International Journal of Medical Toxicology & Forensic Medicine
2026, Volume 16, E52670

Research Paper

Attention-Guided Deep Representation Learning for Suspicious Activity and Anomaly Detection in Cybercrime Forensics Analysis

Jayalakshmi Sambandam[1*], Shamili Alias Shanmugapriya Selvam[2], Kaviya Perumal[2], Lavanya Jeyakumar[2], Roopa Nagavalli Krishnappa[3], Meeradevi Thiagarajan[4]

1. Department of Computer Science and Engineering, SRM IST, Vadapalani Campus, Chennai, India

2. CSE, Sri Venkateswara College of Engineering, Sriperumbudur, Chennai, Tamil Nadu, India

3. Computer Science and Engineering, Sri Siddhartha Institute of Technology, SSAHE, Tumkur, Karnataka, India

4. Department Of ECE, Kongu Engineering College, Erode, Tamil Nadu, India

Citation Sambandam J, Selvam SAS, Perumal K, Jeyakumar L, Krishnappa RN, Thiagarajan M. Attention-Guided Deep Representation Learning for Suspicious Activity and Anomaly Detection in Cybercrime Forensics Analysis. International Journal of Medical Toxicology and Forensic Medicine. 2026; 16:E52670.

https://doi.org/10.22037/ijmtfm.v16.52670

Article info:

Received: 01 July, 2026

Accepted: 15 July, 2026

Published: 22 August, 2026

Keywords:

Cybercrime forensic analysis, Cyber activities, Deep learning, Digital platforms, Network traffic

ABSTRACT

Background: Cybercrime encompasses fraudulent activities conducted in virtual environments, such as identity theft, hacking, ransomware, and phishing attacks. Conventional cybercrime forensic analysis approaches are mainly based on statistical and rule-based approaches. Although recent machine learning and deep learning techniques have improved automated detection, existing approaches still suffer from repetitive features, insufficient dependency modeling, and limited detection performance in dynamic cyber environments.

Methods: This study proposes an Attention-Guided Deep Representation Learning for Effective Cybercrime Forensic Analysis (AGDRL-ECFA) framework. The contribution of the study lies in the design of an attention-guided deep representation-learning framework that improves anomaly detection accuracy and forensic pattern discrimination in large-scale cybercrime environments. For feature selection, the proposed model employs a modified ReliefF that identifies the most significant features and eliminates redundant ones. In addition, the attention-based conditional variational autoencoder is utilized to capture underlying data dependencies and classify anomalous or suspicious activities. Eventually, RMSProp is applied to improve training by dynamically adjusting the learning rate for each parameter.

Results: Simulation experiments are performed to ensure an enhanced outcome of AGDRL-ECFA system on the Cybercrime Forensic Dataset. The proposed model achieves better performance, with an accuracy of 97.73% compared to existing models.

Conclusion: The comparative result analysis demonstrates the improvement of the AGDRL-ECFA method and confirms its effectiveness for intelligent cybercrime forensic investigation and decision-support applications.

*** Corresponding Author:**
Jayalakshmi Sambandam, PhD
Department of Computer Science and Engineering, SRM IST, Vadapalani Campus, Chennai, India.
E-mail: *sjayalakshmi2040@gmail.com*

Introduction

Cybercrime is a continuously evolving criminal behavior, shaped by rapid advancements of the cyberworld and digital technologies. As a result, an important domain of cybercrime investigation, cybercrime forensic science has arisen, grounded in procedures that satisfy legal needs and judicial norms. Cyber forensics plays a vital role in law implementation, largely driven by the fast-paced evolution of internet and computer technologies [1]. The rise of Industry 4.0, enhanced interaction among digital devices including internet of things (IoT) systems, mobile devices, storage, networks, and cyber-physical networks, has enlarged the growth of cybercrimes. In recent times, Machine learning (ML) and Artificial Intelligence (AI) methodologies have been progressively integrated into digital forensics and are greatly improving capabilities in pattern detection and evidence categorization [2] Figure 1 signifies the workflow for distributed model training. Several existing forensic techniques that use the cybercrime forensic dataset depend on simpler, organized features and centralized data processing from individual sources. Accordingly, there is a general failure to gain the complete context of distributed cyber actions and various digital data. To overcome these challenges, this work introduces an Attention-Guided Deep Representation Learning for Effective Cybercrime Forensic Analysis (AGDRL-ECFA) technique.

A brief review of previous research works and existing methodologies related to cybercrime forensic analysis. Alsubaei et al. [3] introduced a DL, Gated Recurrent Unit (GRU), and ResNeXt method, systematically developed for live phishing detection. Dananjana et al. [4] developed an advanced method that employs ML to examine internet activity, particularly browser evidence, revealing criminal actions that would otherwise remain invisible. Mardodaj et al. [5] introduced a StegAnalysis Suite, a tool aimed to assist in the complete forensic analysis of data concealed through steganographic methods. Islam et al. [6] presented SentinelFusion, an ensemble-driven machine learning method aimed at enhancing privacy protection and data integrity. Khazem et al. [7] introduced a live cybercrime detection and forensic automation network that incorporates a Transformer-enhanced CNN-LSTM method with blockchain-supported evidence preservation adhering to ISO/IEC 27037 standards. Puchalski et al. [8] proposed the Trustworthy Cyberattack Detector tool (TCAD), which utilizes ML methods to identify and categorize cyberattacks. Kamble et al. [9] introduced the frequency-enhanced attention-based Deep CNN and bidirectional LSTM (FrEnDTM) method. Babu et al. [10] investigated several ML algorithms for detecting insider threats in cybersecurity, such as RF, XGBoost, SVM, DT, and Logistic Regression.

Although the current cybercrime recognition and digital forensic methods provide significant security benefits, they suffer from data silos, high

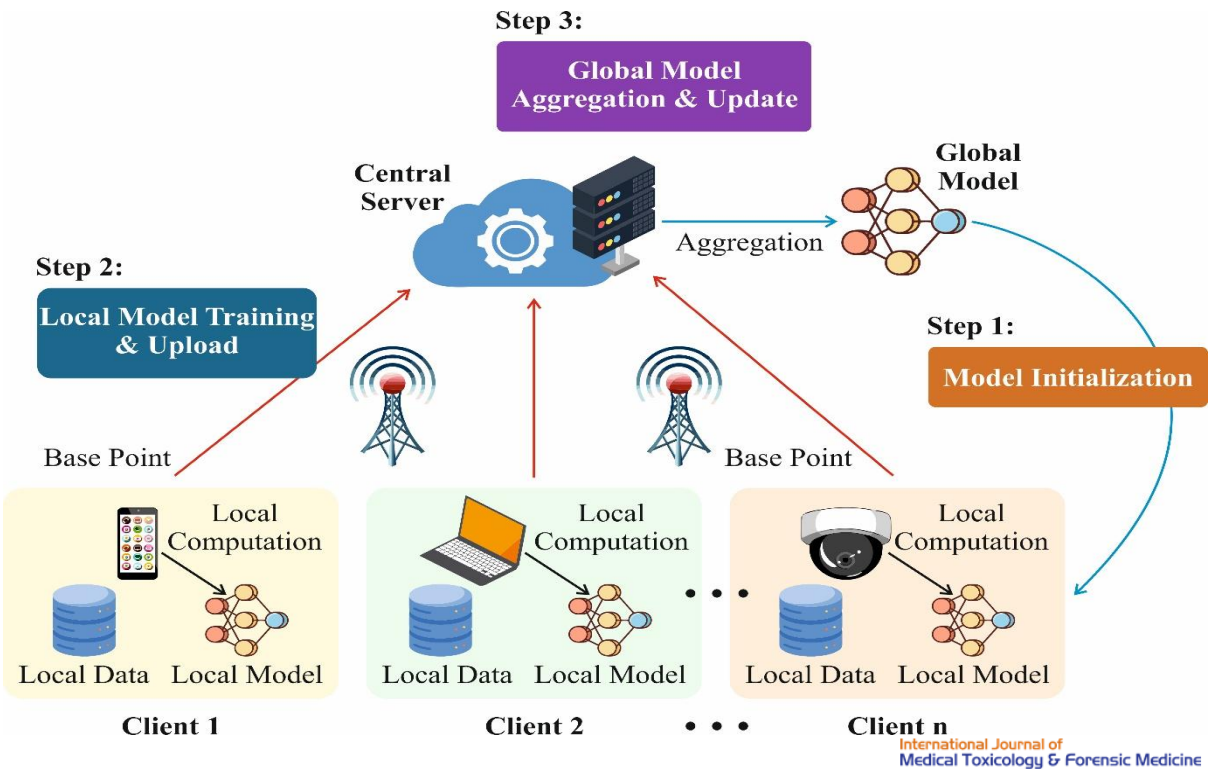

Figure 9. Grad-CAM heatmap visualization with various samples.

computational cost, poor scalability, limited efficiency for identifying more complex cybercrimes, and limitations in handling large, diverse cybercrime datasets. The study aims to propose the AGDRL-ECFA technique to address these limitations in cybercrime forensic analysis. The proposed AGDRL-ECFA approach follows a multi-faceted methodology incorporating modified ReliefF-driven feature extraction, attention-driven DL classification, and parameter tuning. The significance of this study is given below:

- Apply a modified RelieF-based feature selection, which allows the method to select the most relevant and significant features from high-dimensional data.
- Design an attention-based conditional variational autoencoder (Attn-CVAE) to learn meaningful latent representations and classify anomalous or suspicious activities.
- Incorporate an RMSProp optimizer for improving the training process, which helps to adjust the learning rate and ensure stable convergence.

Materials and Methods

Cell Line and Culture Conditions

This study follows a systematic approach for examining cybercrime forensics and categorizes cyber activities that integrate the process of data preprocessing, feature selection, DL-based classification, and optimization. Figure 2 shows the overall framework of the proposed AGDRL-ECFA technique.

The modified ReliefF approach is used for selecting the most relevant and discriminative characteristics from the preprocessed information. Following feature selection, the Attn-CVAE model is used to learn meaningful latent representations and perform classification of anomalous or suspicious cybercrime activities. Hyperparameter optimization is performed using the RMSProp optimizer to increase both the outcome and stability of the method.

Modified ReliefF-based Feature Selection

Using a modified ReliefF approach, the most relevant and discriminative features are identified from the data. MIC is a statistical approach utilized to evaluate the degree of dependence among the features [11]. The MI of features x and y has been computed as:

$$I(u,v) = \sum_{u}\sum_{v} p(u,v)\log_2\left(\frac{p(u,v)}{p(u)p(v)}\right) \quad (1)$$

In this Eq. (4), $p(u,v)$ denotes the combined probability of u and v, and $p(u)$ and $p(v)$ imply their probability intensity, correspondingly.

$$MIC(u,v) = \max\left\{\frac{I(u,\cdot\, v)}{\log_2 \min(a,b)}\right\} \quad (2)$$

Here, b and a signify the count of grids split on y and x axes comprised of u and v, and $\times\, b < M^{0.6}$.

$$s = \begin{Bmatrix} s_{11} & s_{12} & s_{1N} \\ s_{21} & s_{22} & s_{2N} \\ \vdots & \vdots & \vdots \\ s_{N1} & s_{N2} & s_{NN} \end{Bmatrix} \quad (3)$$

Let N denote the overall size of the feature. Describe the distance measure among the instances Z_i

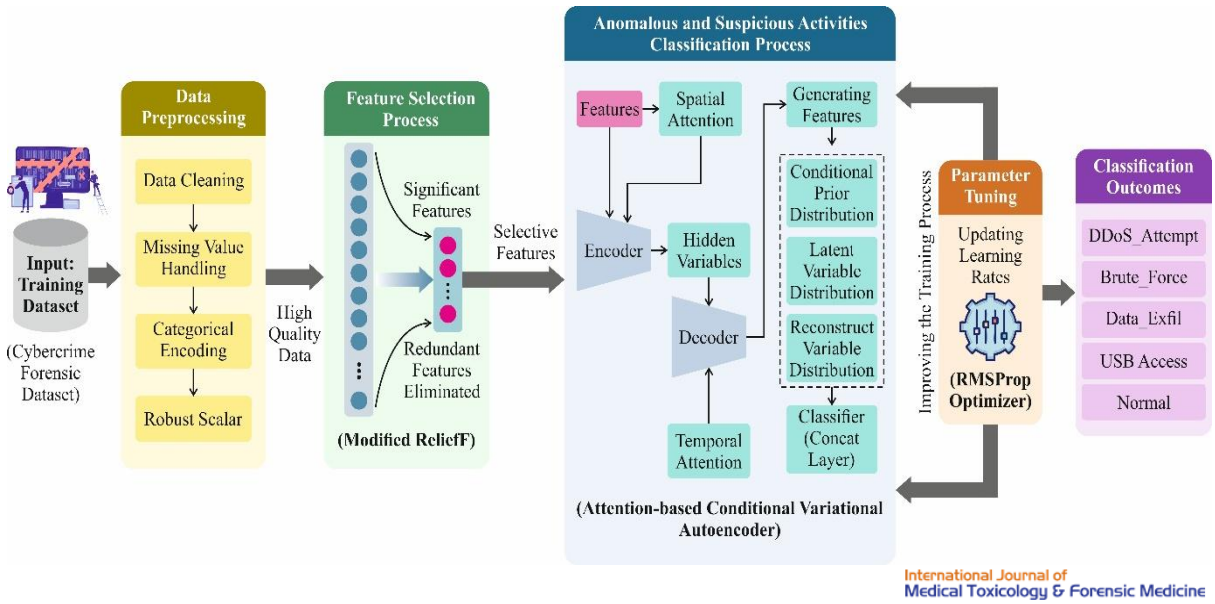

Figure 2. Overall architecture of the proposed AGDRL-ECFA approach.

and Z_j across features f_r:

$$dist(f_r, Zi, Z_j) = diff(f_r, Zj, Z_j) + 1 - \frac{1}{N-1}\sum_{n\neq r}^{N-1} s_{rn} \cdot diff\,(f_n, Zi, Z_j) \quad (4)$$

Therefore, the distance between Z_i and Z_j is:

$$dist\,(Z_i, Z_j) = \frac{1}{N}\sum_{r=1}^{N} d\,ist(f_r, Z_i, Z_j) \quad (5)$$

Attention-based Cybercrime Forensic Analysis

An attention-based conditional variational autoencoder (Attn-CVAR) approach is used to learn important latent features from the data.

Attn-CVAE

The proposed model for cybercrime pattern classification applies an Attn-CVAE. An attention mechanism (AM) assigns dynamic weights to all attributes, capturing differences in network activity, user behavior, and system logs to improve classifier precision.

Attention Mechanism

The conventional attention mechanism (AM) helps extract salient information. In cybercrime forensic analysis, information often comprises numerous parallel activities with intricate relationships, making it complex to interpret.

Encoder

At this encoding phase, a spatial attention module (SAM) obtains features at every time step by allocating larger weights to the most important feature vectors.

$$\tilde{x}_t = [x_t^1 \alpha_t^1, x_t^2 \alpha_t^2, \ldots\ldots x_t^n \alpha_t^n] \quad (6)$$

Decoder

In this decoder phase, a temporal AM is used to extract features across multiple time-step hidden layers.

$$c_t = \sum_{m=1}^{T} \beta_t^m h_{en,m} \quad (7)$$

To further improve model performance the proposed model uses RMSProp, which is represented as,

$$W = W_{t-1} - \alpha.\frac{dw}{\sqrt{vdw} - \varepsilon} \quad (8)$$

$$b = b_{t-1} - \alpha.\frac{db}{\sqrt{db} - \varepsilon} \quad (9).$$

Results

The performance confirmation of the AGDRL-ECFA methods can be examined using the Cybercrime Forensic Dataset [13]. This dataset consists of 7,400 observations replicating several cyber actions and anomalies for cybercrime forensic analysis. It covers data about when a user engages in file management, system access, and network activity, with potential security attacks flagged for forensic examination. The dataset comprises 10 features, of which 7 were designated for analysis. Table 1 shows that the dataset includes five anomaly types, totaling 7,400 instances.

Figure 3 establishes the confusion matrices of the AGDRL-ECFA technique. The outcomes indicate that the AGDRL-ECFA method effectively classifies all types of cybercrime activities with greater accuracy.

Table 1. Details of the dataset.

Anomaly Type	No. of Samples
DDoS_Attempt	282
Brute_Force	308
Data_Exfil	346
USB_Access	297
Normal	6167
Total	**7400**

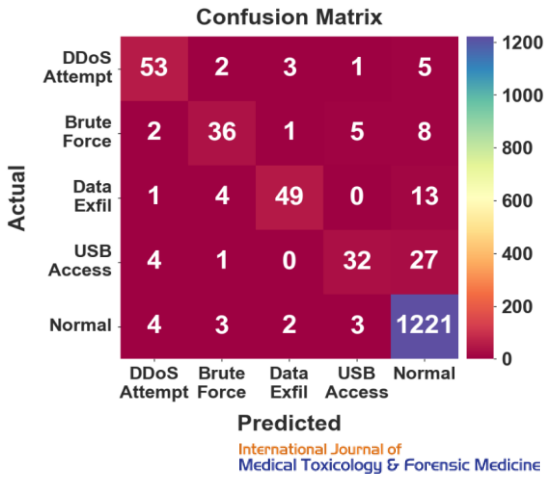

Figure 3. Confusion matrix of the AGDRL-ECFA approach.

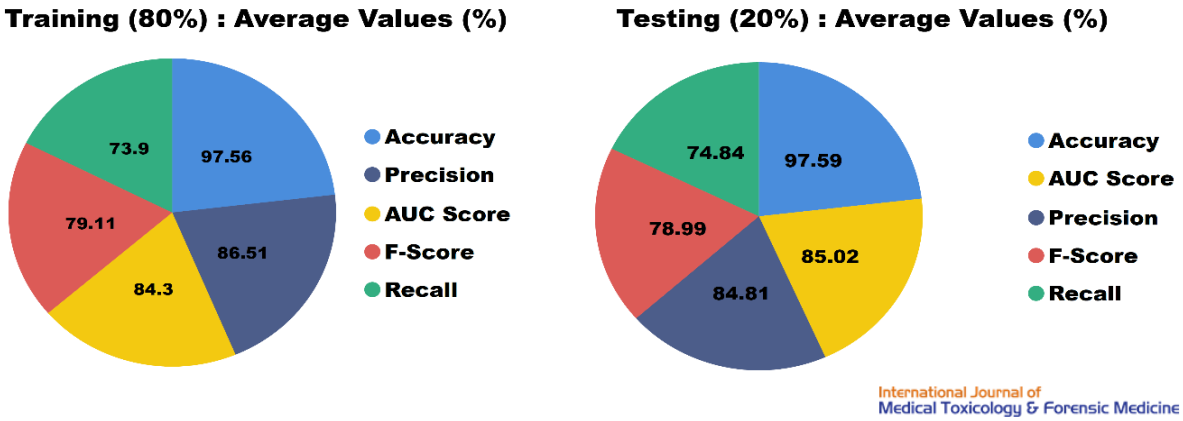

Figure 4. Average value of the AGDRL-ECFA approach with 80:20.

Figure 4 signifies the cybercrime recognition outcome of the AGDRL-ECFA system with an 80:20 split. The outcome implied that the AGDRL-ECFA method correctly identified the types of crimes. On 80% TRAP, the AGDRL-ECFA system reaches an average value of the $accur_y$ of 97.56%, $preci_n$ of 86.51%, $recal_l$ of 73.90%, F_{score} of 79.11%, and AUC_{score} of 84.30%, respectively. For the meantime, on 20% TESP, the AGDRL-ECFA technique achieves an average value with $accur_y$ of 97.59%, $preci_n$ of 84.81%, $recal_l$ of 74.84%, F_{score} of 78.99%, and AUC_{score} of 85.02%, respectively.

Figure 5 establishes the confusion matrices formed by the AGDRL-ECFA method. The findings show that the AGDRL-ECFA method efficiently detects and recognizes each type of cybercrime activity with higher precision.

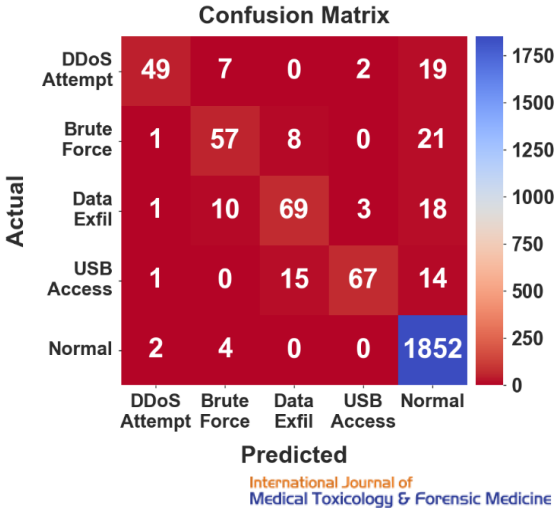

Figure 5. Confusion matrix of the AGDRL-ECFA approach.

Figure 6 shows the cybercrime detection results of the AGDRL-ECFA approach using a 70:30 split. The result suggested that the AGDRL-ECFA method appropriately classified the types of crimes. With 70% TRAP, the AGDRL-ECFA technique attains an average value of the $accur_y$ of 97.61%, $preci_n$ of 87.34%, $recal_l$ of 73.37%, F_{score} of 79.31%, and AUC_{score} of 84.09%, respectively.

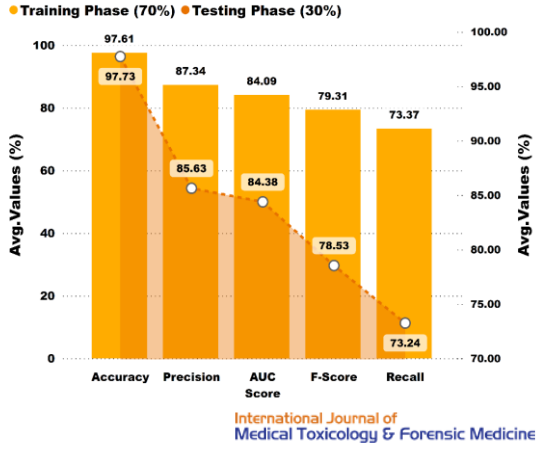

Figure 6. Average value of the AGDRL-ECFA approach with 70:30.

Discussion

Figure 7 presents the comparative outcomes of the AGDRL-ECFA approach under various measures [14-16]. The results implied that the AE-LSTM+Att model has achieved lower performance with $accur_y$ of 85.40%, $preci_n$ of 69.70%, $recal_l$ of 70.78%, and F_{score} of 76.67%, whereas the RNN, DenseNet, CNN-LSTM, C4.5 Model, BERT, and ResNet methods have got slightly better performance. In addition, the BernoulliNB and MultinomialNB approaches produced moderate results. At last, the AGDRL-ECFA model has reached maximal performance with $accur_y$ of 97.73%, $preci_n$ of 85.63%, $recal_l$ of 73.24%, and F_{score} of 78.53%.

Table 2 represents the computational efficiency of the proposed AGDRL-ECFA model with existing approaches. In accordance with the inference time, the AGDRL-ECFA method provides a lesser value of

Table 4. K-fold cross validation of the proposed AGDRL-ECFA approach.

Fold	Accuracy	Precision	Recall	F-Score
k-1	95.42	81.18	68.94	74.56
k-2	95.87	82.34	69.82	75.57
k-3	96.08	82.91	70.36	76.12
k-4	97.10	84.92	72.53	77.61
k-5	96.31	83.47	71.08	76.78
k-6	96.54	83.86	71.55	77.22
k-7	96.18	83.11	70.94	76.54
k-8	96.72	84.28	71.86	77.48
k-9	96.89	84.56	72.21	77.55
k-10	95.63	81.79	69.41	75.09

International Journal of Medical Toxicology & Forensic Medicine

22.76ms, FLOPs of 4.81 G, and GPU Memory of 2.95GB, whereas the ResNet, CNN-LSTM, BERT, AE-LSTM+Att, RNN, and DenseNet models attain greater times of 32.84ms, 38.17ms, 49.36ms, 41.53ms, 27.48ms, and 29.91ms, correspondingly.

Table 3 demonstrates the ablation study of the proposed AGDRL-ECFA methodology. The AGDRL-ECFA (Modified ReliefF + A-CVAE + RMSProp) model achieved the highest performance, $accu_y$ of 97.73%, $prec_n$ of 85.63%, $reca_l$ of 73.24%, and $F1_{score}$ of 78.53%, correspondingly.

Table 2. Computational efficiency of the proposed AGDRL-ECFA model with existing methods.

Methods	Inference Time (ms)	FLOPs (G)	GPU Memory (GB)
ResNet	32.84	8.74	4.86
CNN-LSTM	38.17	10.58	5.63
BERT	49.36	21.47	7.92
AE-LSTM+Att	41.53	13.92	6.14
RNN	27.48	5.86	3.47
DenseNet	29.91	7.42	4.29
AGDRL-ECFA	22.76	4.81	2.95

International Journal of Medical Toxicology & Forensic Medicine

Table 4 represents the K-fold cross-validation of the proposed AGDRL-ECFA model. In fold k-1, the model achieved an accuracy of 95.42%, precision of 81.18%, a recall of 68.94%, and an F-score of 74.56%. However, in fold k-2, the performance slightly increased, with an accuracy of 95.87%, a precision of 82.34%, a recall of 69.82%, and an F-score of 75.57%. Moreover, in fold k-3, the model recorded an accuracy of 96.08%, precision of 82.91%, recall of 70.36%, and F-score of 76.12%.

The presented AGDRL-ECFA architecture efficiently incorporates a modified ReliefF-based feature selection with an attention-guided CVAE to enhance anomaly detection in cybercrime forensic data. By selecting the most relevant features and learning informative latent representations, the architecture achieves high detection performance while reducing the influence of redundant information. These findings signify that the presented AGDRL-ECFA architecture offers a reliable and effective solution for anomaly detection and could serve as a promising foundation for future intelligent cybersecurity applications.

Conclusion

This manuscript has presented an AGDRL-ECFA approach. The primary objective of the proposed AGDRL-ECFA is to investigate cybercrime forensics by identifying anomalous and suspicious patterns. To achieve this, the proposed model begins with data preprocessing, followed by modified ReliefF, Attn-CVAE, and RMSProp. The comparative analysis demonstrates that the AGDRL-ECFA method achieves an accuracy of 97.73%, outperforming existing models. Assessment on a single database can limit its generalizability to other situations, and the method's computational demand can restrict deployment in resource-limited settings. Although the presented methodology illustrates robust anomaly detection performance, certain attack classes with similar behavioral characteristics might still be misclassified. Prediction uncertainty may also arise from noisy or incomplete data, distributional shifts, or previously unseen attack patterns. Additionally, comprehensive evaluations of throughput, inference latency, and resource utilization under real-time, large-scale network settings were beyond the scope of the present study. Future work will concentrate on uncertainty estimation, detailed failure-case analysis, robustness against emerging cyberattack techniques, and comprehensive scalability and real-time performance evaluations, comprising inference latency and resource utilization, to further validate the practical applicability of the presented architecture.

Ethical Approval

None.

Acknowledgment

None.

Funding

No external funding was received for this research.

Conflicts of Interest

The authors report there are no competing interests to declare.

References

[1] Khan A. AI-driven cybercrime forensics for predictive threat detection and investigative intelligence. Int J Sci Interdiscip Res. 2026;7(1):280-324. [DOI: 10.63125/mggyg703]

[2] Islam U, Alwageed HS, Farooq MMU, Khan I, Awwad FA, Ali I, et al. Investigating the effectiveness of novel support vector neural network for anomaly detection in digital forensics data. Sensors. 2023;23(12):5626. [DOI: 10.3390/s23125626]

[3] Alsubaei FS, Almazroi AA, Ayub N. Enhancing phishing detection: a novel hybrid deep learning framework for cybercrime forensics. IEEE Access. 2024;12:8373-89. [DOI: 10.1109/ACCESS.2024.3351946]

[4] Ananjana WP, Arambawela JS, Gonawala DSN, Rathnayaka RGH, Senarathne AN, Siriwardena SDN. Machine learning-based criminal behavior analysis for enhanced digital forensics. PLoS One. 2025;20(10):e0332802. [DOI: 10.1371/journal.pone.0332802]

[5] Mardodaj J, Fetaji B. Integrating advanced algorithms and machine learning for cybercrime investigations. In: Proceedings of the International Conference on Intelligence-Based Transformations of Technology and Business Trends. Cham: Springer Nature Switzerland; 2025. p. 662-72. [DOI: 10.1007/978-3-032-07373-0_50]

[6] Islam U, Alsadhan AA, Alwageed HS, Al-Atawi AA, Mehmood G, Ayadi M, et al. SentinelFusion based machine learning comprehensive approach for enhanced computer forensics. PeerJ Comput Sci. 2024;10:e2183. [DOI: 10.7717/peerj-cs.2183]

[7] Khazem MM, Al Okagaili SM, Jassim BM, Hasan MS, Ahmed SA, Khalaf IZ, Mohammed AA. Real-time detection of cybercrime and digital forensics automation using AI-based legal evidence collection and preservation mechanisms. In: 2025 3rd International Conference on Cyber Resilience (ICCR); 2025 Jul. p. 1-7. [DOI: 10.1109/ICCR67387.2025.11292443]

[8] Puchalski D, Pawlicki M, Kozik R, Renk R, Choraś M. Trustworthy AI-based cyber-attack detector for network cyber crime forensics. In: Proceedings of the 19th International Conference on Availability, Reliability and Security; 2024 Jul. p. 1-8. [DOI: 10.1145/3664476.3670880]

[9] Kamble D, Bartere M. FrEnDTM: digital forensic investigation using frequency-enhanced attention-based deep learning model. SN Comput Sci. 2026;7(2):214. [DOI: 10.1007/s42979-026-04803-1]

[10] Babu MM, Harshini MS, Rao PK, Gowtham R, Jamuna G. Digital forensics for detecting and investigating cyber malicious activities. Int J Hum Comput Intell. 2026;5(3):744-55. [DOI: 10.5281/zenodo.18672461]

[11] Li GM, Liu N, Zhang JA. Speech emotion recognition based on modified ReliefF. Sensors. 2022;22(21):8152. [DOI: 10.3390/s22218152]

[12] Guo W, Sun S, Tang C, Li G, Bai X, Zhao Z. Classification of anomaly patterns in integrated energy systems based on conditional variational autoencoder and attention mechanism. Energies. 2023;16(11):4367. [DOI: 10.3390/en16114367]

[13] Jimohyusuf. Cybercrime forensic dataset [dataset]. Kaggle. [Link]

[14] Dunsin D, Ghanem MC, Ouazzane K, Vassilev V. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Sci Int Digit Investig. 2024;48:301675. [DOI: 10.1016/j.fsidi.2023.301675]

[15] Ananjana WP, Arambawela JS, Gonawala DSN, Rathnayaka RGH, Senarathne AN, Siriwardena SDN. Machine learning-based criminal behavior analysis for enhanced digital forensics. PLoS One. 2025;20(10):e0332802. [DOI: 10.1371/journal.pone.0332802]

[16] Alsubaei FS, Almazroi AA, Ayub N. Enhancing phishing detection: a novel hybrid deep learning framework for cybercrime forensics. IEEE Access. 2024;12:8373-89. [DOI: 10.1109/ACCESS.2024.3351946]