SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Cross-Domain Adaptation Of Intelligent Systems In Heterogeneous Environments

Dr. Pallavi Jamsandekar[1], Tanveer Ahmad Wani[2], Vijayshree Khugshal[3], Dr. Prakash Kuppuswamy[4], Nivetha N[5], Manjula R[6], Dr. S. T. Santhanalakshmi[7], Danish Kundra[8]

[1] Professor and I/C Director, Department of Computer Application, Bharati Vidyapeeth (Deemed to be University) Institute of Management and Rural Development Administration, Sangli, Maharashtra, India. Email: pallavi.jamsandekar@bharatividyapeeth.edu ORCID: 0000-0001-5342-2024100
[2] Department of Physics, Noida International University, Greater Noida, Uttar Pradesh 203201, India. Email: tanveer.ahmad@niu.edu.in
[3] Assistant Professor, Department of Computer Application, Dev Bhoomi Uttarakhand University, Dehradun, Uttarakhand, India. Email: socse.vijayshree@dbuu.ac.in ORCID: 0009-0002-0277-2154
[4] Professor, Department of Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India. Email: prakashcnet@gmail.com ORCID: 0000-0001-9804-8835
[5] Assistant Professor, Department of Computer Science, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, India. Email: nivethan@maher.ac.in
[6] Assistant Professor, Department of Commerce, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, India. Email: manjular@maher.ac.in
[7] Assistant Professor Grade I, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu, India. Email: santhanalakshmi.peccse2024@gmail.com ORCID: 0000-0002-1377-1408
[8] Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab 140401, India. Email: danish.kundra.orp@chitkara.edu.in ORCID: 0009-0004-1739-8219

Abstract
Contemporary intelligent systems are increasingly being deployed in heterogeneous settings such as the Internet of Things (IoT) and Industrial Internet of things (IIoT), which are fraught with differences in protocols, traffic flows, data patterns, etc., making adaptation extremely difficult for the models. However, the current learning models are highly dependent on the underlying data, and consequently, it is difficult to expand to other data. The goal of this research is to improve domain-invariant knowledge transfer and generalization in heterogeneous systems using an effective and generalized cross-domain adaptive learning model. In order to provide a transportable domain invariant representation, an intelligent kernel search recurrent neural network (Int-KS-RNN) is proposed. It is based on recurrent neural networks (RNNs), which describe temporal correlations, and increased feature mapping using intelligent kernel search (Int-KS). By using Min-max normalization to scale down each individual input feature, input values are converged faster, through independent component analysis (ICA), which captures statistically independent and compact domain-invariant features that enhance effective generalization in heterogeneous systems while avoiding redundancy. Simulation is performed in Python to demonstrate stability across heterogeneous datasets with the best performance (detection rate (98.46%), high accuracy (98.48%), F1 score (0.98), and AUC (0.9828) and a very low rate of false alarms (0.72%), compared with the existing model. The suggested model provides a dependable, generalized, and extendable way to increase adaptability for intelligent systems deployment in complicated, diverse contexts.

Keywords: Cross-Domain Adaptation, Intelligent Systems, Heterogeneous Environments, Recurrent Neural Networks, Kernel Optimization.

1. INTRODUCTION

The unprecedented exponential rise of Internet of Things (IoT) and Industrial Internet of Things (IIoT) technologies is turning modern intelligent systems into a complex, interconnected network of data-driven ecosystems [1]. Modern smart manufacturing, industrial automation, and critical infrastructure monitoring systems are continually and automatically collecting enormous quantities of heterogeneous data streams

generated from a multitude of IoT/IIoT devices with varying network configurations, protocols, and under different environments [2, 3]. Even though recently developed Artificial Intelligence (AI) methods significantly enhanced the capabilities of data analytics and system decision making, the robustness of intelligent systems under heterogeneous settings still has a bottleneck issue [4]. The performance drops of intelligent models at out-of-distribution sites compared to performance at training sites are quite drastic, largely because of changes in data distributions and characteristics, as well as network behavioral trends. It's inevitable for intelligent systems with scalability to address the domain shift problem; hence, domain adaptation is an important strategy to handle various heterogeneous situations [5]. Heterogeneous situations cause various kinds of shifts which result in a negative impact on learning performance, diminish prediction capability, and raise the number of false alarm rates [6]. These challenges are especially important for IIoT/IoT systems where varying traffic patterns and conditions are common, and adaptive mechanisms that leverage cross-domain knowledge transfer learning to mitigate catastrophic forgetting are demanded [7, 8]. Thus, a more desirable requirement is the learned feature representations that can be invariant across domains but at the same time able to preserve discriminative information to distinguish among classes [9]. Numerous commonly used learning methods, like machine learning classifiers, deep neural networks, and recurrent learning models, could learn reasonably well on a single dataset [9]. However, typical approaches of supervised learning are biased toward the training domain. Limited transferability of models across domains is observed. Besides, most models can't generalize well on out-of-distribution data, with insufficient feature representation and vulnerability to domain shift [10]. To overcome these limitations, this research proposes an Int-KS-RNN model for cross-domain adaptation. It integrates ICA for extracting compact domain-invariant features and an intelligent kernel search mechanism for optimizing feature representation and knowledge transfer. By combining kernel-driven optimization with recurrent temporal learning, the proposed model enhances adaptability, improves cross-domain generalization, and provides a scalable solution for intelligent systems operating in heterogeneous environments.

The rest of this research is divided into the following parts. Part 2 surveys previous research and highlights research gaps of cross-domain intrusion detection for heterogeneous environments. Part 3 details the Int-KS-RNN model for adaptive feature learning and domain adaptation. Part 4 describes the experimental settings, presents the performance results, and the comparison with previous work. Part 5 concludes this work and provides some perspectives on future work.

2. LITERATURE REVIEW

Recent research on cross-domain adaptation have dedicated on enhancing the model's generalization ability across heterogeneous environments. Decoupling Feature Alignment (DFA) [11] with Mean-Covariance Adjustment Feature Alignment (MCAFA) and Data Decoupling (DD) was presented to handle unsupervised domain adaptation under a non-independent and identically distributed environment. High feature alignment and adaptation accuracy were obtained, but performance was dependent on the domain's characteristics and paid for increased computational complexity. Hint Sense [12] improved semantic interoperability on Internet of Things (IoT) environments based on a blend of Resource Description Framework (RDF), Graph Neural Network Optimization with Squeeze-and-Excitation-based ResNeXt (GO-SER), and Machine-to-Machine Measurement (M3) reasoning. This model has improved throughput and accuracy while reducing computational overheads, although it introduces higher structural complexities and relies on ontology-based knowledge representations. The multi-stream classification framework proposed in [13] maps heterogeneous data from different domains into a shared latent feature space, thereby enabling effective cross-domain classification of unlabeled target-domain samples. It attained higher classification accuracy than existing approaches on various benchmarks, but there were still obstacles concerning the computation of the algorithm and the generalization ability with high heterogeneous feature distribution. Regarding the task of cross-domain detection, proposed a step-wise domain-adaptive You Only Look Once (YOLO) framework [14], incorporating the aid of auxiliary domain construction and multiple domain adaptation techniques, showing substantial improvement in the detection performance of several multi-source datasets, but subject to synthetic domain generation and extensive training costs. Recently, Open-set Federated Adversarial Domain Adaptation (OS-FADA) [15] proposed a fault diagnosis scheme based on federated learning and adversarial adaptation methods for privacy protection, and it was improved by about 20%. However, the communication cost, scalability, and complexity of implementation were this models' problem. An adversarial AI based on domain invariant learning was proposed to enhance cross-user Human Activity Recognition from WiFi Channel State Information (CSI) signals [16]. The system produced better recognition results and less simulation time, but was hard to generalize across the environment. A CNN-based IDS integrated with SHapley Additive explanations (SHAP) [17] enhances the performance for cross-dataset attack detection and improves

interpretability; Nevertheless, computational overhead and adaptation for unseen attacks are limitations to the deployment. Features Reduction and ML approaches were researched for Network Intrusion Detection System (NIDS) across multiple datasets using Autoencoder (AE), LDA, and Machine Learning (ML) models in [18], showing that dataset-specific features were generated, but no general features were obtained for those features.

3. METHODOLOGY

The suggested method intends to identify intrusions in these heterogeneous networks by performing efficient and reliable cross-domain adaptation to overcome the difficulties presented by the IoT and IIoT environments. As shown in Figure 1, the approach effectively decreases the domain shift while guaranteeing system dependability and lowering the computational cost by utilizing multi-domain learning and recurrent modeling that adapt to network fluctuations.

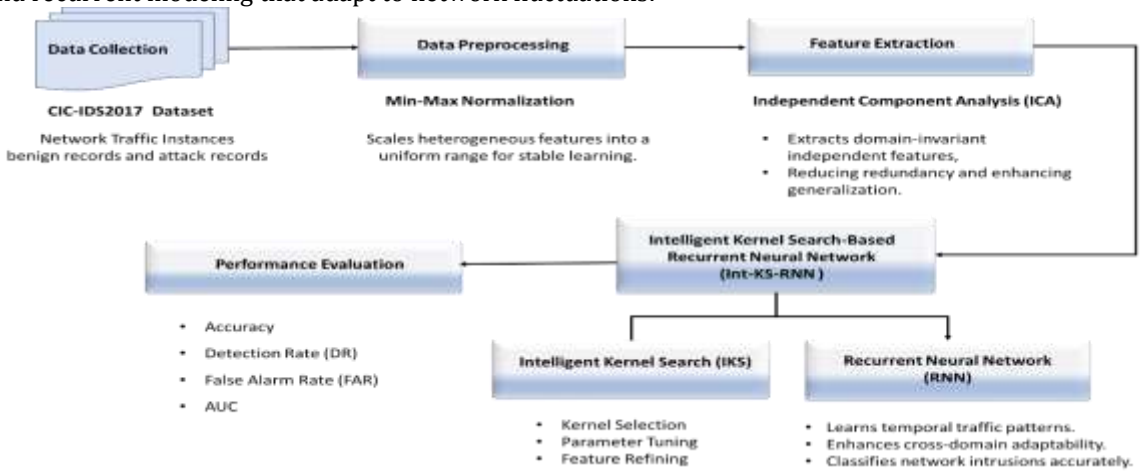

Figure 1: Proposed Int-KS-RNN Methodology for Cross-Domain Adaptation

3.1 Data Collection

The experiments used the CIC-IDS2017 data, from a Kaggle source (https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset). The total instances of network traffic: benign and malicious attack instances. There are several classes of attack, which include the web attack, infiltration attack, brute force, DoS attack/DDoS attack, Botnet attack, and portScan attack that were collected for consecutive days. The CIC-IDS2017 data is appropriate for evaluating the cross-domain transfer capacity and generalization of the intelligent intrusion detection models, and it provides a wide range of traffic behavior features. To train and evaluate the proposed model, the dataset was partitioned into training and testing subsets using an 80:20 ratio, where 80% of the samples were used for model training and 20% were reserved for performance evaluation.

3.2 Min-Max Normalization for Feature Standardization

The normalization transforms each feature value in the heterogeneous dataset, including network traffic statistics, sensor readings, and temporal attributes, into a unified range between 0 and 1 using Equation (1).

$$y_{norms} = \frac{y - y_{min}}{y_{max} - y_{min}} \quad (1)$$

Here, y_{norms} represents the normalized feature value within the range [0, 1], while y denotes the original feature value extracted from the dataset. The terms y_{min} and y_{max} show the dataset's features' lowest and highest values. Ensures uniform feature scaling, reduces bias, and improves training stability in the proposed model.

3.3 ICA for Feature Extraction

ICA is used in the proposed research to extract statistically independent and domain-invariant features from heterogeneous data. It decomposes observed multivariate signals into underlying independent components, reducing redundancy and improving feature separability across different domains. Given the observed vector w(s), ICA assumes a linear mixture model (2):

$$w(s) = Bt(s) \quad (2)$$

where B is the mixing matrix representing data fusion across heterogeneous sources, and t(s) represents independent source signals, representing underlying domain-invariant features. The objective is to estimate the source signals using a demixing matrix X calculated as (3):

$$z = Xw \quad (3)$$

where $X = B - 1$ and z denotes the resulting domain-invariant independent components used for kernel optimization and recurrent learning, and w represents the projection (weight) vector used to identify statistically independent components. Statistical independence is typically enforced by maximizing non-Gaussianity. Statistical independence is typically enforced by maximizing non-Gaussianity. Classical kurtosis is defined as (4); however, due to sensitivity to outliers in IoT/IIoT data, a robust quantile-based kurtosis is preferred (5):

$$\beta_1 = \frac{F(w-\mu)^4}{(F(w-\mu)^2} - 3 = \frac{\mu_4}{\sigma^4} - 3 \quad (4)$$

$$\text{Kurtosis} = \frac{(F_7 - F_5) + (F_3 - F_1)}{(F_6 - F_2)} \quad (5)$$

Where w denotes heterogeneous feature values, μ is the mean, and F(·) is the expectation. β measures ICA-based non-Gaussianity. $F_1 - F_7$represent octiles of the feature distribution. The quantile-based kurtosis provides robust outlier handling, supporting stable ICA feature extraction for cross-domain learning in the proposed model.

3.4 Intelligent Kernel Search Recurrent Neural Network (Int-KS-RNN) for Cross-Domain Adaptive Learning

The proposed Int-KS-RNN pipeline starts with a wide-ranging heterogeneous dataset collected from multiple domains. To ensure that all features are similar, Min-Max normalization is first applied to this diverse range of datasets. After that, ICA is used with the intent of obtaining compact and statistically independent feature representations. The features collected through the ICA procedure are then processed using Int-KS to discover appropriate kernel mappings and extract feature representations with respectable domain invariant abilities. Later, the RNN model incorporates the dynamic information within time series, allowing it to predict and classify effectively in the new domain, showing that Int-KS-RNN outperforms others in the presence of drift and heterogeneous domains.

3.4.1 RNN for Temporal Dependency Modeling

Unlike feedforward networks, which cannot learn the dynamics of input sequences, RNNs are employed in the proposed model to capture the temporal reliance of sequential streams on heterogeneous settings. RNN maintains history information via dynamic history-hidden states and can learn from temporal sequences of network traffic and data collected from sensors. Let $w^{\langle s \rangle}$ represent the input feature vector obtained after ICA-based feature extraction and kernel optimization. The hidden state $g^{\langle s \rangle}$ is updated as (6):

$$g^{\langle s \rangle} = \begin{cases} p & \text{if } s = 0 \\ e_1\left(g^{\langle s-1 \rangle}, w^{\langle s \rangle}\right) & \text{otherwise} \end{cases} \quad (6)$$

Where $g^{\langle s \rangle}$ is the RNN hidden state capturing temporal dependencies; p is the initial state; s denotes time step; e_1 is activation; $g^{\langle s-1 \rangle}$is the previous state; $w^{\langle s \rangle}$ is the ICA and kernel-optimized input feature vector. The hidden state evolution can be further expressed in Equation (7):

$$g^{\langle s \rangle} = e_1\left(vg^{\langle s-1 \rangle} + xw^{\langle s \rangle} + a_g\right) \quad (7)$$

In Equation (6), $g^{\langle s \rangle}$ represents temporal state learning in the current hidden state, $g^{\langle s-1 \rangle}$ represents past cross-domain memory, $w^{\langle s \rangle}$represents optimized features, v and x recurrent/input weights, a_g bias, and $e_1$nonlinear activation.Finally, the output at time step s is computed using Equation (8):

$$z^{\langle s \rangle} = e_2\left(og^{\langle s \rangle} + a_z\right) \quad (8)$$

where $z^{\langle s \rangle}$is the output vector at time steps, $g^{\langle s \rangle}$ is the RNN hidden state, bias is represented by a_z, the output weight matrix by o, and the activation function generating classification probabilities is represented by $e_2(\cdot)$. This formulation enables the RNN component within the Int-KS-RNN model to effectively capture sequential dependencies while supporting robust learning across heterogeneous and non-stationary environments.

3.4.2 Int-KSO for Kernel Parameter Optimization

KSO is a population-based metaheuristic used for kernel optimization through exploration, search, and selection of candidate solutions, as shown in Figure 2. In this research, it is adopted for its ability to handle high-dimensional, non-linear data and support cross-domain feature learning. But local utilization alone is not sufficient in a heterogeneous situation, where kernel refining can be impacted, so differential evolution is incorporated into the local search to further improve the kernel refinement and overall performance. Differential Evolution (DE) enhances solution refinement through mutation, crossover, and selection mechanisms. The mutation operation is defined in Equation (9):

$$u_j = w_{q1} + E_n(w_{q2} - w_{q3}) \quad (9)$$

u_j is the mutated kernel solution in Int-KS-RNN; w_{q1}, w_{q2} and w_{q3} are randomly selected population kernel vectors, and E_n controls mutation strength, enabling balanced exploration and exploitation in heterogeneous cross-domain optimization. The crossover process is given in Equation (10):

$$v_{j,i} = \begin{cases} u_{j,i}, \text{if} rand < CRorrandj(1-C) = i \\ w_{j,i}, \text{if} rand > CRorrandj(1-C) \neq i \end{cases} \quad (10)$$

$v_{j,i}$ is the trial kernel vector generated during crossover in Int-KSO, $u_{j,i}$ is the DE-mutated kernel candidate, and $w_{j,i}$) represents the original KSO population solution. j and i denote population and feature indices. CR is the crossover rate, (rand) introduces stochastic kernel exploration, $randj(1-C)$ ensures mutation inheritance, and C defines kernel space dimensionality in Int-KS-RNN. The selection strategy is defined in Equation (11):

$$w_{j+1} = \begin{cases} w_j, \text{if} e(v_j) > e(w_j) \\ v_j \text{ . others} \end{cases} \quad (11)$$

w_j current kernel configuration in Int-KS-RNN for cross-domain feature mapping; $e(w_j)$ refined KSO solution; v_j DE-generated trial solution; $e(v_j)$ fitness measuring kernel effectiveness for cross-domain adaptation (accuracy/generalization); w_{j+1} updated Int-KS solution for improved feature transformation. The proposed Int-KS-RNN achieves reliable cross-domain learning by effectively handling heterogeneous feature distributions in heterogeneous environments. It delivers improved robustness and generalization under domain shift with stable predictive performance.

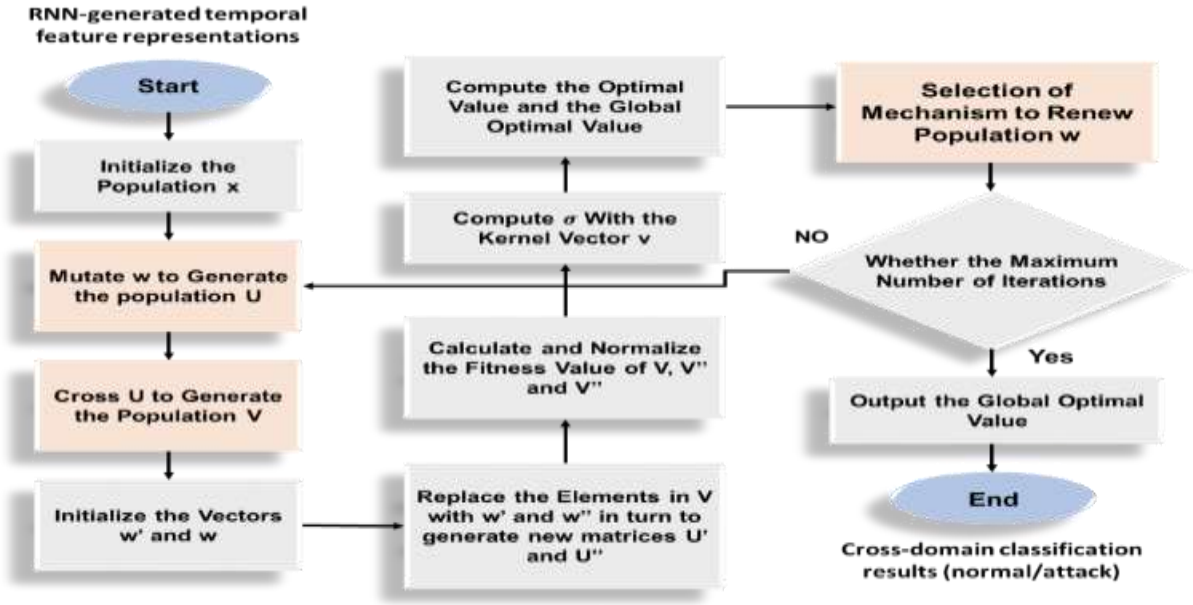

Figure 2: Int-KSO Workflow for Cross-Domain Adaptive Feature Optimization

4. RESULTS

The suggested Int-KS-RNN model was built with Python 3.10. The CSE-CIC-IDS2018 dataset, which includes benign traffic as well as several cyberattack categories, was used for experimental evaluation. The model is trained using 34 features as input, with 2 recurrent layers of 128 hidden units, with a batch size of 32, learning_rate = 0.001, and trained with 100 epochs with performance metrics, and validated.

The proposed Int-KS-RNN model demonstrates strong adaptability and reliability across heterogeneous IoT environments characterized by significant cross-domain variations. The domain-level environment analysis and corresponding reliability heat map presented in Figure 3(a) reveal the model's capability to maintain stable feature representations despite environmental differences among domains. The model achieves high feature stability of approximately 78–79% and communication reliability of about 86%, indicating effective domain adaptation performance. Computational efficiency is further evaluated through CPU utilization under varying traffic conditions, as shown in Figure 3(b). CPU consumption increases from 30.5% during normal operation to 57.0% under unstable traffic states, reflecting the additional processing demands associated with heavier workloads. Despite this increase, the model maintains stable computational behavior, demonstrating its ability to operate efficiently in dynamic and resource-intensive scenarios. These results confirm the feasibility, robustness, and scalability of the proposed Int-KS-RNN framework for supporting large-scale IoT deployments in heterogeneous environments.

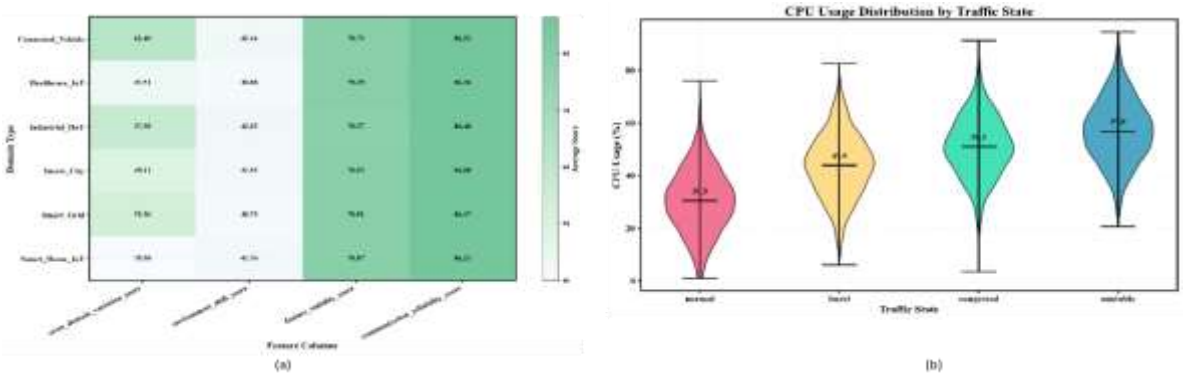

Figure 3: Domain Adaptation and Resource Utilization Analysis of Int-KS-RNN (a) Domain Adaptation Reliability Analysis, and (b) CPU Utilization under Diverse Traffic Conditions

4.1 Performance Comparison

To illustrate the efficacy of the proposed model in detecting attacks, this model is tested against existing standard machine learning and deep learning classifiers in the literature, such as Convolutional Neural Network (CNN), K-Nearest Neighbors (KNN) [17], and Deep Feed Forward, Decision Tree (DT) [18]. The assessment metrics are as follows. **Accuracy** measures the general efficiency and overall accuracy regarding both classifications of benign traffic and attack. **F1-Score** determines the balance between recall and precision, reflecting the overall stability and reliability of the detector's classification performance. **Detection Rate (DR)** represents how well each detection method can successfully discriminate the attack traffic, to obtain a high coverage rate in detecting any attack in cross-domain situations. **False Alarm Rate (FAR)** calculates the fraction of false positives, where the lower values reflect the reliability of detecting attacks. **Area under the Curve (AUC)** shows the separability of positive classes from negative classes, representing the model's ability to generalize across disparate datasets. As suggested in Table 1, Int-KS-RNN achieves the best performance in accuracy (98.48%), resulting from the adaptation mapping through kernel-space optimization, decorrelation of statistical independence features using ICA, and modeling on sequentially of intrusions through time across a diversified range of domains.

Table 1: Accuracy Comparison of Existing and Proposed Models

Model	Accuracy (%)
KNN [17]	96.93
CNN [17]	96.18
DFF [18]	96.11
DT [18]	98.15
Int-KS-RNN [Proposed]	98.48

Table 2 and Figure 4 reveal that the proposed Int-KS-RNN exhibits the top F1-Score (0.98) and effectively strikes a better balance between precision and recall, which is encouraging. Moreover, the significantly enhanced DR (98.46%) proves that the proposed model is able to detect more maliciously behaving flows, and performs well across domains, while the much lower FAR (0.72%) shows improved robustness on the non-malicious traffic classification. Besides that, the outstanding AUC value (0.9828) proves significant reparability and domain-invariance learning property.

Table 2: Cross-Domain Performance Comparison of Proposed with Baseline Models

Model	F1-Score	DR (%)	FAR (%)	AUC
DFF [18]	0.86	81.83	1.39	0.9504
DT [18]	0.94	94.94	1.29	0.9683
Int-KS-RNN [Proposed]	0.98	98.46	0.72	0.9828

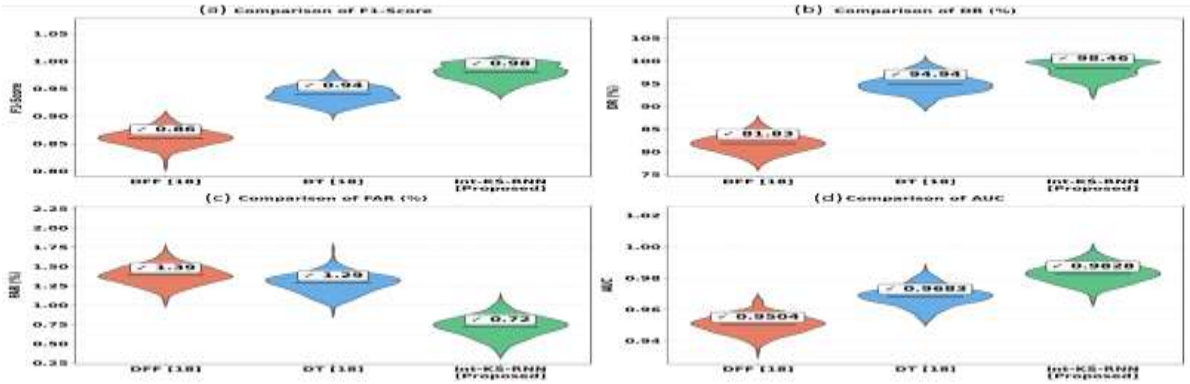

Figure 4: Performance Evaluation of Proposed Int-KS-RNN for Cross-Domain Adaptive Intrusion Detection (a) F1-score, (b) DR, (c) FAR, and (d) AUC

To ensure a fair and unbiased comparison, K-Nearest Neighbors (KNN), Convolutional Neural Network (CNN) [17], Deep Feedforward Network (DFF), and Decision Tree (DT) [18] models were implemented and evaluated under identical experimental conditions, utilizing the CIC-IDS2017 dataset and an 80:20 training–testing data partition. Table 3 demonstrates that the proposed Int-KS-RNN model outperforms KNN, CNN, DFF, and DT across all evaluation metrics, achieving the highest accuracy (98.48%). Furthermore, the model records the lowest false alarm rate (0.72%), highlighting its effectiveness and reliability for cross-domain recommendation on the proposed dataset.

Table 3: Performance Evaluation of Cross-Domain Recommendation on Proposed Dataset

Model	Accuracy (%)	F1-Score	DR (%)	FAR (%)	AUC
KNN	96.70	0.94	95.60	1.50	0.9610
CNN	96.05	0.93	94.50	1.55	0.9575
DFF	95.90	0.85	81.20	1.42	0.9490
DT	97.95	0.93	94.20	1.33	0.9665
Int-KS-RNN [Proposed]	98.48	0.98	98.46	0.72	0.9828

4.2 Discussion

The suggested Int-KS-RNN is intended to tackle cross-domain intrusion detection in heterogeneous networking settings through incorporating recurrent temporal learning with intelligent kernel-space optimization. This approach enables adaptive transformation of the feature space to improve generalization across the target domain, in contrast to a number of popular techniques like KNN, CNN [17], DFF, and DT [18], whose performance deteriorates under non-stationary distributions and domain shift issues. ICA ensures the decorrelation of the features to determine the statistically independent latent representation, and the intelligence in the kernel-space aids in finding the optimal adaptive discriminative mapping across heterogeneous domains, in addition to the benefit of Min-Max normalization for improved convergence stability. Results indicate that Int-KS-RNN outperforms existing methods, achieving a lower false alarm rate (0.72%) and higher accuracy (98.48%). **Practical Implication:** This proposed model provides scalable and efficient IoT, IIoT environments with improved generalization and robustness, and distributed intelligent system security based on enhanced detection rate, reduced rate of false positive alarms, and adaptive security monitoring in varied network environments.

5. CONCLUSION

An efficient and scalable cross-domain adaptation model, referred as Int-KS-RNN, is developed by coupling a recurrent neural network with intelligent kernels to extract domain-invariant features and capture spatio-temporal dependencies, enabling effective knowledge transfer across heterogeneous intelligent systems. The suggested model's efficacy and dependability are shown by extensive trials on datasets. where improved accuracy (98.48%), F1-score (0.98), detection rate (98.46%), and AUC (0.9828) are achieved, and a lower false alarm rate (0.72%) is maintained, compared with other state-of-the-art algorithms. It reveals better detection performance and a higher generalization capacity, as well as effective detection capability with a lower rate of false positives. However, its performance might vary due to dataset diversity and kernel-related computational complexity. Future research may focus on lightweight kernel optimization strategies, online adaptation mechanisms, multi-domain adaptation techniques, and the integration of explainability frameworks to enhance interpretability and generalization across diverse cross-domain tasks and previously unseen scenarios.

REFERENCES

1. Javed, S.H., Ahmad, M.B., Asif, M., Almotiri, S.H., Masood, K. and Ghamdi, M.A.A., 2022. An intelligent system to detect advanced persistent threats in industrial internet of things (I-IoT). Electronics, 11(5), p.742. https://doi.org/10.3390/electronics11050742
2. Abdullahi, I., Longo, S. and Samie, M., 2024. Towards a distributed digital twin framework for predictive maintenance in industrial internet of things (IIoT). Sensors, 24(8), p.2663. https://doi.org/10.3390/s24082663
3. Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S. and Alnazzawi, N., 2025. Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. Sensors, 25(1), p.213. https://doi.org/10.3390/s25010213
4. Zhang, A., Xing, L., Zou, J. and Wu, J.C., 2022. Shifting machine learning for healthcare from development to deployment and from models to data. Nature biomedical engineering, 6(12), pp.1330-1345. https://doi.org/10.1038/s41551-022-00898-y
5. Rajawat, A.S., Goyal, S.B., Chauhan, C., Bedi, P., Prasad, M. and Jan, T., 2023. Cognitive adaptive systems for industrial internet of things using reinforcement algorithm. Electronics, 12(1), p.217. https://doi.org/10.3390/electronics12010217
6. Zuo, T.Y., Di, K., Li, P. and Jiang, Y., 2026. Autonomous domain adaptation self-optimization approach for cross-domain industrial agents. ACM Transactions on Intelligent Systems and Technology, 17(1), pp.1-25. https://doi.org/10.1145/3776560
7. Zhang, J., Zhou, Q. and Zhou, W., 2026. Domain-invariant fault representation learning for rotating machinery via causal excitation and conditional alignment. Electronics, 15(6), p.1252. https://doi.org/10.3390/electronics15061252
8. Saeed, A., A. Khan, M., Akram, U., J. Obidallah, W., Jawed, S. and Ahmad, A., 2025. Deep learning based approaches for intelligent industrial machinery health management and fault diagnosis in resource-constrained environments. Scientific Reports, 15(1), p.1114. https://doi.org/10.1038/s41598-024-79151-2
9. Przybyś-Małaczek, A., Antoniuk, I., Szymanowski, K., Kruk, M., Sieradzki, A., Dohojda, A., Szopa, P. and Kurek, J., 2024. Comparative study of conventional machine learning versus deep learning-based approaches for tool condition assessments in milling processes. Applied Sciences, 14(13), p.5913. https://doi.org/10.3390/app14135913
10. Kaliyannan, D., Thangamuthu, M., Pradeep, P., Gnansekaran, S., Rakkiyannan, J. and Pramanik, A., 2024. Tool condition monitoring in the milling process using deep learning and reinforcement learning. Journal of Sensor and Actuator Networks, 13(4), p.42. https://doi.org/10.3390/jsan13040042
11. Wen, Z., Li, Q., Wang, Y., Xu, L., Shao, H. and Sun, G., 2024. DFA: Decoupling feature alignment for unsupervised domain adaptation. IEEE Internet of Things Journal, 11(20), pp.33151-33163. https://doi.org/10.1109/JIOT.2024.3423794
12. Anitha, K., Kumar, B.M. and Prasad, K.V., 2025. Heterogeneous interoperable sensors integrating cognitive knowledge for iot-based cross-domain applications. IEEE Sensors Journal, 25(7), pp.12119-12127. https://doi.org/10.1109/JSEN.2025.3526284
13. Li, Y.F., Gao, Y., Ayoade, G., Khan, L., Singhal, A. and Thuraisingham, B., 2022. Heterogeneous domain adaptation for multistream classification on cyber threat data. IEEE Transactions on Dependable and Secure Computing, 21(1), pp.1-11.
14. Li, G., Ji, Z., Qu, X., Zhou, R. and Cao, D., 2022. Cross-domain object detection for autonomous driving: A stepwise domain adaptative YOLO approach. IEEE Transactions on intelligent vehicles, 7(3), pp.603-615.
15. Xu, S., Ma, J. and Song, D., 2023. Open-set federated adversarial domain adaptation based cross-domain fault diagnosis. Measurement Science and Technology, 34(11), p.115004. https://doi.org/10.1088/1361-6501/ace734
16. Hassan, M., Kelsey, T. and Rahman, F., 2024. Adversarial AI applied to cross-user inter-domain and intra-domain adaptation in human activity recognition using wireless signals. Plos one, 19(4), p.e0298888. https://doi.org/10.1371/journal.pone.0298888
17. Onuorah, M.O., Sun, Y. and Mashao, D., 2026. Toward Generalization and Interpretable Deep Learning–based Intrusion Detection System for Heterogeneous Network Environments. IEEE Access, 14.https://doi.org/10.1109/ACCESS.2026.3675887
18. Sarhan, M., Layeghy, S., Moustafa, N., Gallagher, M. and Portmann, M., 2024. Feature extraction for machine learning-based intrusion detection in IoT networks. Digital Communications and Networks, 10(1), pp.205-216.https://doi.org/10.1016/j.dcan.2022.08.012