An Artificial Intelligence-Driven Deep Representation Learning Model for Securing Privacy-Preserving Applications in Human–Computer Interface Systems

Hadi Oqaibi
Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
hoqaibi@kau.edu.sa (corresponding author)

Received: 25 October 2025 | Revised: 24 November 2025 and 12 December 2025 | Accepted: 13 December 2025

 DOI: https://doi.org/10.48084/etasr.15772

ABSTRACT

The rapid progression of Internet connections has led to a significant increase in cyber-attack events, often resulting in severe and disastrous consequences. Malware is one of the primary weapons used to achieve malicious objectives in cyberspace, either through the exploitation of newly discovered vulnerabilities or through the misuse of features introduced by new technologies. The development of more effective and robust malware defense mechanisms is considered a critical necessity in cybersecurity. Human–Computer Interface (HCI) systems have become increasingly important, and as communication, computing, and display technologies continue to advance, conventional HCI methods may become a bottleneck in effectively handling the growing data flow. Federated Learning (FL) is a Machine Learning (ML) paradigm that aims to train models through decentralized devices, whereas the local data are kept private. In this manuscript, a Secure and Efficient Federated Learning using Optimization Algorithms and Deep Learning for Cybersecurity Applications (SEFL-OADLCA) model is proposed for HCI systems. The aim is to present an effective FL framework to address cybersecurity issues. First, the min–max scaler method is applied for data preprocessing. For the Dimensionality Reduction (DR) process, the Mountain Gazelle Optimizer (MGO) technique is employed. Furthermore, a hybrid Temporal Convolutional Network and Long Short-Term Memory (TCN+LSTM) technique is utilized for the attack classification process. Finally, the hyperparameter selection process is performed using the Remora Optimization Algorithm (ROA) to optimize the classification results. The comparison study of the SEFL-OADLCA method portrayed a superior accuracy of 99.46% compared with existing approaches on the NSL-KDD dataset.

Keywords-Federated Learning (FL); Deep Learning (DL); cybersecurity; Human–Computer Interface (HCI); Remora Optimization Algorithm (ROA)

I. INTRODUCTION

Recently, owing to the rising dependence on the Internet of Things (IoT) and digitalization, several security incidents have occurred. Cybercrime and threats can cause destructive economic losses and impact organizations as well as individuals [1]. Therefore, organizations are required to implement and adopt robust cybersecurity models to reduce these losses. Based on existing studies, the national security of a country depends on the government, individual citizens, and businesses having access to tools and applications that are highly safeguarded [2]. Thus, effectively recognizing diverse cyber incidents, both previously unseen and known, and intelligently protecting critical systems from such cyber threats are major concerns that must be addressed urgently [3]. With the increasing importance of computers in society, Human–Computer Interface (HCI) systems have now become a progressively significant portion of everyday life [4]. During the last half-century, the Information and Communication Technology (ICT) industries have developed significantly and are widely and closely integrated with the modern world [5]. Consequently, safeguarding ICT applications and systems from cyber threats has gained significant attention from security policymakers in recent years [6]. Artificial Intelligence (AI) is gradually being integrated into cyberthreats [7]. By using ML and Deep Learning (DL), AI-driven systems can classify anomalies and identify complex cyber-threats, such as Distributed Denial-of-Service (DDoS) attacks [8]. Federated Learning (FL) is proposed as a promising ML paradigm that permits handling concerns like security, access rights, and data privacy [9]. FL presents a better solution for resolving the above restrictions of centralized Intrusion Detection Systems (IDS) while also addressing cybersecurity attacks [10].

Authors in [11] developed a recognition system using radar and DL, specifically Visual Geometry Group Network

(VGGNet). Authors in [12] explored recent advancements in Natural Language Processing (NLP) and voice recognition technologies. In [13], a dedicated token through Centralized Authentication Authority (CAA) is presented. Additionally, a two-layer token validation mechanism is introduced through the Centralized Server Firewall Authentication Layer (CSFAL) and the Authentication Authority Valuation Layer (AAVL). Authors in [14] utilized Blockchain (BC) for privacy and security, and an artificial immune system for threat detection. Authors in [15] developed a system using FL with Deep Fuzzy Clustering (DFC) and Deep Convolutional Neural Networks (DCNN) models. Authors in [16] proposed a secure Support Vector Machine (SVM) utilizing BC and homomorphic encryption. Authors in [17] proposed selective image obfuscation strategies. Authors in [18] developed an Adaptive FL Framework (AFLF) using a hierarchical edge–fog–cloud model, a Secure Data Collaboration Protocol (SDCP), an Adaptive Personalized FL Algorithm (APFLA), and gradient compression. Authors in [19] developed a system by utilizing FL. Authors in [20] presented a privacy-preserving Automatic Speech Recognition (ASR) system for children using discrete speech. Authors in [21] developed a privacy-preserving word vector learning scheme for IoT applications that enables training on encrypted data over cloud servers. Authors in [22] provided a unified review of AI, Explainable AI (XAI), and FL. The existing studies concentrate on discrete applications or depend on centralized or partially secure frameworks, resulting in privacy, scalability, and computational efficiency issues. Moreover, a research gap exists due to the lack of a unified, privacy-preserving, and resource-efficient approach.

In this manuscript, a Secure and Efficient Federated Learning using Optimization Algorithms and Deep Learning for Cybersecurity Applications (SEFL-OADLCA) model is proposed for HCI systems:

- The normalization of input data is achieved by applying the min–max scaler. This step enhances learning efficiency, data consistency, and scaling. Additionally, it reduces training time and ensures that subsequent processes are performed more effectively.
- The Mountain Gazelle Optimizer (MGO) is used for Dimensionality Reduction (DR) to select and retain critical features while also reducing complexity. Also, the Temporal Convolutional Network and Long Short-Term Memory (TCN+LSTM) model is employed for capturing both spatial and temporal patterns, thus enhancing attack detection efficiency, accuracy, and robustness in HCI systems.
- The Remora Optimization Algorithm (ROA) technique is utilized for fine-tuning the hyperparameters of the TCN+LSTM model, thus improving the stability and ensuring reliable performance. This process also mitigates overfitting.
- The SEFL-OADLCA model presents a novel framework by integrating MGO-based feature selection, a TCN+LSTM hybrid model, and ROA-based optimization within an FL setup, thus enhancing privacy-preserving cybersecurity, detection accuracy, and efficient HCI system protection.

II. METHODOLOGY

In this manuscript, a novel SEFL-OADLCA model is proposed. The aim is to present an effective FL structure for cybersecurity issues. Figure 1 describes the workflow of the SEFL-OADLCA approach.

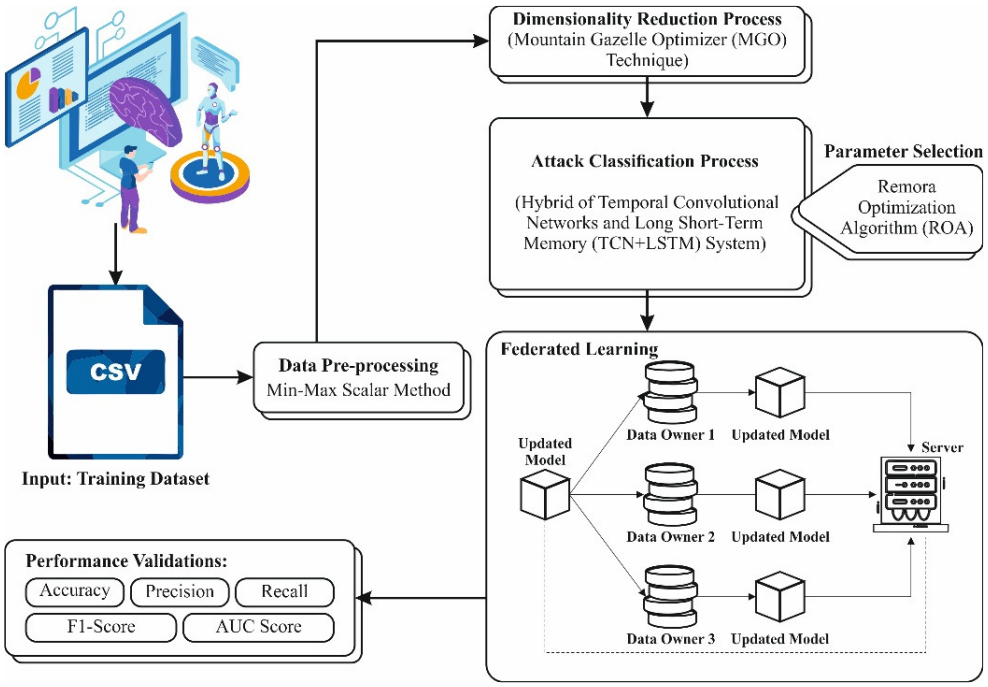

Fig. 1. Workflow of the SEFL-OADLCA model.

A. Min–Max Scaler

At first, the min–max scaler method is utilized. This method is chosen for its efficiency in normalizing data to a consistent range and for preserving the original data dispersion while also ensuring that all features contribute proportionally. This is significant for downstream learning tasks compared with models such as z-score normalization. This step is also crucial for mitigating the influence of varying scales and measurement units. The method involves normalizing the values of dissimilar variables to a common range, typically between (0, 1) or (−1, 1), utilizing diverse methods. The min–max scaler function is expressed in (1):

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (1)$$

where x' refers to the scaled value, and x denotes the original value.

B. Dimensionality Reduction Using the Mountain Gazelle Optimizer

For the DR process, the MGO technique is employed [23]. This method is adopted because it effectively explores the search space to choose the most relevant features, enhancing model performance. MGO can also handle nonlinear and intrinsic feature interactions compared with conventional techniques, thus resulting in better optimization, and reduced computational overhead. The MGO model derives its inspiration from the natural behaviors of mountain gazelles. Several important characteristics are considered in MGO optimization: non-grouping behavior and patterns associated with food searching. MGO models the social behavior of mountain gazelles—male territorial competition, maternity group dynamics, stag male dominance, and long-range migration—to guide the optimal solution search. Male zones simulate young males competing for territory using position updates, as illustrated in (2):

$$M_z = m_g - |ri_1 \times YM - ri_2 \times X(t) \times F| \times cv \quad (2)$$

Maternity groups refine positions through cooperative movement using (3):

$$MG = (YM \times cv) + \left(ri_3 \times m_g - ri_4 \times x_{rand}\right) \times cv \quad (3)$$

Here, x_{rand} denotes the vector position of a mediator that is randomly designated from the overall population and ri_3 and ri_4 indicate random coefficient values.

These behaviors balance exploration and exploitation. The Fitness Function (FF) in MGO represents a balance between minimizing the number of selected attributes in all solutions and maximizing classifier precision:

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|} \quad (4)$$

Here, α and β denote dual parameters linked to the significance of classification quality and subset length, $\gamma_R(D)$ refers to the classification error rate of the given classifier, $|R|$ denotes the cardinality of the selected subset, and $|C|$ represents the total number of features within the data set.

C. Temporal Convolutional Network and Long Short-Term Memory Hybrid Model

Furthermore, the hybrid TCN+LSTM model is utilized [24]. This model offers advantages by integrating the strengths of TCN in capturing long-range temporal dependencies with LSTM's ability to model sequential patterns. The hybrid approach also enhances the accuracy and robustness of attack classification compared with using TCN or LSTM alone, specifically for intrinsic and time-dependent data. The hybrid TCN+LSTM method combines the capabilities of TCN and LSTM to effectively predict across both short-term and long-term temporal intervals. The TCN layer captures temporal dependences and recognizes patterns over its structural characteristics, beginning with causal convolution.

$$y(t) = \sum_{k=0}^{K-1} w_k x(t-k) \quad (5)$$

To efficiently capture long-range dependencies, this method uses dilated convolutions, which expand the receptive field with network depth through dilation factor d:

$$y(t) = \sum_{k=0}^{K-1} w_k x(t-d) \quad (6)$$

Furthermore, TCN incorporates residual connections that assist in preserving gradient flow and improve the training efficacy of deep networks. The architecture of a residual block is expressed in (7):

$$y(t) = x(t) + F\big(x(t)\big) \quad (7)$$

TCN captures short-range dependencies, whereas LSTM's gating mechanisms model long-range sequences and manage cell states, mitigating gradient issues as shown in (8):

$$i_t = \sigma(w_i \cdot [h_{t-1}, x_t] + b_i) \quad (8)$$

Here, i_t refers to the input gate at time-step t, w_i and b_i denote weights and bias, h_{t-1} stands for the hidden layer from the preceding time step, and x_t denotes the present input. The σ sigmoid function restricts the output to the range (0, 1), representing the portion of new data to be integrated. The forget gate controls the removal of data from the previous cell state, with its function defined mathematically in (9):

$$f_t = \sigma\big(w_f \cdot [h_{t-1}, x_t] + b_f\big) \quad (9)$$

Here, f_t, w_f, and b_f represent the forget gate, weights, and bias. These gates produce outputs in the interval (0–1), identifying the percentage of the preceding cell state to be retained, as expressed in (10):

$$\tilde{C}_t = \tanh(w_c \cdot [h_{t-1}, x_t] + b_c) \quad (10)$$

Here, b_c and w_c denote weights and bias for the candidate cell state. The novel cell state is then calculated as in (11):

$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t \quad (11)$$

The output gate selects the next hidden layer h_t based on the upgraded cell state C_t and the input, as shown in (12) and (13):

$$o_t = \sigma(w_o \cdot [h_{t-1}, x_t] + b_o) \quad (12)$$

$$h_t = o_t * \tanh(C_t) \quad (13)$$

where o_t, w_o, and b_o refer to the output gate, weights, and bias.

D. Parameter Optimization Using the Remora Optimization Algorithm

Finally, hyperparameter selection is performed using ROA to optimize the classification results [25]. This method effectively explores the search space to detect optimal configurations, enhancing classification performance. ROA attains better accuracy with lower computational cost and faster convergence compared with conventional methods like grid or random search. The position of the remora fish is calculated using (14):

$$P_i = lower + random \times (upper - lower) \quad (14)$$

Here, P_i refers to the remora fish location, $lower$ and $upper$ denote the search space limits, and $random$ signifies a randomly generated number in [0, 1].

During the exploration phase, the remora attaches to the host fish and moves next to it. The position update equation is given in (15):

$$P_n^{i+1} = P_b^i - \left(random \times \left(\frac{P_b^i + P_{random}^i}{2}\right) - P_{random}^i\right) \quad (15)$$

Here, P_n^{i+1} represents the next iteration solution, P_b^i is the current best solution at iteration i, and P_{random}^i denotes a randomly selected remora.

In this exploration phase, a limited number of candidate positions are generated based on the host location and the previous remora positions. The tentative position update is expressed in (16):

$$P_{t\alpha} = P_n^i + \left(P_n^i + P_{pg}\right) \times random \quad (16)$$

Here, $P_{t\alpha}$ represents the tentative position, P_{pg} is the position of the fish, and $random$ is a number in [0, 1]. The tentative position $P_{t\alpha}$ is evaluated against the current position P_n^i and a probabilistic rule determines whether it replaces the current position:

$$fit\ (P_n^i) < fit(P_{t\alpha}) \quad (17)$$

$$C(n) = round(random) \quad (18)$$

During the exploitation phase, the remora attaches to the whale and moves next to it. The position update is given in the following equations:

$$P_n^{i+1} = \rho \times e^{\gamma} \times \cos(2\pi\alpha) + P_n^i \quad (19)$$

$$\rho = \left|P_b^i - P_n^i\right| \quad (20)$$

$$\gamma = random \times (\alpha - 1) + 1 \quad (21)$$

$$\alpha = -\left(1 + \frac{i}{I}\right) \quad (22)$$

Here, P_n^{i+1} is the next iteration solution, ρ refers to the distance between the previous best solution and the current position, γ is a random value in [−1, 1], α refers to value that decreases linearly from −2 to 1, $random$ is in (0,1), i is the current iteration number, and I is the maximum number of iterations. The position update equations for this stage are expressed in the following equations:

$$P_n^{i+1} = P_n^i + \tau \quad (23)$$

$$\tau = \beta \times (P_n^i - \varepsilon \times P_b) \quad (24)$$

$$\beta = 2 \times \omega \times random - \omega \quad (25)$$

$$\omega = 2 \times \left(1 - \frac{i}{I}\right) \quad (26)$$

Here, τ represents the distance traveled by the remora, ε is a constant set to 0.1, β and ω represent host and remora fish parameters, $random$ is a random number in [0, 1], i is the current iteration, and I is the maximum number of iterations.

FL enables privacy and security by collaboratively training a model without sharing raw data. The server integrates these updates to form a global model, thus improving performance while conserving data confidentiality.

The fitness selection determines the performance of the ROA technique. The hyperparameter range method encodes candidate solutions and evaluates their effectiveness:

$$Fitness = \max(P) \quad (27)$$

$$P = \frac{TP}{TP + FP} \quad (28)$$

Here, TP and FP represent the true positive and false positive values, respectively.

III. EXPERIMENTAL VALIDATION

The performance of the SEFL-OADLCA model was evaluated using the NSL-KDD dataset [26]. The dataset contains 148,517 samples across five classes with 27 selected features. The experiments were conducted on Python 3.6.5 using an Intel i5-8600k CPU, 4 GB GPU, 16 GB RAM, learning rate of 0.01, ReLU activation, 50 epochs, dropout of 0.5, and batch size of 5.

Figure 2 presents the classifier results of the SEFL-OADLCA model, illustrating the confusion matrices, Precision–Recall (PR), and Receiver Operating Characteristic (ROC) curves for all classes.

Table I compares the proposed SEFL-OADLCA model with widely used conventional and deep learning baseline classifiers [27, 28]. The results indicate that SEFL-OADLCA achieved an accuracy ($accu_y$) of 99.46%, precision ($prec_n$) of 91.86%, recall ($reca_l$) of 87.83%,F1-score ($F1_{Score}$) of 89.38%, and a Classification Time (CT) of 1.12 s, outperforming DCNN, LSTM, Contractive Autoencoder (CAE), k-Nearest Neighbors (k-NN), Event Profile-based Fully Connected Neural Network (EP-FCNN), Naïve Bayes (NB), and AE models.

Table II presents a comparative evaluation of the SEFL-OADLCA model against recent state-of-the-art techniques [29]. The experimental results indicate that the proposed approach achieves an accuracy ($accu_y$) of 97.00%, precision ($prec_n$) of 96.97%, recall ($reca_l$) of 97.20%, and an F1-Score ($F1_{Score}$) of 97.02%, outperforming existing methods such as Siamese Capsule, FC-Net, Fully Connected Anomaly Detection (FCAD), Deep Neural Network (DNN), and Few-Shot with L2F.

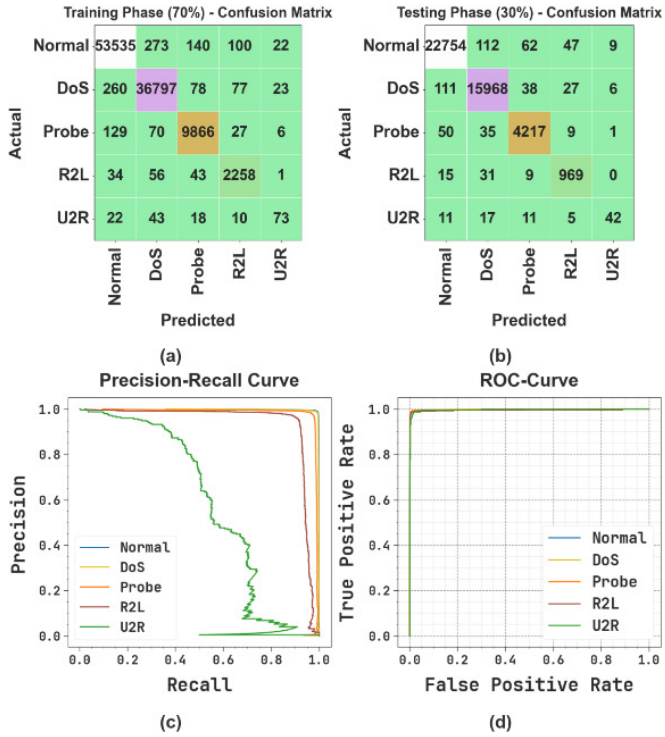

Fig. 2. Classifier results of the SEFL-OADLCA model: (a) training phase confusion matrix, (b) testing phase confusion matrix, (c) PR curve, (d) ROC curve.

TABLE I. COMPARATIVE OUTCOMES OF THE PROPOSED SEFL-OADLCA MODEL WITH BASELINE METHODS

Method	$Accu_y$ (%)	$Prec_n$ (%)	$Reca_l$ (%)	$F1_{score}$ (%)	CT (s)
DCNN [27]	96.34	90.04	76.05	81.00	4.98
LSTM [27]	93.83	85.66	85.92	86.21	5.11
CAE [27]	97.19	87.85	84.96	85.51	2.34
k-NN [27]	94.08	84.74	84.42	78.90	4.77
EP-FCNN [28]	98.27	83.15	84.74	77.54	2.06
NB [27]	91.83	85.19	86.93	80.71	5.00
AE [27]	92.56	90.00	79.82	86.03	3.98
SEFL-OADLCA [proposed]	99.46	91.86	87.83	89.38	1.12

TABLE II. COMPARATIVE ANALYSIS OF THE PROPOSED SEFL-OADLCA MODEL WITH STATE-OF-THE-ART TECHNIQUES

Technique	$Accu_y$ (%)	$Prec_n$ (%)	$Reca_l$ (%)	$F1_{score}$ (%)
Siamese Capsule [29]	93.87	94.66	93.72	90.34
FC-Net [29]	95.56	94.44	91.53	91.81
FCAD [29]	94.30	94.75	93.10	91.30
DNN [29]	96.71	90.04	95.35	90.01
Few-Shot with L2F [29]	94.66	91.94	95.04	91.65
SEFL-OADLCA [proposed]	97.00	96.97	97.20	97.02

Table III presents the ablation study of the SEFL-OADLCA model. TCN+MGO and LSTM+MGO show slight improved results, whereas the hybrid TCN+LSTM+MGO achieves the optimal results. However, the complete SEFL-OADLCA model demonstrates superior performance with an $accu_y$ of 97.57%, $prec_n$ of 89.66%, $reca_l$ of 85.99%, and $F1_{score}$ of 87.24%.

TABLE III. ABLATION STUDY ANALYSIS OF THE SEFL-OADLCA METHODOLOGY

Methodology	$Accu_y$ (%)	$Prec_n$ (%)	$Reca_l$ (%)	$F1_{score}$ (%)
TCN+MGO (TCN with DR process)	97.57	89.66	85.99	87.24
LSTM+MGO (LSTM with DR process)	98.17	90.32	86.52	88.03
TCN+LSTM+MGO (hybrid with DR process)	98.67	91.10	87.02	88.80
SEFL-OADLCA (hybrid TCN+LSTM+MGO with ROA)	97.57	89.66	85.99	87.24

Table IV clearly highlights that the SEFL-OADLCA model achieves the lowest FLOPs of 8.23 M, lowest GPU memory usage of 678.00 MB, and fastest inference time of 1.09 s, outperforming BaseNetwork, ReducedNetwork, U-Net, U-Net-Reduced, CustomBackbone, and VGG16.

TABLE IV. COMPUTATIONAL EFFICIENCY EVALUATION OF THE SEFL-OADLCA MODEL

Methods	FLOPs (M)	GPU (MB)	Inference time (s)
BaseNetwork	100.52	3,108	3.83
ReducedNetwork	63.29	4,764	5.87
U-Net	78.48	4,130	5.83
U-Net-Reduced	113.07	2,856	4.15
CustomBackbone	104.01	3,918	5.04
VGG16	57.72	3,282	3.31
SEFL-OADLCA	8.23	678.00	1.09

IV. CONCLUSION

In this manuscript, a novel Secure and Efficient Federated Learning using Optimization Algorithms and Deep Learning for Cybersecurity Applications (SEFL-OADLCA) methodology is proposed. The model comprises a min–max scaler, Mountain Gazelle Optimizer (MGO)-based Dimensionality Reduction (DR), a hybrid of Temporal Convolutional Network and Long Short-Term Memory (TCN+LSTM)-based attack classification, and Remora Optimization Algorithm (ROA)-based hyperparameter selection. This establishes a novel privacy-preserving framework within a Federated Learning (FL) setup, improving cybersecurity, detection accuracy, and ensuring robust protection for Human–Computer Interface (HCI) systems. The comparison study of the SEFL-OADLCA method demonstrated a superior accuracy value of 99.46% over existing approaches under the NSL-KDD dataset. The limitations include dependence on simulated datasets and controlled environments, which may not fully capture real-world variability. Additionally, the computational demands may pose challenges for large-scale deployment. Future work may concentrate on extending the model to heterogeneous real-world data, thus improving scalability and adaptability for dynamic environments.

REFERENCES

[1] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, Jan. 2024, Art. no. 100031, https://doi.org/10.1016/j.csa.2023.100031.

[2] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability*, vol. 15, no. 18, Sept. 2023, Art. no. 13369, https://doi.org/10.3390/su151813369.

[3] M. S. Alkatheiri, "Artificial intelligence assisted improved human-computer interactions for computer systems," *Computers and Electrical Engineering*, vol. 101, July 2022, Art. no. 107950, https://doi.org/10.1016/j.compeleceng.2022.107950.

[4] S. Gulati, J. McDonagh, S. Sousa, and D. Lamas, "Trust models and theories in human–computer interaction: A systematic literature review," *Computers in Human Behavior Reports*, vol. 16, Dec. 2024, Art. no. 100495, https://doi.org/10.1016/j.chbr.2024.100495.

[5] T. Unwin, *Reclaiming Information and Communication Technologies for Development*. Oxford, U.K.: Oxford University Press, 2017, https://doi.org/10.1093/oso/9780198795292.001.0001.

[6] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, https://doi.org/10.1016/j.egyr.2021.08.126.

[7] A. Sanmorino, L. Marnisah, and H. D. Kesuma, "Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16444–16449, Oct. 2024, https://doi.org/10.48084/etasr.8362.

[8] S. Alqaraleh, "An Efficient Ensemble Network Anomaly Detection System for Cyber-Attacks," *Engineering, Technology & Applied Science Research*, vol. 15, no. 4, pp. 25549–25554, Aug. 2025, https://doi.org/10.48084/etasr.11920.

[9] A. Tariq *et al.*, "Trustworthy Federated Learning: A Comprehensive Review, Architecture, Key Challenges, and Future Research Prospects," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 4920–4998, 2024, https://doi.org/10.1109/OJCOMS.2024.3438264.

[10] M. J. Idrissi *et al.*, "Fed-ANIDS: Federated learning for anomaly-based network intrusion detection systems," *Expert Systems with Applications*, vol. 234, Dec. 2023, Art. no. 121000, https://doi.org/10.1016/j.eswa.2023.121000.

[11] H. Hameed *et al.*, "Recognizing British Sign Language Using Deep Learning: A Contactless and Privacy-Preserving Approach," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 2090–2098, Aug. 2023, https://doi.org/10.1109/TCSS.2022.3210288.

[12] J. Silva and M. Gomez, "Advancements in Human-Computer Interaction Through Natural Language Processing and Voice Recognition," *Journal of Computing Innovations and Applications*, vol. 3, no. 1, pp. 8–12, Jan. 2025.

[13] S. T. Ahmed, A. C. Kaladevi, V. V. Kumar, A. Shankar, and F. Alqahtani, "Privacy Enhanced Edge-AI Healthcare Devices Authentication: A Federated Learning Approach," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 5676–5682, May 2025, https://doi.org/10.1109/TCE.2025.3542955.

[14] N. Elisa, L. Yang, F. Chao, N. Naik, and T. Boongoen, "A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity," *IEEE Access*, vol. 11, pp. 8773–8789, 2023, https://doi.org/10.1109/ACCESS.2023.3239814.

[15] C. S. Kolli, V. V. Krishna Reddy, T. S. Reddy, M. K. Chandol, D. B. Dasari, and M. R. Reddy, "Deep learning-based privacy-preserving recommendations in federated learning," *International Journal of General Systems*, vol. 53, no. 6, pp. 651–677, Aug. 2024, https://doi.org/10.1080/03081079.2024.2302605.

[16] Z. Xihua, S. B. Goyal, M. Tesfayohanis, and C. Verma, "Blockchain-Based Privacy-Preserving Approach Using SVML for Encrypted Smart City Data in the Era of IR 4.0," *Journal of Nanomaterials*, vol. 2022, no. 1, July 2022, Art. no. 7463513, https://doi.org/10.1155/2022/7463513.

[17] T. Kandappu, V. Subbaraju, and Q. Xu, "PrivacyPrimer: Towards Privacy-Preserving Episodic Memory Support For Older Adults," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW2, Oct. 2021, Art. no. 306, https://doi.org/10.1145/3476047.

[18] U. Islam, H. Ullah, N. Khan, I. Ahmad, and K. Saleem, "Adaptive Federated Learning Framework for Privacy-Preserving Consumer-Centric IoMT: A Novel Secure Data Collaboration Model," *IEEE Transactions on Consumer Electronics*, 2025, https://doi.org/10.1109/TCE.2025.3606642.

[19] M. Wang, L. Zhou, X. Huang, and W. Zheng, "Towards Federated Learning Driving Technology for Privacy-Preserving Micro-Expression Recognition," *Tsinghua Science and Technology*, vol. 30, no. 5, pp. 2169–2183, Oct. 2025, https://doi.org/10.26599/TST.2024.9010098.

[20] S. Dutta, D. Irvin, and J. H. L. Hansen, "Exploring discrete speech units for privacy-preserving and efficient speech recognition for school-aged and preschool children," *International Journal of Human-Computer Studies*, vol. 199, May 2025, Art. no. 103460, https://doi.org/10.1016/j.ijhcs.2025.103460.

[21] N. Jia, S. Fu, G. Xu, K. Huang, and M. Xu, "Towards privacy-preserving and efficient word vector learning for lightweight IoT devices," *Digital Communications and Networks*, vol. 10, no. 4, pp. 895–903, Aug. 2024, https://doi.org/10.1016/j.dcan.2022.10.019.

[22] Y. Harrath, O. Adohinzin, J. Kaabi, and M. Saathoff, "Bridging Domains: Advances in Explainable, Automated, and Privacy-Preserving AI for Computer Science and Cybersecurity," *Computers*, vol. 14, no. 9, Sept. 2025, Art. no. 374, https://doi.org/10.3390/computers14090374.

[23] B. Abdollahzadeh, F. S. Gharehchopogh, N. Khodadadi, and S. Mirjalili, "Mountain Gazelle Optimizer: A new Nature-inspired Metaheuristic Algorithm for Global Optimization Problems," *Advances in Engineering Software*, vol. 174, Dec. 2022, Art. no. 103282, https://doi.org/10.1016/j.advengsoft.2022.103282.

[24] J. Bi, X. Zhang, H. Yuan, J. Zhang, and M. Zhou, "A Hybrid Prediction Method for Realistic Network Traffic With Temporal Convolutional Network and LSTM," *IEEE Transactions on Automation Science and Engineering*, vol. 19, no. 3, pp. 1869–1879, July 2022, https://doi.org/10.1109/TASE.2021.3077537.

[25] H. Jia, X. Peng, and C. Lang, "Remora optimization algorithm," *Expert Systems with Applications*, vol. 185, Dec. 2021, Art. no. 115665, https://doi.org/10.1016/j.eswa.2021.115665.

[26] "NSL-KDD." Kaggle. [Online]. Available: https://www.kaggle.com/datasets/hassan06/nslkdd.

[27] S. Naseer *et al.*, "Enhanced Network Anomaly Detection Based on Deep Neural Networks," *IEEE Access*, vol. 6, pp. 48231–48246, 2018, https://doi.org/10.1109/ACCESS.2018.2863036.

[28] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," *IEEE Access*, vol. 7, pp. 165607–165626, 2019, https://doi.org/10.1109/ACCESS.2019.2953095.

[29] J. Bo, K. Chen, S. Li, and P. Gao, "Boosting Few-Shot Network Intrusion Detection with Adaptive Feature Fusion Mechanism," *Electronics*, vol. 13, no. 22, Nov. 2024, Art. no. 4560, https://doi.org/10.3390/electronics13224560.