International Journal of Basic and Applied Sciences, 14 (6) (2025) 44-50

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/kk1qt007
Research paper

A Cybersecurity Threat Detection Using Advanced Neural Network Methodologies

Dheeraj Hebri [1], Swagatika Devi [2], Prabu Selvam [3], Valluri Venkata Gopala Rao [4], Robins A Kattoor [5], M. Sridharan [6], B. Selvalakshmi [7], Arun Chokkalingam [8], P. Prakash [9], Ashwini Shinde [10], R G Vidhya [11] *

[1] Department of Master of Computer Applications, Srinivas Institute of Technology, Karnataka, India.
[2] Department of CSE, Institute of Technical Education and Research, Bhubaneswar, Odisha 751030, India.
[3] School of Computing, SRM Institute of Science & Technology, Tiruchirapalli Campus, Tiruchirapalli, India.
[4] Department of Computer Applications, Aditya University, Surampalem, Andhra Pradesh 533437, India.
[5] Department of Computer Applications, Marian College Kuttikkanam Autonomous, Kerala 685531, India.
[6] Department of Mathematics, NPR College of Engineering and Technology (Autonomous), Dindigul, India.
[7] Department of Computer Science and Engineering, Tagore Engineering College, Chennai, Tamil Nadu 600127, India.
[8] Department of Biomedical Engineering, Vels Institute of Science, Technology & Advanced Studies, Chennai, India.
[9] Department of Artificial Intelligence and Data Science, Sri Sairam Engineering College, Chennai, India.
[10] Department of E&TC, Nutan Maharashtra Institute of Technology, Maharashtra, India.
[11] Department of ECE, HKBK College of Engineering, Bangalore, India.
**Corresponding author email: vidhya50.ece@gmail.com*

Received: July 31, 2025, Accepted: September 13, 2025, Published: October 4, 2025

Abstract

As the sophistication of cybersecurity threats continues to rise, colleges and universities are increasingly faced with threats to their digital assets. Traditional approaches to forecasting cybersecurity threats tend to fall short in accurately classifying specific threats, processing ultra-high-dimensional data, and responding suitably to patterns of attacks. To address these challenges, this study introduces a novel prediction model: BPNN-CPOA-CSP-UAC. The model incorporates a Backpropagation Neural Network (BPNN), a heavily used model that can learn complexities in data. To address parameter tuning deficiencies, the model employs the Crested Porcupine Optimization Algorithm (CPOA) to discover the best weights and biases for the neural network, significantly enhancing learning performance and predictive accuracy. Further performance improvements are achieved using the Harbor Seal Whiskers Optimization Algorithm (HSWOA) for feature selection. This eliminates duplicate information by choosing the most descriptive features and eliminating irrelevant information, thus improving the model's accuracy. Tanh-estimator normalization is also used during pre-processing to scale input features and thus ensure high-quality data during training. The model was trained and tested using two benchmark intrusion detection datasets, CIC-IDS-2017 and UNSW-NB15. Performance on testing is remarkable with precision and accuracy both at 99.99%, recall, and F1-score at 99.98%. The model also yielded a minimum false positive ratio of 0.0175%, a false negative ratio of 0.0165%, and a quick execution time of 90.5 milliseconds. These results suggest BPNN-CPOA-CSP-UAC as a practical and efficient academic institution cybersecurity threat prediction model. Since it can predict threats quickly and effectively, it is a strong defense tool against emerging cyber threats in educational institutions.

Keywords: *Cyber threat detection, Backpropagation Neural Network (BPNN), Crested Porcupine Optimization Algorithm (CPOA), Harbor Seal Whiskers Optimization Algorithm (HSWOA), Tanh-estimator normalization.*

1. Introduction

The growing Evolution to greater sophistication and the constantly changing nature of cyber threats have required cybersecurity forecasting as a mandatory need for colleges and universities. Organizations operate in highly dynamic and diverse environments where students, faculty, researchers, and administrative staff collectively constitute a large attack surface for the attackers [1,2]. Traditional security measures—signature-based and anomaly-based detection—have failed to impress. Signature-based techniques rely on the availability of known patterns of attack and are ineffective against new threats, while anomaly detection techniques give high false positives, generating tens of thousands of alarms that saturate security infrastructures [3,4]. As threats to the cyber world evolve at an increasingly improved level, there is an increasingly greater demand for intelligent, adaptive, and affordable security. Though Network Intrusion Detection Systems (NIDS) remain at the center of security frameworks, they must possess precise and timely threat prognosis capabilities to be effective [5,6]. The traditional NIDS, with time, have developed, but their incapability in handling unknown and emerging threats has established

Copyright © Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

the importance of applying machine learning (ML) and deep learning (DL) for intrusion detection [7,8]. However, such models are prone to oversimplification, insufficient flexibility, and reliance on over-complicated feature sets [9,10]. To avoid such limitations, the present study proposes a new cybersecurity prediction model: BPNN-CPOA-CSP-UAC, optimized for the higher education context [11,12]. The model couples a Backpropagation Neural Network (BPNN) with the Crested Porcupine Optimization Algorithm (CPOA) to improve the learning efficiency and prediction precision. It also employs the Harbor Seal Whiskers Optimization Algorithm (HSWOA) for feature extraction, thus using only the most informative and salient features as inputs. This optimizes interpretability while reducing noise [13,14]. The model is evaluated on two benchmark intrusion detection datasets, CIC-IDS-2017 and UNSW-NB15, with preprocessing conducted using Tanh-estimator normalization. Experimental results depict excellent accuracy, precision, recall, and F1-score, with virtually zero false positive and false negative rates, achieved within quick execution times. The findings demonstrate the strength of BPNN-CPOA-CSP-UAC in making quick and correct predictions for cyberthreats, which is a valuable contribution towards securing computer networks in universities and colleges [15,16]. The rest of the paper is discussed as follows: Section 2 discusses related work and current cybersecurity prediction problems. Section 3 presents the research design and key components of the proposed model. Section 4 presents experimental results and performance comparisons. Finally, Section 5 concludes with key findings, contributions, and future research directions.

2. Literature Survey

There has been a recent flow of cybersecurity research, designing prediction methods to be implemented in universities and colleges because of their complicated network infrastructures and growing vulnerability to cyberattacks. One such framework used an enormous pre-processing pipeline—categorical and numerical feature management, normalization, sampling, and transformation—to pre-process data for prediction [17,18]. Though this technique had a staggering accuracy of 98.42%, its excessively lengthy execution time made it impractical. Another model, the LSTM-CSP-UAC, was also proposed in another research, employing Long Short-Term Memory (LSTM) networks to forecast weekly rates of malware incidents in Brazilian universities [19,20]. The model was able to detect temporal patterns with real-world data but had a relatively low prediction rate of 87.34%, necessitating increased accuracy. Pre-processing in this case involved outlier removal with the ADASYN (Adaptive Synthetic Sampling) method. Another model was very accurate at 99.97% in identifying cybersecurity threats but possessed a low F1-score, representing performance imbalances in classification [21,22]. Similarly, Alghamdi and Ragab (2022) introduced the DNN-SROA-CSP-UAC model, with median filtering applied during pre-processing and feature extraction with DenseNet-77. Classification was performed with a deep neural network optimized with the Search and Rescue Optimization Algorithm (SROA) [23,24]. Even though this system achieved high recall values, low precision limited its capacity to minimize false positives. These studies, collectively, point towards repeating problems in constructing cybersecurity prediction systems that can achieve a balance between precision, recall, accuracy, and computational cost. The increasing size and complexity of cyber-attacks on universities tend to leave vulnerabilities in existing models, ranging from high execution times to low F1-scores and lower precision [25,26]. To mitigate the above constraints, this research puts forward the BPNN-CPOA-CSP-UAC model that merges Backpropagation Neural Networks (BPNN) with the Crested Porcupine Optimization Algorithm (CPOA) [27,28]. The integration yields a better adaptive, computationally lightweight, and intelligent predictive system. Overcoming the limitations of the past approaches and employing robust optimization and learning strategies, the introduced model aims to improve the cybersecurity resilience of colleges and universities by a significant degree [29,30].

3. Proposed Methodology

This chapter presents the BPNN-CPOA-CSP-UAC model, which is intended to deliver accurate and efficient cybersecurity threat prediction for college and university environments. The proposed model integrates a Backpropagation Neural Network (BPNN) with the Crested Porcupine Optimization Algorithm (CPOA) to enhance learning and prediction functionality. As presented in Figure 1, the process is separated into three major phases: Data pre-processing using Tanh-estimator normalization, Feature selection using the Harbor Seal Whiskers Optimization Algorithm (HSWOA), Threat Prediction using the BPNN-CPOA-CSP-UAC model. The following subsections detail each step, along with the training and test datasets employed, which are publicly available benchmark datasets.

3.1 Dataset Description for Cybersecurity Prediction in Universities and Colleges

For measuring model performance, two widely used benchmark datasets are employed: CIC-IDS-2017 and UNSW-NB15. Each of the datasets mimics actual traffic and includes a mix of various attack vectors characteristic of the most prevalent threats to higher education networks.

3.1.1 CIC-IDS-2017 Dataset

CIC-IDS-2017 dataset, developed by the Canadian Institute for Cybersecurity (CIC), provides a realistic and comprehensive representation of contemporary network traffic [31,32]. Provided in PCAP format and processed using CICFlowMeter-V3.0, it contains 78 feature-extracted features with correct attack labels. Traffic is recorded from 25 users with varying usage patterns of network protocols like HTTP, HTTPS, FTP, SSH, and email, thereby simulating typical usage patterns and abnormal activities (CIC, 2024). Normal and malicious traffic is both incorporated, spread across 2,830,743 records in differing categories of attacks like DoS, brute force, botnet, infiltration, and web-based attacks [33–35]. Because of its richness of features and attack vector variability, CIC-IDS-2017 is extremely appropriate for academic institution cybersecurity prediction model designing and testing. Its elaborate breakdown of attack types is provided in Table 1.

Table 1: CIC-IDS-2017 Dataset Distribution

Traffic Type	Category/Attack Type	Number of Records	Percentage (%)
Normal Traffic	Benign	22,73,097	88.27
DoS Attacks	GoldenEye	41,508	1.61
	Hulk	2,31,073	8.97
	SlowHTTPTest	5,796	0.23
	Slow Loris	5,796	0.23
Brute Force	FTP-Patator	7,938	0.31
	SSH-Patator	5,897	0.23

Web Attacks	SQL Injection	21	0
	XSS	652	0.03
	Brute Force–Web	1,507	0.06
Infiltration	Infiltration Attacks	36	0
Botnet	Botnet Activity	1,966	0.08
Total Records	—	25,75,287	100

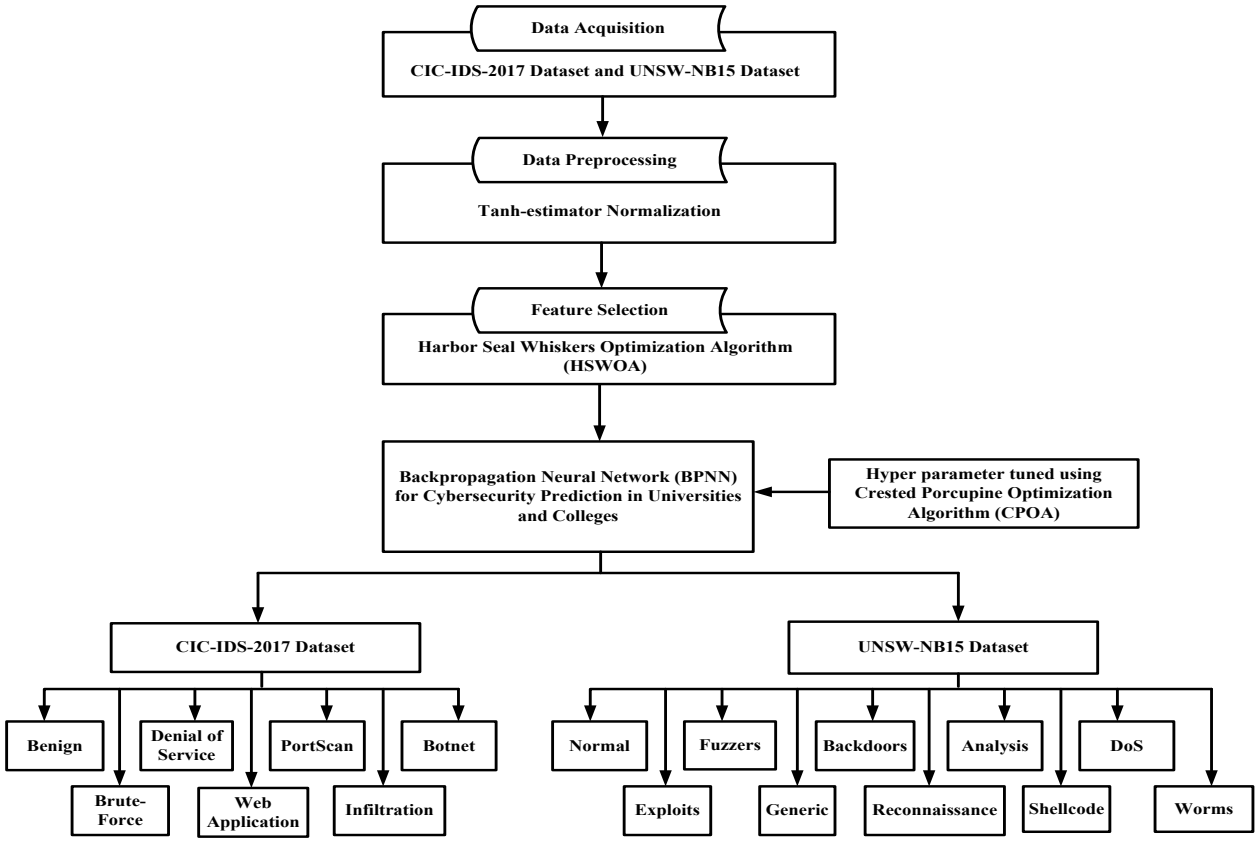

Fig. 1: Block diagram illustrating the BPNN-CPOA-CSP-UAC methodology

3.2 Pre-processing Process

Data Pre-processing is a crucial process for constructing stable and precise cybersecurity prediction models. In this study, Tanh-estimator normalization is employed to normalize the input data [36,37]. It employs the hyperbolic tangent function to scale raw data to a normalized range, which enhances the stability of training and preserves the essential properties of the dataset. Furthermore, the Hampel estimator is included to counter the influence of outliers so that training is not distorted by extreme values [38,39]. The overall effect of such pre-processing techniques is to bring features to a common range, remove noise, and retain the natural data distribution, thereby benefiting both model accuracy and robustness. Figure 2 shows the Architecture diagram of BPNN.

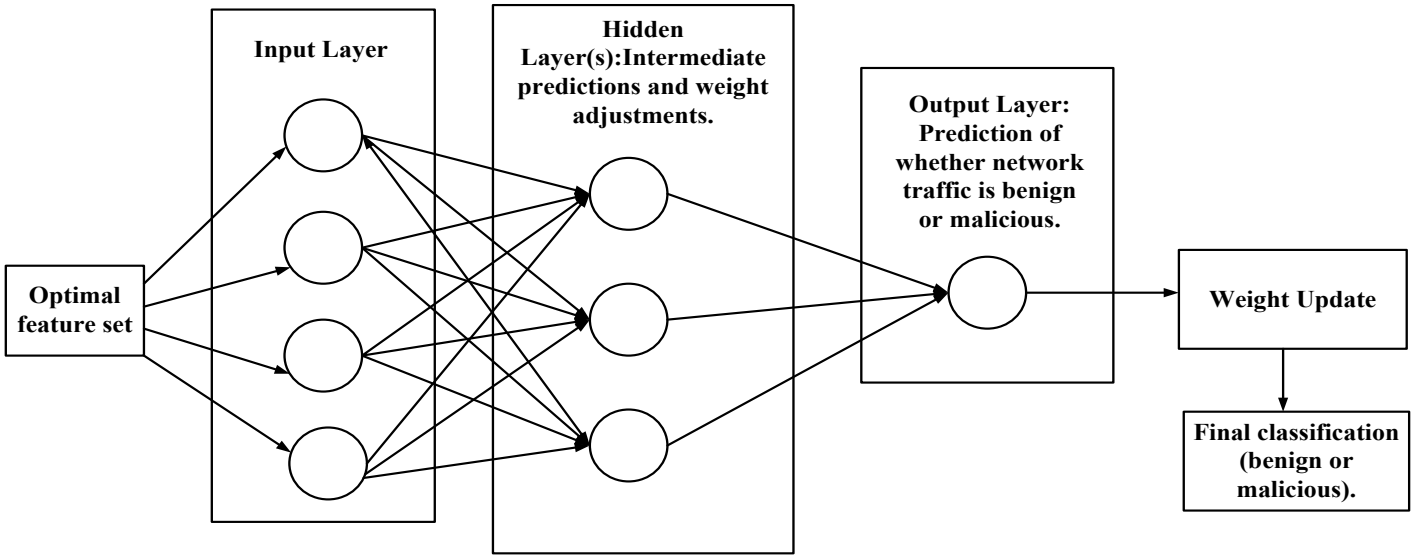

Fig. 2: Architecture diagram of BPNN.

Table 2: BPNN-CPOA-CSP-UAC Model Hyperparameters

Hyperparameter	Value
Learning Rate	0.005
Number of Hidden Layers	4
Number of Neurons per Layer	128
Batch Size	64
Activation Function	ReLU
Epochs	150
Optimization Algorithm	Crested Porcupine Optimization (CPOA)
Population Size	50
Number of Iterations	200
Fitness Function	Accuracy Improvement
Search Space Dimension	10

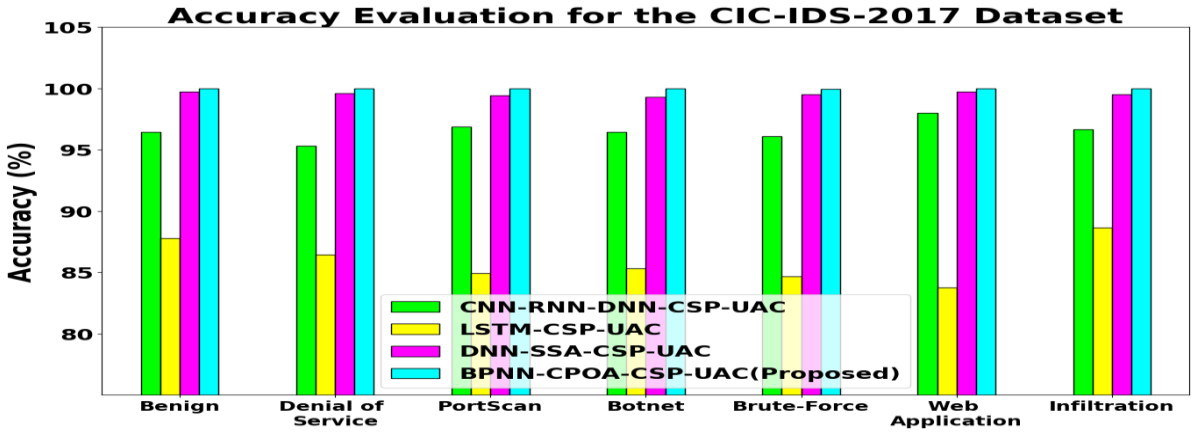

Fig.3: Comparative Accuracy Analysis on CIC-IDS-2017

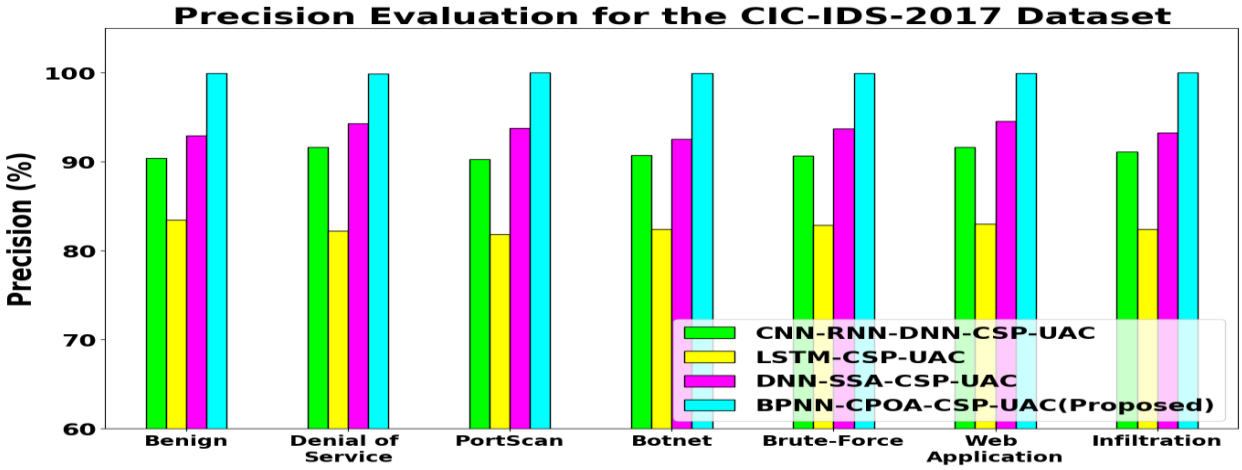

Fig. 4: Comparative Precision Analysis on CIC-IDS-2017

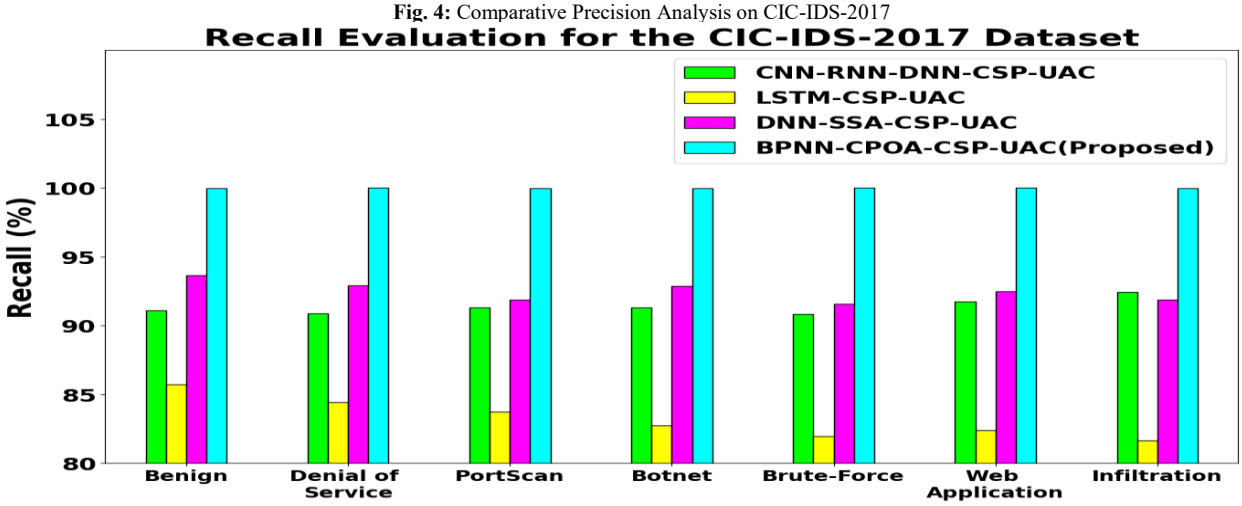

Fig. 5: Comparative Recall Analysis on CIC-IDS-2017

For verifying the accuracy of the effectiveness of the model, the BPNN-CPOA-CSP-UAC framework was experimented with the CIC-IDS-2017 dataset, where data were divided into training set, validation set, and testing set in a 3:1:1 proportion [40,41]. The experiments were conducted on an Intel Core i7 (2.50 GHz) processor-based machine having 8 GB RAM, Windows 10 OS, and a Python-based development environment [42,43]. The hyperparameters employed in the model are summarized in Table 2. For comparison purposes, the

proposed method was compared against three earlier models—CNN-RNN-DNN-CSP-UAC (Barik et al., 2022), LSTM-CSP-UAC (de Souza et al., 2024), and DNN-SSA-CSP-UAC (Al-Ghamdi et al., 2022). The outcomes depicted that BPNN-CPOA-CSP-UAC performed better than baselines for all categories of attacks. Specifically, in accuracy, the model recorded gains of 2.05% to 4.87% over DNN-SSA-CSP-UAC, 12.79% to 19.38% over CNN-RNN-DNN-CSP-UAC, and 0.27% to 0.68% over LSTM-CSP-UAC [44,45]. Precision measures recorded even greater gains with values of 9.02% to 10.71% over DNN-SSA-CSP-UAC, 19.78% to 22.14% over CNN-RNN-DNN-CSP-UAC, and 5.74% to 7.99% over LSTM-CSP-UAC. Similarly, recall performance also ensured the robustness of the model, with improvements of 8.14% to 10.09% against DNN-SSA-CSP-UAC, 16.62% to 22.44% against CNN-RNN-DNN-CSP-UAC, and 6.76% to 9.21% against LSTM-CSP-UAC. The results demonstrate that the BPNN-CPOA-CSP-UAC model is not only precise but also more trustworthy and stronger in predicting cybersecurity attacks in academic networks [46,47]. By ensuring greater accuracy, precision, and recall, the model is extremely useful in defending institutions of higher learning against emerging cyberattacks. Figures 3–8 present a comparative performance analysis of the proposed BPNN-CPOA-CSP-UAC model against existing baseline models on two benchmark intrusion detection datasets: CIC-IDS-2017 and UNSW-NB15. Figure 3 shows the comparative accuracy of the models on the CIC-IDS-2017 dataset [48,49]. The proposed model demonstrates superior accuracy, indicating its effectiveness in correctly identifying both normal and attack traffic [50,51]. Figure 4 illustrates the comparative precision on CIC-IDS-2017. The higher precision of the proposed model indicates a lower rate of false positives, ensuring that benign traffic is rarely misclassified as malicious. Figure 5 displays the recall comparison on CIC-IDS-2017. The elevated recall reflects the model's strong ability to detect actual attacks, minimizing false negatives. Figure 6 shows the comparative accuracy on the UNSW-NB15 dataset. The proposed model consistently outperforms baseline approaches, highlighting its generalization capability across different network environments. Figure 7 illustrates the precision comparison on UNSW-NB15. The model maintains high precision, confirming its reliability in distinguishing between attack and normal traffic. Figure 8 presents the recall comparison on UNSW-NB15. The proposed model achieves higher recall, demonstrating robust detection of diverse attack types.

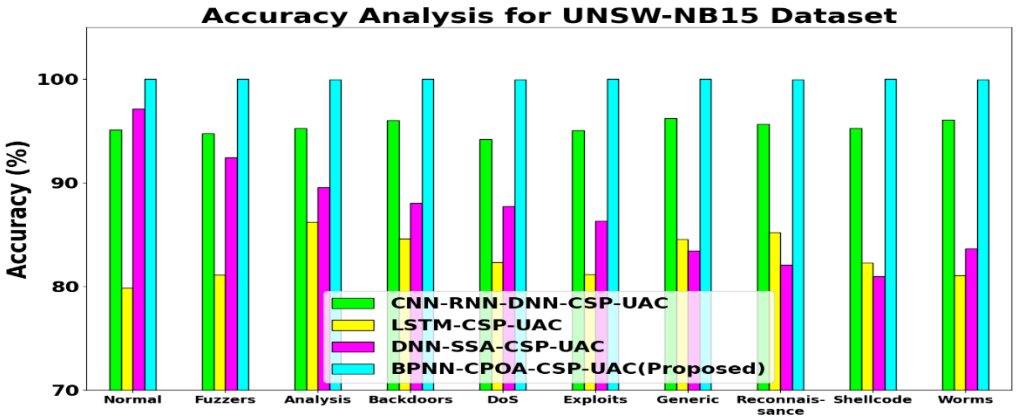

Fig. 6: Comparative accuracy Analysis on UNSW-NB15 dataset

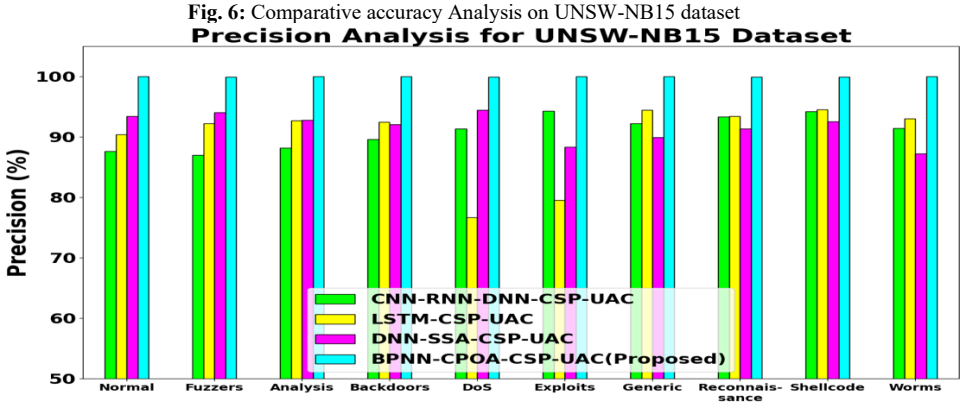

Fig. 7: Comparative precision Analysis on UNSW-NB15 dataset

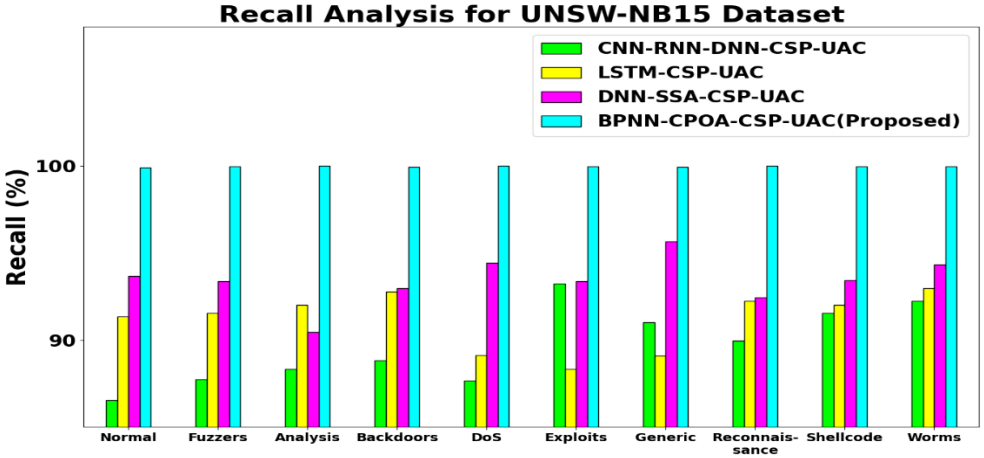

Fig. 8: Comparative recall Analysis on UNSW-NB15 dataset

4. Conclusion

The results firmly demonstrate the robustness and effectiveness of the BPNN-CPOA-CSP-UAC model in handling diverse attack scenarios in educational networks. On both the CIC-IDS-2017 and UNSW-NB15 datasets, the proposed model consistently outperforms baseline approaches across multiple evaluation metrics. For CIC-IDS-2017, it achieves higher accuracy, precision, recall, and F1 scores, while significantly reducing false positive and false negative rates, alongside markedly lower execution time. Similarly, on UNSW-NB15, the model maintains superior accuracy, precision, recall, and F1 scores, with substantially reduced FPR, FNR, and computational overhead. These results confirm that BPNN-CPOA-CSP-UAC not only enhances detection performance but also ensures efficiency and reliability, highlighting its suitability for practical deployment in educational network environments.

Acknowledgement

I express my sincere gratitude to Almighty God for granting me the strength, health, and determination to carry out this research successfully. I acknowledge all the authors and researchers whose work has laid the foundation and inspired this study. Their contributions in the field of cybersecurity and artificial intelligence have been instrumental in shaping the methodology and direction of this research.

References

[1] I.F. Kilincer, F. Ertam, A. Sengur, "A comprehensive intrusion detection framework using boosting algorithms", Computers and Electrical Engineering, Vol. 100, No.1, pp.107869, 2022, doi: 10.1016/j.compeleceng.2022.107869.
[2] E.E. Abdallah, A.F. Otoom, "Intrusion detection systems using supervised machine learning techniques: a survey", Procedia Computer Science, Vol.201, No.1, pp.205–212, 2022, doi: 10.1016/j.procs.2022.02.025.
[3] A. Khanan, Y.A. Mohamed, A.H. Mohamed, M. Bashir, "From Bytes to Insights: A Systematic Literature Review on Unraveling IDS Datasets for Enhanced Cybersecurity Understanding", IEEE Access, Vol.. 12, No.1, pp.1–20,2024, doi: 10.1109/ACCESS.2024.3374469.
[4] A. Thakkar, R. Lohiya, "Fusion of statistical importance for feature selection in Deep Neural Network-based Intrusion Detection System", Information Fusion, Vol.90, No.1, pp.353–363, 2023, doi: 10.1016/j.inffus.2022.09.004.
[5] T. Al-Shehari, M. Kadrie, T. Alfakih, H. Alsalman, T. Kuntavai, et al., "Blockchain with secure data transactions and energy trading model over the internet of electric vehicles," Sci. Rep., vol. 14, no. 1, p. 19208, 2024, doi: 10.1038/s41598-024-56894-w.
[6] P. Selvam, N. Krishnamoorthy, S. P. Kumar, K. Lokeshwaran, M. Lokesh, et al., "Internet of Things Integrated Deep Learning Algorithms Monitoring and Predicting Abnormalities in Agriculture Land," Internet Technol. Letters, 2024, doi: /10.1002/itl2.607.
[7] B. Ramesh, V. V. Kulkarni, Ashwini Shinde, Dinesh Kumar J. R, Prasanthi,et al.," Optimizing EV Energy Management Using Monarch Butterfly and Quantum Genetic Algorithms," International Journal of Basic and Applied Sciences" vol.14, no.2, pp. 311-318, 2025, doi: 10.14419/xaqk1294
[8] K. Maithili, A. Kumar, D. Nagaraju, D. Anuradha, S. Kumar, et al., "DKCNN: Improving deep kernel convolutional neural network-based covid-19 identification from CT images of the chest," J. X-ray Sci. Technol., vol. 32, no. 4, pp. 913–930, 2024, doi: 10.3233/XST-230424.
[9] T. A. Mohanaprakash, M. Kulandaivel, S. Rosaline, P. N. Reddy, S. S. N. Bhukya, et al., "Detection of Brain Cancer through Enhanced Particle Swarm Optimization in Artificial Intelligence Approach," J. Adv. Res. Appl. Sci. Eng. Technol., vol. 33, no. 3, pp. 174–186, 2023, doi: 10.37934/araset.33.2.174186.
[10] Wange N. K., Khan I., Pinnamaneni R., Cheekati H., Prasad J., et al., "β-amyloid deposition-based research on neurodegenerative disease and their relationship in elucidate the clear molecular mechanism," Multidisciplinary Science Journal, vol. 6, no. 4, pp. 2024045–2024045, 2024, doi: 10.31893/multiscience.2024045.
[11] Anitha C., Tellur A., Rao K. B. V. B., Kumbhar V., Gopi T., et al., "Enhancing Cyber-Physical Systems Dependability through Integrated CPS-IoT Monitoring," International Research Journal of Multidisciplinary Scope, vol. 5, no. 2, pp. 706–713, 2024. 10.47857/irjms.2024.v05i02.0620.
[12] Balasubramani R., Dhandapani S., Sri Harsha S., Mohammed Rahim N., Ashwin N., et al., "Recent Advancement in Prediction and Analyzation of Brain Tumour using the Artificial Intelligence Method," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 33, no. 2, pp. 138–150, 2023, doi: 10.37934/araset.33.2.138150.
[13] Chaturvedi A., Balasankar V., Shrimali M., Sandeep K. V., et al., "Internet of Things Driven Automated Production Systems using Machine Learning," International Research Journal of Multidisciplinary Scope, vol. 5, no. 3, pp. 642–651, 2024, doi: 10.47857/irjms.2024.v05i03.01033.
[14] Saravanakumar R., Arularasan A. N., Harekal D., Kumar R. P., Kaliyamoorthi P., et al., "Advancing Smart Cyber Physical System with Self-Adaptive Software," International Research Journal of Multidisciplinary Scope, vol. 5, no. 3, pp. 571–582, 2024, doi: 10.47857/irjms.2024.v05i03.01013.
[15] Vidhya R. G., Surendiran J., Saritha G., "Machine Learning Based Approach to Predict the Position of Robot and its Application," Proc. Int. Conf. on Computer Power and Communications, pp. 506–511, 2022, doi: 10.1109/ICCPC55978.2022.10072031.
[16] Sivanagireddy K., Yerram S., Kowsalya S. S. N., Sivasankari S. S., Surendiran J., et al., "Early Lung Cancer Prediction using Correlation and Regression," Proc. Int. Conf. on Computer Power and Communications, pp. 24–28, 2022, doi: 10.1109/ICCPC55978.2022.10072059.
[17] Vidhya R. G., Seetha J., Ramadass S., Dilipkumar S., Sundaram A., Saritha G., "An Efficient Algorithm to Classify the Mitotic Cell using Ant Colony Algorithm," Proc. Int. Conf. on Computer Power and Communications, pp. 512–517, 2022, doi: 10.1109/ICCPC55978.2022.10072277.
[18] Sengeni D., Muthuraman A., Vurukonda N., Priyanka G., et al., "A Switching Event-Triggered Approach to Proportional Integral Synchronization Control for Complex Dynamical Networks," Proc. Int. Conf. on Edge Computing and Applications, pp. 891–894, 2022, doi: 10.1109/ICECAA55415.2022.9936124.
[19] Vidhya R. G., Rani B. K., Singh K., Kalpanadevi D., Patra J. P., Srinivas T. A. S., "An Effective Evaluation of SONARS using Arduino and Display on Processing IDE," Proc. Int. Conf. on Computer Power and Communications, pp. 500–505, 2022, doi: 10.1109/ICCPC55978.2022.10072229.
[20] Kushwaha S., Boga J., Rao B. S. S., Taqui S. N., et al., "Machine Learning Method for the Diagnosis of Retinal Diseases using Convolutional Neural Network," Proc. Int. Conf. on Data Science, Agents & Artificial Intelligence, 2023, doi: 10.1109/ICDSAAI59313.2023.10452440.
[21] Maheswari B. U., Kirubakaran S., Saravanan P., Jeyalaxmi M., Ramesh A., et al., "Implementation and Prediction of Accurate Data Forecasting Detection with Different Approaches," Proc. 4th Int. Conf. on Smart Electronics and Communication, pp. 891–897, 2023, doi: 10.1109/ICOSEC58147.2023.10276331.
[22] Mayuranathan M., Akilandasowmya G., Jayaram B., Velrani K. S., Kumar M., et al., "Artificial Intelligent based Models for Event Extraction using Customer Support Applications," Proc. 2nd Int. Conf. on Augmented Intelligence and Sustainable Systems, pp. 167–172, 2023, doi: 10.1109/ICAISS58487.2023.10250679.
[23] Gold J., Maheswari K., Reddy P. N., Rajan T. S., Kumar S. S., et al., "An Optimized Centric Method to Analyze the Seeds with Five Stages Technique to Enhance the Quality," Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, pp. 837–842, 2023, doi: 10.1109/ICAISS58487.2023.10250681.
[24] Anand L., Maurya J. M., Seetha D., Nagaraju D., et al., "An Intelligent Approach to Segment the Liver Cancer using Machine Learning Method," Proc. 4th Int. Conf. on Electronics and Sustainable Communication Systems, pp. 1488–1493, 2023, doi: 10.1109/ICESC57686.2023.10193190.
[25] Harish Babu B., Indradeep Kumar, et al., "Advanced Electric Propulsion Systems for Unmanned Aerial Vehicles," Proc. 2nd Int. Conf. on Sustainable Computing and Smart Systems (ICSCSS), pp. 5–9, 2024, doi: 10.1109/ICSCSS60660.2024.10625489.

[26] Jagan Raja V., Dhanamalar M., Solaimalai G., et al., "Machine Learning Revolutionizing Performance Evaluation: Recent Developments and Breakthroughs," Proc. 2nd Int. Conf. on Sustainable Computing and Smart Systems (ICSCSS), pp. 780–785, 2024, doi: 10.1109/ICSCSS60660.2024.10625103.
[27] Sivasankari S. S., Surendiran J., Yuvaraj N., et al., "Classification of Diabetes using Multilayer Perceptron," Proc. IEEE Int. Conf. on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1–5, IEEE, 2022, doi: 10.1109/ICDCECE53908.2022.9793085.
[28] Anushkannan N. K., Kumbhar V. R., Maddila S. K., et al., "YOLO Algorithm for Helmet Detection in Industries for Safety Purpose," Proc. 3rd Int. Conf. on Smart Electronics and Communication (ICOSEC), pp. 225–230, 2022, doi: 10.1109/ICOSEC54921.2022.9952154.
[29] Reddy K. S., Vijayan V. P., Das Gupta A., et al., "Implementation of Super Resolution in Images Based on Generative Adversarial Network," Proc. 8th Int. Conf. on Smart Structures and Systems (ICSSS), pp. 1–7, 2022, doi: 10.1109/ICSSS54381.2022.9782170.
[30] Joseph J. A., Kumar K. K., Veerraju N., Ramadass S., Narayanan S., et al., "Artificial Intelligence Method for Detecting Brain Cancer using Advanced Intelligent Algorithms," Proc. Int. Conf. on Electronics and Sustainable Communication Systems, pp. 1482–1487, 2023, doi: 10.1109/ICESC57686.2023.10193659.
[31] Surendiran J., Kumar K. D., Sathiya T., et al., "Prediction of Lung Cancer at Early Stage Using Correlation Analysis and Regression Modelling," Proc. 4th Int. Conf. on Cognitive Computing and Information Processing, 2022, doi: 10.1109/CCIP57447.2022.10058630.
[32] Goud D. S., Varghese V., Umare K. B., Surendiran J., et al., "Internet of Things-based Infrastructure for the Accelerated Charging of Electric Vehicles," Proc. Int. Conf. on Computer Power and Communications, 2022, pp. 1–6. doi:10.1109/ICCPC55978.2022.10072086.
[33] Vidhya R. G., Singh K., Paul J. P., Srinivas T. A. S., Patra J. P., Sagar K. V. D., "Smart Design and Implementation of Self-Adjusting Robot using Arduino," Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, pp. 1–6, 2022, doi: 10.1109/ICAISS55157.2022.10011083
[34] Vallathan G., Yanamadni V. R., et al., "An Analysis and Study of Brain Cancer with RNN Algorithm-based AI Technique," Proc. Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), pp. 637–642, 2023, doi: 10.1109/I-SMAC58438.2023.10290397.
[35] Vidhya R. G., Bhoopathy V., Kamal M. S., Shukla A. K., Gururaj T., Thulasimani T., "Smart Design and Implementation of Home Automation System using Wi-Fi," Proc. Int. Conf. on Augmented Intelligence and Sustainable Systems, pp. 1203–1208, 2022, doi: 10.1109/ICAISS55157.2022.10010792
[36] Vidhya R., Banavath D., Kayalvili S., Naidu S. M., Prabu V. C., et al., "Alzheimer's Disease Detection using Residual Neural Network with LSTM Hybrid Deep Learning Models," J. Intelligent & Fuzzy Systems, 2023; vol. 45, no. 6, pp. 12095–12109. 2023, https://doi.org/10.3233/JIFS-235059.
[37] Balasubramaniyan S., Kumar P. K., Vaigundamoorthi M., Rahuman A. K., et al., "Deep Learning Method to Analyze the Bi-LSTM Model for Energy Consumption Forecasting in Smart Cities," Proc. Int. Conf. on Sustainable Communication Networks and Application, pp. 870–876, 2023, doi: 10.1109/ICSCNA58489.2023.10370467.
[38] Somani V., Rahman A. N., Verma D., et al., "Classification of Motor Unit Action Potential Using Transfer Learning for the Diagnosis of Neuromuscular Diseases," Proc. 8th Int. Conf. on Smart Structures and Systems (ICSSS), pp. 1–7, .2022, doi: 10.1109/ICSSS54381.2022.9782209.
[39] Vidhya R. G., Saravanan R., Rajalakshmi K., "Mitosis Detection for Breast Cancer Grading," Int. J. Advanced Science and Technology, 2020; vol. 29, no. 3, pp. 4478–4485.
[40] Gupta D., Kezia Rani B., Verma I., et al., "Metaheuristic Machine Learning Algorithms for Liver Disease Prediction," Int. Res. J. Multidisciplinary Scope, vol. 5, no. 4, 2024, pp. 651–660. https://doi.org/10.47857/irjms.2024.v05i04.01204
[41] Sudhagar D., Saturi S., Choudhary M., et al., "Revolutionizing Data Transmission Efficiency in IoT-Enabled Smart Cities: A Novel Optimization-Centric Approach," Int. Res. J. Multidisciplinary Scope, vol. 5, no. 4, pp. 592–602, 2024, doi: https://doi.org/10.47857/irjms.2024.v05i04.01113.
[42] Vidhya R. G., Batri K., "Segmentation, Classification and Krill Herd Optimization of Breast Cancer," J. Medical Imaging and Health Informatics, vol. 10, no. 6, pp. 1294–1300, 2020, DOI: 10.1166/jmihi.2020.3060.
[43] Chintureena Thingom, Martin Margala, S Siva Shankar, Prasun Chakrabarti, RG Vidhya, " Enhanced Task Scheduling in Cloud Computing Using the ESRNN Algorithm: A Performance-Driven Approach", Internet Technology Letters, vol. 8, no. 4, pp. e70037, 2025, https://doi.org/10.1002/itl2.70037.
[44] V. V. Satyanarayana, Tallapragada , Denis R , N. Venkateswaran , S. Gangadharan , M. Shunmugasundaram, et.al.," A Federated Learning and Blockchain Framework for IoMT-Driven Healthcare 5.0", International Journal of Basic and Applied Sciences, vol. 14, no. 1, pp. 246-250, 2025, doi: 10.14419/n1npsj75.
[45] Thupakula Bhaskar , K. Sathish , D. Rosy Salomi Victoria , Er.Tatiraju. V. Rajani Kanth , Uma Patil, et.al.," Hybrid deep learning framework for enhanced target tracking in video surveillance using CNN and DRNN-GWO", International Journal of Basic and Applied Sciences, vol. 14, no. 1, pp. 208-215, 2025, doi: 10.14419/wddeck70.
[46] Thupakula Bhaskar, Hema N , R.Rajitha Jasmine , Pearlin , Uma Patil , Madhava Rao Chunduru , et.al.," An adaptive learning model for secure data sharing in decentralized environments using blockchain technology", International Journal of Basic and Applied Sciences, vol. 14, no. 1, pp. 216-221, 2025, doi: 10.14419/9f4z3q54.
[47] D, D. Krishnamoorthy, N. Ramapraba, P. S. Nagababu , K.Balaji, K. Reddy , M. K.John , W. M. Chaudhary , S. Boga , J. & Vidhya, R. G. . (2025). Deep Learning Driven Anomaly Detection in Social Graphs by Using Anti-Corona Political Optimization. International Journal of Basic and Applied Sciences, 14(4), 220-228. https://doi.org/10.14419/qw8xgz45
[48] Manivannan, T. ., Deepa , K. ., Devendran , A. ., Neeli, G. S. . ., Uike , D. ., D, C. S. ., D, P., Chaudhary , S. ., Aancy , H. Mickle ., & Vidhya, R. G. . (2025). AI Driven Inventory Optimization Framework Using Deep Learning and Metaheuristic Algorithms. International Journal of Basic and Applied Sciences, 14(4), 405-411. https://doi.org/10.14419/vp1eee47
[49] Anakal , S. ., Arif , M. ., Artheeswari , S. ., Balaji , K. ., Pankajam , A. ., Augustine , P. J. ., Mohitha , . M. R. ., Patil , A. ., Aancy , H. M. ., & Vidhya, R. G. . . (2025). A Blockchain-Enabled Adaptive Learning Model for Secure and Scalable Data Sharing. International Journal of Basic and Applied Sciences, 14(4), 229-236. https://doi.org/10.14419/y90y2496
[50] Devi , S. ., Nisha , , S. R. ., Marotrao , S. S. ., R, R. ., Maheswari , B. U. ., Murugeswari , P. ., Augustine, P. J. . ., Chaudhary , S. ., Aancy, H. M. ., Vidhya , R. G. ., & G, S. . (2025). A Deep Learning Framework for Human Motion RecognitionUsing Compact CNNs and Swarm Optimization. International Journal of Basic and Applied Sciences, 14(4), 211-219. https://doi.org/10.14419/km6frv17.