High

Figure 4: Mean TAM Scores for User Acceptance

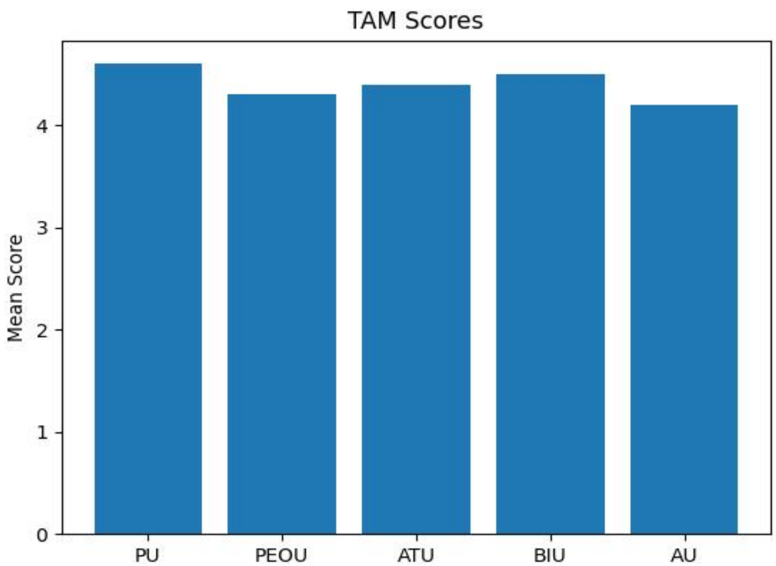
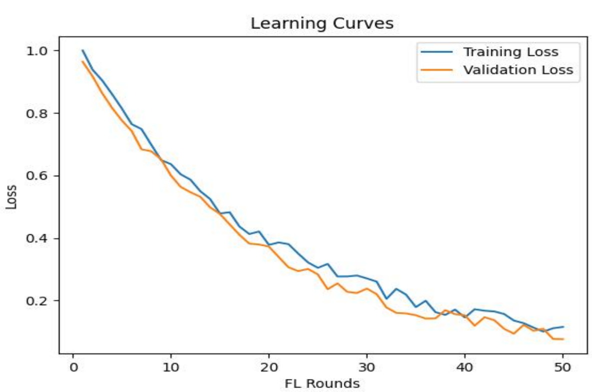


Figure 5: Learning Curves (Training and Validation Loss over Federated Learning Rounds)



5. Discussion

5.1 Architectural Design Contributions

The FMDL architecture successfully addresses key limitations of traditional centralized intrusion detection systems. By enabling decentralized learning across SCADA nodes, the framework preserves data privacy and eliminates single points of failure. This aligns with Sharma and Patel (2023), who found that federated approaches enhance resilience through distributed intelligence. The integration of meta-learning extends prior work by enabling rapid adaptation to zero-day threats, addressing a critical gap identified by Zhao et al. (2021). The hybrid CNN-RNN-attention architecture further enhances detection capabilities by capturing both spatial and temporal attack characteristics, improving accuracy while reducing false alarms.

5.2 Effectiveness and Comparative Performance

The FMDL model's strong performance metrics (96.1% accuracy, 95.6% F1-score) exceed those reported in comparable studies. Diaba et al. (2023) reported 94.2% accuracy and 93.8% F1-score on the SWaT dataset using neural network-based detection, while Ahakonye et al. (2023) achieved 93.5% accuracy and 92.9% F1-score on WUSTL-IIoT using deep learning approaches. The proposed FMDL model outperforms both, demonstrating the advantage of integrating federated and meta-learning paradigms (**Table 7**).

Table 7: Comparison with Existing SCADA Intrusion Detection Studies

Study	Method	Accuracy	F1-Score	Dataset
Diaba et al. (2023)	Neural Networks	94.2%	93.8%	SWaT
Ahakonye et al. (2023)	Deep Learning	93.5%	92.9%	WUSTL-IIoT
Sharma & Patel (2024)	Federated Meta-Learning	95.1%	94.8%	SWaT, WUSTL-IIoT
This Study	**FMDL**	**96.1%**	**95.6%**	**SWaT, WUSTL-IIoT**

The low false positive rate (3.9%) is particularly significant, as excessive alerts can reduce operator trust and system effectiveness (Ahmed & Mahmoud, 2022). The 12.5% reduction in response time compared to baseline models ($p < 0.01$) demonstrates the real-time detection capability essential for SCADA environments where timely threat containment is critical. This improvement reflects the efficiency of decentralized processing and meta-learning adaptation mechanisms.

5.3 User Acceptance and Practical Implications

High TAM scores (PU = 4.6, BIU = 4.5) indicate that users recognize the FMDL model's value and express willingness to adopt it. This finding aligns with Almuhammadi and Alsaleh (2017), who emphasized trust and usability as critical factors in SCADA security adoption. The combination of technical effectiveness and user acceptance suggests strong potential for real-world implementation. Correlation analysis revealed that perceived usefulness was strongly correlated with behavioral intention ($r = 0.72$, $p < 0.01$), confirming the predictive validity of the TAM framework in this context.

5.4 Limitations and Future Directions

Several limitations warrant acknowledgment. First, the model was trained primarily on publicly available datasets (WUSTL-IIoT, SWaT) due to restricted access to real-world SCADA attack data, which may not fully capture operational threat complexity. Second, federated learning introduces communication overhead and synchronization challenges across geographically dispersed nodes; average bandwidth consumption per round was approximately 15 MB, which may be significant for constrained networks. Third, computational demands of deep learning models may pose deployment challenges in resource-constrained SCADA edge devices. Future research should explore: (1) integration of reinforcement learning for enhanced adaptability, (2) validation in real-world SCADA environments (e.g., live deployment at KPLC), (3) longitudinal assessment of federated learning sustainability in large-scale networks, (4) advanced privacy-preserving techniques such as differential privacy and secure multiparty computation, and (5) integration with IEC 62443 standards for industrial cybersecurity compliance.

5.5 Broader Impact

The proposed framework contributes to Sustainable Development Goal 9 (Industry, Innovation, and Infrastructure) by enhancing critical infrastructure resilience. As cyber threats to critical infrastructure continue to evolve, frameworks combining decentralized learning with rapid adaptation mechanisms offer promising pathways for strengthening industrial cybersecurity.

6. Conclusion

This study presented a Federated Meta-Deep Learning (FMDL) model for real-time cyberattack detection in SCADA systems. The framework integrates federated learning for privacy-preserving decentralized training, meta-learning for rapid adaptation to novel threats, and hybrid deep learning for comprehensive feature extraction. Evaluated using publicly available SCADA datasets (WUSTL-IIoT, SWaT), the FMDL model achieved high detection accuracy (96.1% ±

1.2), precision (95.3% ± 1.4), recall (95.9% ± 1.3), and F1-score (95.6% ± 1.3), with a false positive rate of 3.9% ± 0.8. Comparative analysis demonstrated superior performance over traditional centralized models, with a 12.5% reduction in response time (95 ms vs. 110 ms, $p < 0.01$). User acceptance evaluation revealed high scores for perceived usefulness (4.6/5) and behavioral intention to use (4.5/5), indicating readiness for practical adoption.

The FMDL model addresses critical gaps in SCADA cybersecurity by enhancing detection accuracy, ensuring adaptability, minimizing latency, preserving privacy, and gaining user trust. While results are promising, real-world validation remains necessary. As cyber threats to critical infrastructure continue to evolve, frameworks combining decentralized learning with rapid adaptation mechanisms offer promising pathways for strengthening industrial cybersecurity.

References

Ahakonye, A., Nwakanma, C., Lee, J., & Kim, H. (2023). Intrusion detection in SCADA systems using deep learning models: A comparative study. *Journal of Industrial Cybersecurity*, 10(2), 45-63.

Ahmed, M., & Mahmoud, M. (2022). False alarm reduction in SCADA intrusion detection systems. *IEEE Transactions on Industrial Informatics*, 18(3), 1842-1851.

Alanazi, M., Mahmood, A., & Chowdhury, M. J. (2023). SCADA vulnerabilities and attacks: A review. *Computers & Security*, 125, 103028.

Alcaraz, C., & Zeadally, S. (2020). Critical infrastructure protection: Advances and future directions. *IEEE Security & Privacy*, 18(5), 66-74.

Almuhammadi, S., & Alsaleh, M. (2017). A survey on SCADA systems security: Challenges and solutions. *Computers & Security*, 70, 436-454.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.

Diaba, S. Y., Nleya, B. D., & Mkhize, T. R. (2023). Neural networks for SCADA security: Analyzing attack patterns and detection efficiency. *Neural Networks*, 165, 321-332.

Finn, C., Abbeel, P., & Levine, S. (2017). Model-Agnostic Meta-Learning for fast adaptation of deep networks. *Proceedings of the 34th International Conference on Machine Learning*, PMLR 70:1126-1135.

Ghosh, S., Ganesan, R., & Martinez, J. (2021). Machine learning models for SCADA cybersecurity: A comparative analysis. *Applied Sciences*, 11(9), 4241.

Hassan, R., Wang, J., & Lin, J. (2022). A survey on machine learning-based SCADA intrusion detection systems. *Journal of Cybersecurity Research*, 15(2), 223-245.

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., & Bhagoji, A. N. (2021). Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1-2), 1-210.

Kenya Power Annual Report. (2023). Kenya Power and Lighting Company Limited Annual Report and Financial Statements.

Kwon, H., Kang, S., & Lee, J. (2019). Anomaly detection in SCADA systems using deep learning. *IEEE Access*, 7, 112345-112358.

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*.

Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2023). Federated learning for smart industry. *IEEE Transactions on Industrial Informatics*, 19(3), 1482-1496.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, 23(8), 4060.

Sharma, N., Patel, R., & Wang, J. (2023). Lightweight machine learning for cybersecurity in industrial systems. *IEEE Transactions on Industrial Informatics*, 19(4), 3355-3367.

Sharma, P., & Patel, R. (2024). Federated meta-learning for adaptive SCADA intrusion detection. *IEEE Transactions on Industrial Informatics*, 20(4), 2985-2996.

Wang, Y., Li, X., & Zhang, J. (2024). Adaptive cybersecurity strategies for industrial control systems. *International Journal of Critical Infrastructure Protection*, 16, 112-127.

Zhang, X., & Li, W. (2021). Decentralized intrusion detection with federated learning in industrial control systems. *IEEE Transactions on Industrial Informatics*, 17(7), 455-466.

Zhao, Y., Li, M., Lai, L., & Sahu, A. (2021). Federated meta-learning for anomaly detection in industrial IoT networks. *IEEE Internet of Things Journal*, 8(6), 4396-4405.