Advances in Computational Design, *Vol. 10, No. 3 (2025) 233-250*
https://doi.org/10.12989/acd.2025.10.3.233

Optimized adaptive intrusion detection framework for big data in social media application

Chinnakka Sudha*[1] and Sreenivasulu Bolla[2]

[1]*Department of Computer Science and Engineering*, *Koneru Lakshmaiah Education Foundation*, *Vaddeswaram*, *AP*, *India*
[2]*Department of Artificial Intelligence & Data Science*,*Koneru Lakshmaiah Education Foundation*, *Vaddeswaram*, *AP*, *India*

(Received April 24, 2025, Revised June 25, 2025, Accepted July 15, 2025)

Abstract. Social media has become a significant aspect of individuals' everyday lives as it enables communication and information exchange. However, these channels are also being used to spread misinformation and harm others. A novel approach called the Coati Attention Transformer Prediction (CATP) framework was implemented, where social network intrusion detection data was initially considered and trained in the system. Preprocessing was conducted to eliminate noise variations from the trained database, and present features in the database were estimated by the coati optimal behavior. Then, the attack was predicted, and classification was conducted based on different classes. The suggested model exhibits an outstanding success rate, achieving an F1-score of 99.98%, a recall of 99.98%, a precision of 99.98%, an error rate as minimal as 0.02%, and an accuracy of 99.98%. The proposed model shows the best success rate with accuracy.

Keywords: classification; coati optimization; intrusion detection; preprocessing

1. Introduction

The Big data analytics (BDA) involves complex procedures that oversee significant amounts of data, ensuring their effective handling and transmission (Hang *et al*. 2024). However, managing such large amounts of data is becoming increasingly difficult (Kamyab *et al*. 2023). This issue is especially relevant, considering the everyday generation and sharing of massive volumes of data across multiple digital platforms such as social media, blogs, and online forums (Acampa *et al*. 2023). The expansion of digital communications has increased the number of cyber challenges (Ehiane *et al*. 2023), such as cybercrime and online terrorism, which use computer networks and technology for illegal purposes (Rekha *et al*. 2023). The enhanced security measures must be taken immediately to protect people and organizations around the world (Kizza *et al*. 2024). Intrusion detection systems (IDS) (Abdallah *et al*. 2024), which monitor and evaluate data flow to detect any security threats that could compromise system integrity and user privacy, are a key part of

*Corresponding author, Ph.D., E-mail: sudhareddychinnakka@gmail.com
[a]Associate Professor, Email: sreenivasb8@gmail.com

http://www.techno-press.org/?journal=acd&subpage=7 ISSN: 2383-8477 (Print), 2466-0523 (Online)

cyber security (Nivaashini *et al*. 2024). Deep learning (DL) (Altunay *et al*. 2023) and machine learning (ML) (Ferrag *et al*. 2024) methods effectively improve IDS performance by improving pattern analysis and anomaly detection (Mishra *et al*. 2023). To handle big data applications, techniques such as Deep Belief Networks (DBN) (Hnamte *et al*. 2023), Long Short-Term Memory (LSTM), (Mishra *et al*. 2023) and Convolutional Neural Networks (CNN) are commonly used (Ahmad *et al*. 2024). These methods improve detection accuracy and support threat analysis (Mansouri *et al*. 2025). Classifiers like Random Forests (Govindaraj *et al*. 2024) can help the system discriminate between various forms of threats (Kandhro *et al*. 2023); Deep Neural Networks (DNN) (Singh *et al*. 2025) and gradient-boosted trees are used to classify threats into multiple classes (Abdelkader *et al*. 2024).

Traditional ML methods (Gangula *et al*. 2023) faced difficulties when used in intrusion detection since shallow structures, complexity, and susceptibility to noise in large-volume data environments characterize them (Gangula *et al*. 2023). DL-based IDS, on the other hand, employs methods like feature extraction, anomaly classification, and information fusion to facilitate expert threat detection and security evaluation (Shailaja *et al*. 2023). The methods improve collective decision-making, facilitate early risk detection, and promote active avoidance of problems (Gangula *et al*. 2022) With increasing reliance on internet-based platforms, the protection of user accounts and sensitive information is a matter of high priority for business organizations and web-based social communities (Gangula *et al*. 2024).

IDS perform a vital role in the monitoring and analysis of malicious and innocuous traffic within a network (Gangula *et al*. 2023). However, one of the persistent IDS problems is its excessive false positive alarm rate, which obscures true security events (Gangula *et al*. 2022). Fixing the same is a high priority in a bid to make the system more trustworthy and ensure the prevention of cyber intrusions (Gangula *et al*. 2024). The main contribution of this study can be outlined as follows:

- Initially, the social network intrusion detection data was considered and trained on the Python system.
- Moreover, a new framework known as the Coati Attention Transformer Prediction (CATP) was developed, and preprocessing is performed in the hidden layer
- Furthermore, the current features were examined and projected using the coati optimal features. Consequently, attack categories were predicted and classified based on several classifications.
- Performance was measured based on accuracy, precision, recall, F1-score, and error rate, and comparison is made with other traditional models.

The paper is broken into several sections. The second portion of this thesis examines the relevant research literature. While the fourth section looks at a detailed discussion of the proposed technique, the third section discusses the limitations. Section Five analyzes and compares the results, while Section Six presents the conclusions.

2. Literature review

Several current related studies are outlined below,

Mary *et al*. (2024) have created a novel feature selection approach that combines the Aquila Optimizer (AO) and Fuzzy Entropy Mutual Information (FEMI) algorithms. The CICDDoS2019 and ToN-IoT datasets have been used to validate this method, and various performance indicators

have been used to evaluate its effectiveness. Simulation results indicate that this method surpasses existing techniques and exhibits a strong resilience in detecting network intrusions. Nevertheless, a notable limitation of this study is the computational complexity associated with the implementation of various optimization strategies.

Qaddos *et al*. (2024) created the Horse Herd Optimization method (HOA), a quantum-inspired method for detecting network intrusions. This algorithm uses horse behaviour and a K-nearest neighbor classifier to identify intrusive features. This algorithm has a 6% success rate and 99.8% accuracy but requires increased computational overhead.

Noori *et al*. (2023) refined the GP-connector by creating the Dynamic Feature Aware GP Ensemble (DFA-GPE). It tackles the issue of feature drift through the implementation of variable-length multi-objective particle swarm optimization (VLMO-PSO) and introduces an innovative method for prototype selection. DFA-GPE achieves 99.09% and 92.64% accuracy on standard datasets but may cause information loss due to feature set reduction, which may affect classification results.

Keshk *et al*. (2023) created a unique explainable intrusion detection methodology designed for IoT networks. This approach utilizes an LSTM model to identify cyberattacks and elucidate the rationale behind its decision-making. Implementing a distinctive SPIP framework for the training and assessment of the LSTM model surpasses alternative methods in detection accuracy, processing speed, and interpretability. This technique can aid administrators and decision-makers in understanding complex attack behaviours. However, developing attack patterns causes challenges for the LSTM-based IDS.

The networks of the Internet of Things (IoT) are becoming progressively essential for applications that require real-time functionality. Still, they are vulnerable to security threats due to a lack of effective security measures. A new ID using a DL model, specifically whale-integrated LSTM (WILS) networks, was presented by Jyoti *et al*. (2023). A data collection unit in this system detects hostile devices during attacks and predicts different types of attacks to be expected. Nevertheless, it faces challenges related to limited processing power and memory capacity.

Madhuridevi *et al*. (2025) have developed an intrusion detection system based on a hybrid convolutional neural network and long short-term memory (CNN-LSTM) with Cat Swarm Elephant Optimisation (CSEO) for managing large amounts of data. It determines relevant class differences by using enhanced min-max normalization, correlation, and flow feature extraction. The model outperforms other models, as shown by its validation over conventional models. By attaining a high accuracy of 95.029%, it increases the computational complexity.

Asif (2025) introduced an innovative optimized Ensemble stacked network (OESN) method for identifying intrusion in diverse networks. It provides reliable and accurate intrusion detection via the use of deep neural networks and ensemble learning. Using a stacking technique, the framework integrates three pre-trained convolutional neural networks. The discriminative skills of the models are improved via a new channel and spatial attention method. It achieves high accuracy on four difficult datasets and proves its generalizability, but the limitation is that it consumes more time.

Salehpour *et al*. (2025) have focused on enhanced security in medical networks and introduced a resource-efficient detection framework by using ensemble-based ranking techniques (EbRT). The system aims to strike a compromise between detection accuracy and processing economy, and Random Forest is selected for the final classification. Tested on three benchmark datasets, the system demonstrated significant improvements in detecting DDoS and DoS attack types. Though it performs well in three different datasets, it is limited in classifying different types of intrusions.

Benmalek and Seddiki, (2025) have proposed an intrusion detection system that makes use of

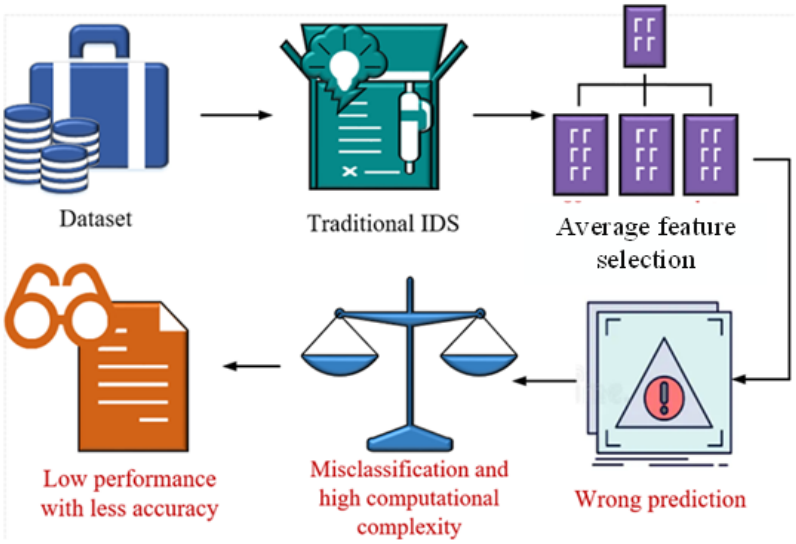

Fig. 1 Limitations of existing models

machine learning and deep learning with particle swarm optimisation models (MLDL-PSO). The system optimizes and selects features via PSO, which boosts model performance. To distinguish between malicious and regular assaults. A comprehensive evaluation is performed with multiple classifiers, and PSO demonstrates its robustness and efficiency, but these models lack in generalizability.

Vellela *et al*. (2025) have presented a novel approach by using GloVe word embeddings, a self-attention mechanism, and a Bidirectional LSTM (BiLSTM) model. The approach increases the accuracy of detection by capturing global co-occurrence correlations in network events. Principal Component Analysis is used for feature reduction after random oversampling balances attack category distributions. To increase computational efficiency, Single candidate and graylag goose optimization are used to fine-tune the model's parameters. The methodology enhances intrusion detection and ranks high-risk threats. The use of word embeddings is effective for capturing textual relationships, but it is not suitable for all types of intrusion data.

3. System model with problem description

The rapid growth of social media platforms has increased the amount of user-generated data, making them more vulnerable to cyber threats such as phishing, misinformation, illegal access, and data theft (Hajarian *et al*. 2024). Traditional IDS have issues with scalability, false positives and negatives, and adjusting to new threats (Abdulganiyu *et al*. 2024). Current models rely on fixed rules and immutable datasets, which reduce their effectiveness when creating attacks (Lu *et al*. 2025). Traditional feature extraction methods are inefficient, resulting in unnecessary data processing and delays in detection (Möller *et al*. 2023). DL-based frameworks have potential, but they demand significant computing resources. The limitations of the traditional methods are displayed in Fig. 1.

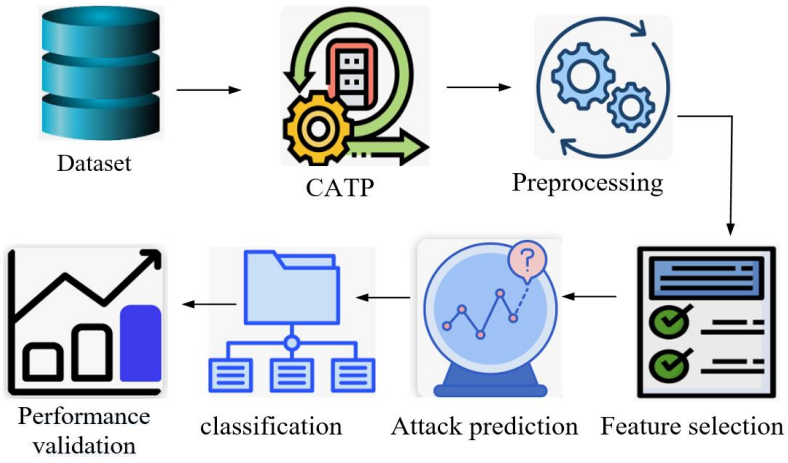

Fig. 2 Architecture of developed model

4. Proposed methodology

This research introduces the Coati Attention Transformer Prediction (CATP), which was developed to predict and classify attacks. This method involves several stages, such as preprocessing, feature extraction, prediction, and classification. The database was cleaned up during the preparation stage to remove any unnecessary noise. Following that, characteristics were retrieved from the cleaned data, and CATP was used to predict and categorize assaults in the dataset. The proposed architecture is illustrated in Fig. 2.

4.1 Process of the proposed CATP

The Coati Attention Transformer Prediction (CATP) system combines the Coati Optimization Algorithm (COA) (Dehghani *et al*. 2023), attention algorithms, and transformer to identify intrusions. This process begins with data preprocessing, which removes noise to ensure the dataset is clean. Next, COA is used to improve feature selection by mimicking the natural hunting and escape behaviours of coatis to determine the most important characters. These selected features are predicted using an attention process that provides appropriate estimates for key patterns in the data. A transformer-based classification model is used to estimate feature correlations and predict attack types. The classification was performed based on feature importance scores from COA and attention processes. This hybrid technique increases intrusion detection accuracy, improves feature extraction, reduces system complexity, and creates a more efficient cyber security system.

4.1.1 Initialize the data

The current detection system's data initialization takes data directly from the standard Kaggle repository and trains it in a Python environment. This process began with the successful transformation of the data into a data frame structure suitable for numerical and categorical analysis. Data initialization primarily involves establishing a fundamental data structure where each row corresponds to a network connection, and each column signifies the associated attribute. The initialization method described in Eq. (1).

$$Z(d) = \{R1, R2, R3 \ldots . Rm\} \tag{1}$$

Here, $Z(d)$ indicates the initialized dataset, $(R1, R2, R3)$ and the row in the dataset Rm indicates the total count of features. After the initialization process, the preprocessing was started.

4.1.2 Data preprocessing

Preprocessing attempted to improve the dataset by reducing noise. This included managing missing data and standardizing numerical attributes. The purpose of the min-max scaler is to identify and correct the components that cause excessive noise during training. The preprocessing method is expressed in Eq. (2).

$$N = \frac{a_i - min(a)}{max(a) - min(a)} \tag{2}$$

Here, N indicates the preprocessing variable, $max(a), min(a)$ indicates the minimum and the maximum characters, a_i and indicates the original dataset. This procedure ensured that the dataset was clean, consistently structured, and ready for the feature selection and model training steps.

4.1.3 Feature selection

The feature selection approach uses the COA to find the most important characteristics by repeatedly updating the coat positions depending on hunting and escape techniques. And they optimize their locations during the exploitation phase, ensuring convergence towards the best solution. Only those features that improve prediction performance are retained after being evaluated by the objective function. The mathematical representation of the feature selection process is as follows: Eq. (3).

$$Fi = \frac{max(F_{best} - Sf)}{1 + e^{-E}} \tag{3}$$

The Feature Selection is symbolized by Fi. The intensity of exploitation, represented by E, determines local optimum solutions and can be tuned for optimization. The e^{-E} word represents the influence of exploitation on convergence. F_{best} indicates the best fitness value

4.1.4 Attack Prediction

For intrusion prediction, an attention model is very helpful because it improves the system's ability to focus on important characteristics in user behaviour. Dynamically assigning importance to input features ensures that the model prioritizes relevant information over noise, which increases the accuracy of intrusion prediction. The mathematical representation of the prediction process is as follows: Eq. (4).

$$P_a = fitness(X_{best}) + \alpha \cdot Fi \tag{4}$$

Here, P_{attack} denotes the prediction process variable, Fi indicates the outcomes of the feature selection process, α and the weighting factor, X_{best} denotes the best solution.

4.1.5 Classification

Following the prediction of an attack, specific types of attacks in the dataset can be identified using a classification method. The recognition can be divided into six groups. After that, a

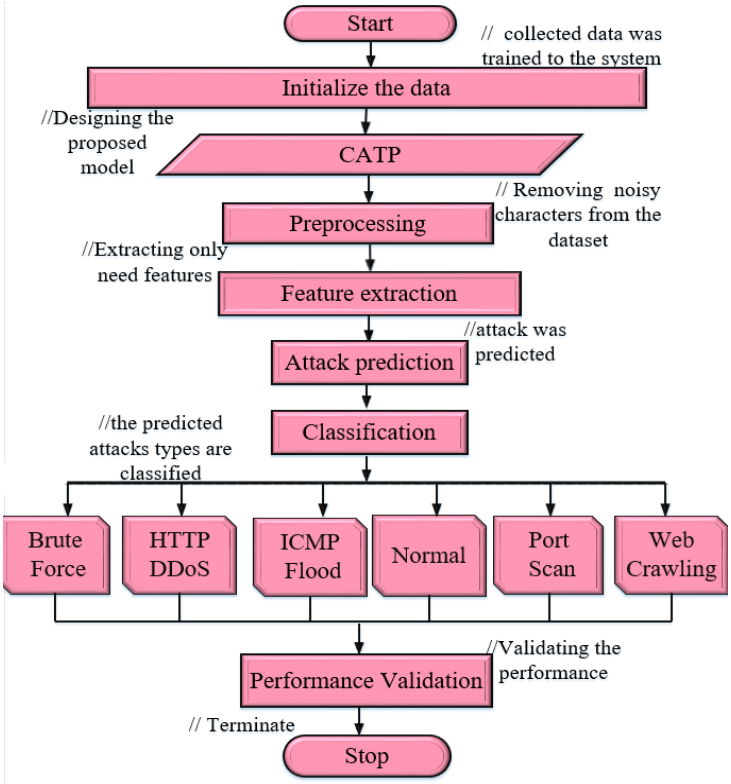

Fig. 3 Flowchart of the CATP

transformer is used to do the categorization operation. The classification process can be carried out as specified in Eq. (5).

$$C_T = \begin{cases} if(P_a = 0)Bruteforce \\ if(P_a = 1)HTTPDDoS \\ if(P_a = 2)ICMPFlood \\ if(P_a = 3)Normal \\ if(P_a = 4)PortScan \\ if(P_a = 5)WebCrawling \end{cases} \quad (5)$$

Here, C_T indicate the classification variable $0,1,2,3,4 and 5$represents the attack classes. The attack types are HTTP DDoS, Normal, Port Scan, Web Crawling, Brute Force, and ICMP Flood. Social media apps are at risk of being exposed to many types of cyber threats, including brute force attacks, in which attackers try to guess passwords through repeated login attempts, and HTTP DDoS, which are APIs with excessive requests, slow down the process. ICMP flood attacks can overload servers with message requests. Port scanning is used to detect vulnerabilities, which is often the starting point for larger attacks. Web crawling is the act of gathering data with bots, often for illegal reasons like misinformation.

Fig. 3 depicts the procedure for developing the model. Algorithm 1 depicts the proposed CATP algorithm in sequential order, using pseudocode to demonstrate the complete process.

Algorithm 1 CATP

	Start
Step: 1	Data initialization() Required variables were initialized
Step: 2	Preprocessing () $enable \rightarrow min\_max \quad scalar$ perform regularization and dropout Noisy features and redundancy data was managed
Step: 3	Feature selection() $enable \rightarrow coati \quad optimal \quad Features$ present features in the data was extracted
Step: 4	Attack Prediction () $Pr\,e\,dict \rightarrow Attack \quad features$ Attack features were predicted based on coati food searching behavior
Step: 5	Classification () Attack classification with different classess
	Stop

Table 1 Requirement specification

Requirement	Description
Programming platform	Python
OS	Windows 10
Version	3.7.6
Dataset	MSCAD
Data count	128799
Optimization	Coati

5. Results and discussion

The novel CATP algorithm was evaluated in Python and executed on the Windows 10 operating system. Initially, the social network intrusion detection data was considered and trained in the system. The CATP framework was implemented for the analysis process. The description of the parameter is presented in Table 1. The hyper parameters of the CATP algorithm is activation function Relu, batch size 25, learning rate 0.01, optimizer coati, iteration 100, maximum epoch 50, 3 hidden layers and 2 filters.

5.1 Case study

A series of validation experiments were conducted to assess the efficacy of the proposed method, and the findings are detailed. Additionally, an investigation was performed to verify the success of the suggested CATP strategy. The dataset served to assess the effectiveness of the models that were developed. The newly introduced CATP is utilized to evaluate the proposed

Table 2 dataset sample details

Total samples:128799	
Training(80%): 103039	
HTTP DDoS	517
ICMP Flood	33
Normal	22854
Brute Force	70827
Port Scan	8788
Web Crawling	20
Testing (20%):25760	
HTTP DDoS	124
ICMP Flood	12
Brute Force	17675
Normal	5648
Port Scan	2293

model. This dataset, referred to as the Multi-Step Cyber-Attack Dataset (MSCAD), was sourced from the official Kaggle website.
(/https://www.k aggle.com/datasets/drjamailalsawwa/mscad?select=MSCAD.csv//)

The MSCAD dataset, evaluated using Wireshark, includes 77 network metrics labelled by traffic type. The dataset comprises (port scan, DDoS, normal, web crawling, and brute force). It also has two multi-step cyber-attack scenarios. Multi-step Attack Scenario A, an attacker plans to execute a password cracking operation by employing a port scan, the HTTrack Website Copier, and a password list containing 47 and 10 entries. In Multi-step assault Scenario B, an attacker launches a volume-based DDoS assault with a port scan, HTTP Slow Loris DDoS, and Radware tools. The data was split using 80:20 ratios. The dataset details are illustrated in Table 2.

The MSCAD dataset consists of 128,799 samples, 80 percent of which are reserved for training, totaling 103,039 samples and 20 percent for testing, totaling 25,760 samples. The data categorization includes 88,502 instances of brute force attacks, 28,502 instances of normal traffic, 11,081 port scans, 641 HTTP DDoS attacks, 45 ICMP floods, and 28 web crawling activities.

The CATP accuracy validation is continuing, and the usefulness of the attack prediction system is proven by extracting scores from training and testing validation. The loss value measures the mistake rate, and these metrics are evaluated concurrently throughout the test validation and training phases. Validation of the accuracy of the CATP suggested in the accuracy and loss curve (Fig. 4) is now underway.

The outcomes of the expected prediction were illustrated in a confusion matrix shown in Fig. 5. The classification results were detailed as positive and negative scores corresponding to true and false categories. The forecasts were divided into six categories: ICMP Flood, Normal, HTTP DDoS, Port Scan, and Web Crawling, Brute Force.

5.2 Performance analysis

The assessment is carried out using metrics including recall, F1-score, Precision, error rate, and

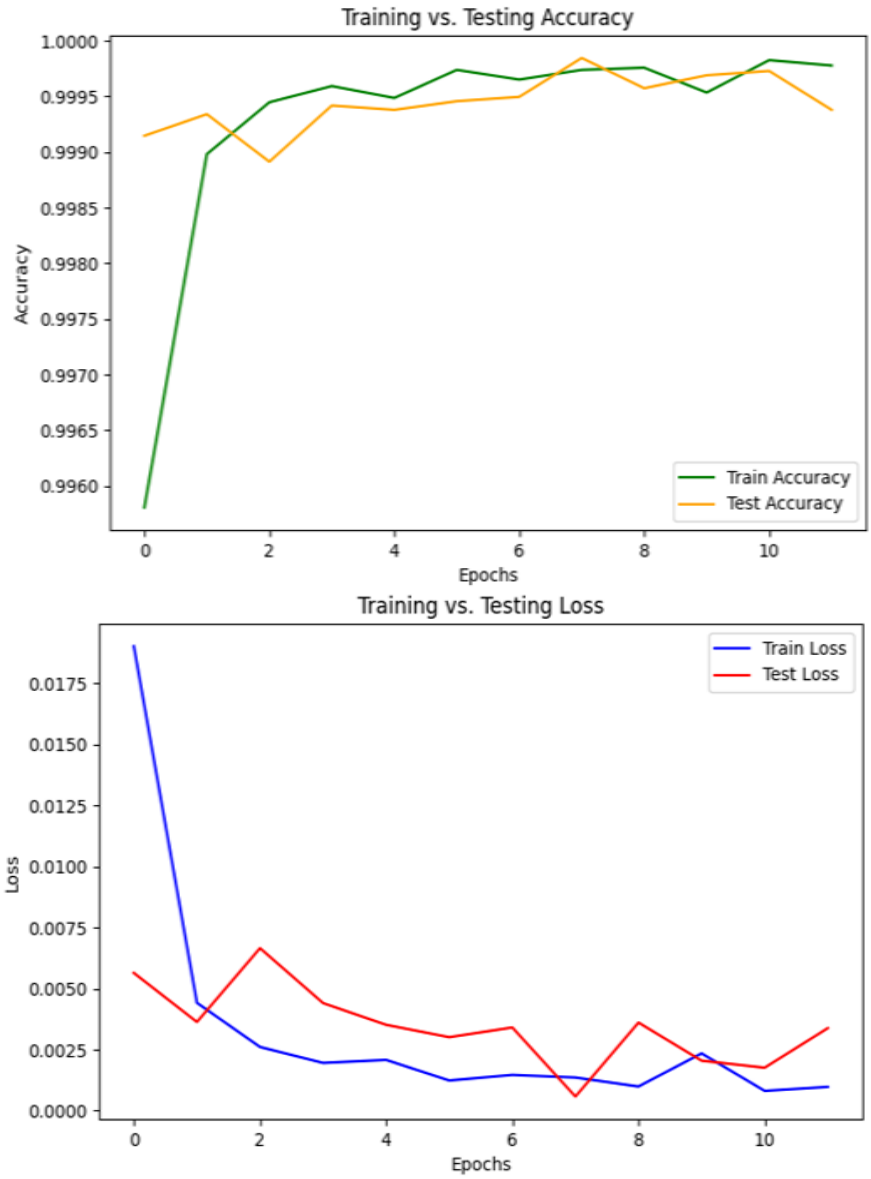

Fig. 4 Accuracy and loss curve

accuracy. The success of the suggested method is compared against various ML techniques, including Gated Recurrent Unit (GRU) (Ali *et al*. 2024), Naïve Bayes (NB) (Ali *et al*. 2024), LSTM (Ali *et al*. 2024), Random Forest (RF) (Ali *et al*. 2024), Multilayer Perceptron (MLP) (Ali *et al*. 2024), and Instance-based IDS for ICS networks (ICS-IDS) (Ali *et al*. 2024).

5.2.1 Recall

The recall was calculated as the ratio of correctly predicted positive events to the total number of actual positive occurrences. The GRU model demonstrated a recall of 86.32% and the MLP

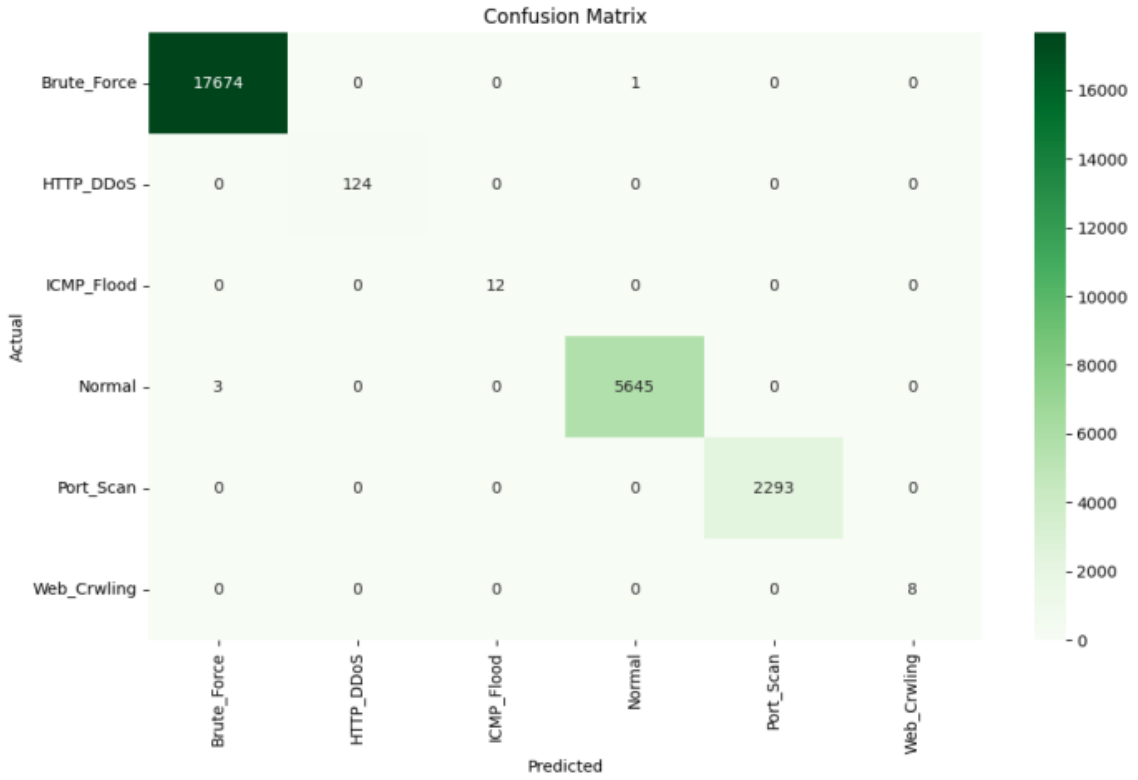

Fig. 5 Confusion matrix

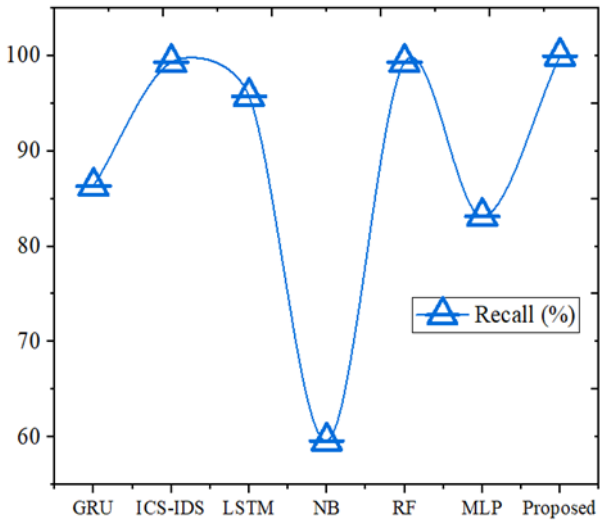

Fig. 6 Correlation of recall

83.15% in detecting intrusions, while the LSTM showed a better performance of 95.75%. The NB method had a poor recall of 59.60% in complex systems. The RF model showed a recall of 99.75%

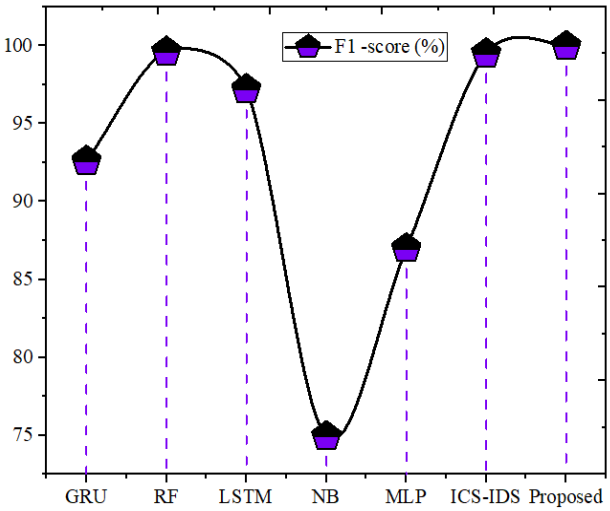

Fig. 7 Correlation of F1-score

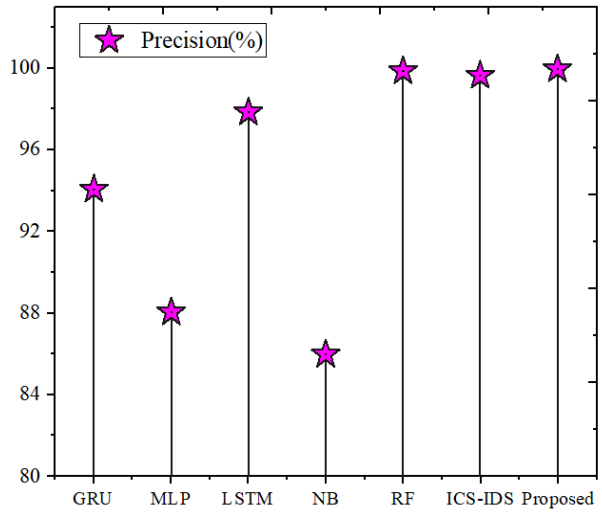

Fig. 8 Correlation of the Precision

in classification tasks, while the ICS-IDS had a powerful detection ability of 99.58%. The improved CATP model outperformed all previous methods, achieving 99.98% recall. Fig. 9 shows the recall correlations.

5.2.2 F1-Score

It determines a singular score by averaging recall and Precision. Fig. 7 shows the F1-score. Various intrusion detection techniques have limited F1-scores, which are a measure of Precision and recall. The MLP and LSTM models recorded F1 scores of 86.98% and 97.52%, respectively, whereas the GRU model attained an F1 score of 92.60%. The ICS-IDS model achieved an

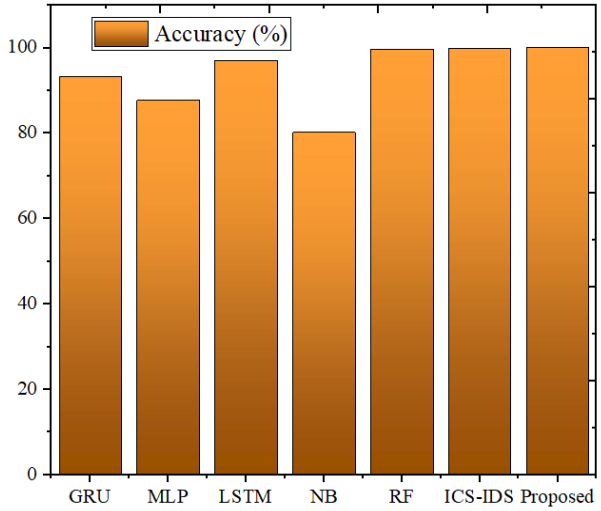

Fig. 9 Correlation of accuracy

impressive F1 score of 99.66%, while the Random Forest model reached an F1 score of 99.87%. The recommended CATP model performed better than any other strategy, with an excellent F1 score of 99.98%.

5.2.3 Precision

Accuracy is calculated by taking the total number of attacks recorded in the data and dividing it by the number of attacks that were predicted correctly.

The correlation of accuracy is clearly seen in Fig. 8. The accuracy of various intrusion detection methods is as follows: GRU achieved 94.07%, MLP achieved 88.05%, LSTM achieved 97.86%, NB obtained 85.98%, RF performed at 99.88%, ICS-IDS achieved 99.66%, and the suggested CATP model attained the maximum Precision of 99.98%, resulting in fewer false positives and more precise threat identification.

5.2.4 Accuracy

Accuracy is determined by the proportion of correctly identified attack types to the overall dataset. The success rate of various IDS is assessed as follows: The GRU technique achieved an accuracy of 93.21%, the MLP recorded 87.74%, the LSTM reached 97.60%, the NB obtained 80.24%, the RF performed at 99.87%, and the ICS-IDS achieved 99.96%. Notably, the suggested CATP model outperformed all others with an accuracy of 99.98%. The correlation of accuracy is seen in Fig. 9.

5.2.5 Error rate

The error rate metrics are utilized to assess the frequency of misclassifications made by the model. This metric is determined by dividing the total count of incorrect predictions by the overall number of datasets.

Fig. 10 shows the correlation of error rates for several intrusion detection methods: GRU recorded 6.79%, MLP recorded 12.26%, LSTM reached 2.4%, and NB had the highest error rate at

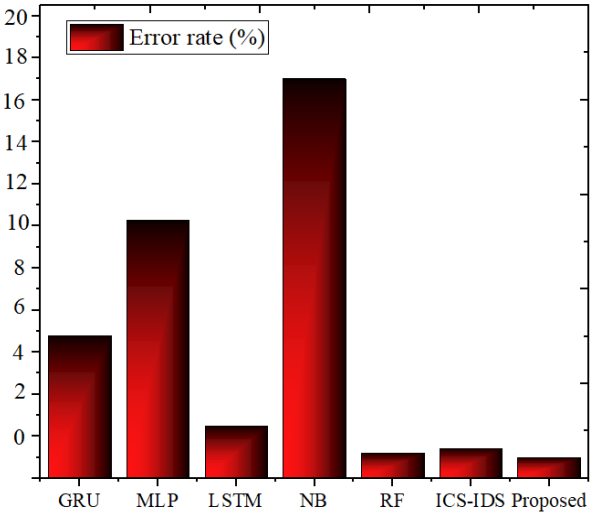

Fig. 10 Correlation of error rate

Table 4 Ablation study for the proposed with existing models

Methods	Convolutional neural network	Transformer model	particle swarm optimization	Elman network with GA	Proposed
Accuracy (%)	76	80	78.5	86.5	99.97
Recall (%)	76	80.3	78.5	86	99.97
Precision (%)	76.1	80.4	78.5	86	99.97
F1-Score (%)	76	80.35	78.5	86	99.97
Error Rate (%)	24	20	21.5	86	0.03

19.76%, indicating poor reliability. RF showed the lowest error rate of 0.2%, while ICS-IDS improved by 0.04%. The proposed CATP model had the lowest error rate of 0.02%.

5.3 Discussions

This study designs the CATP model, and the contribution of this article is to improve the performance successfully. The testing of the resulting data shows that the suggested model performs well in assault categorization. Furthermore, its stability is assessed and compared with other models to ensure its effectiveness. To justify the proposed model further, some of the traditional models like Convolutional neural network, Transformer model, Particle swarm optimization, and Elman network with Genetic algorithm (GA). Here, all the models were executed in the same proposed platform and outcomes were compared with each other. In addition, to make the cross-validation, the data was processed in the form of 70% training and 30% testing.

The comparative study demonstrates that the developed model has achieved extraordinary results compared to other techniques. The success rate of the recommended model is depicted in Table 4. The proposed model excels in intrusion detection with an F1-score of 99.98%, demonstrating a high combination of Precision and recall. It accurately identifies most true positive cases with 99.98% accuracy, ensuring accurate predictions without false alarms. The

model's 99.98% accuracy and low error rate of 0.02% ensure minimal misclassification, demonstrating its durability and reliability. In addition, to avoid the overfitting and data leakage, the regularization and dropout function (Salehin *et al*. 2023) is performed in the preprocessing phase. It can avoid the overfitting and data leakage issues.

6. Conclusions

The research paper aimed to create a CATP with the ability to predict and classify attacks. The system was trained using data from the Kaggle platform, preprocessed to remove noise variations, and used the best features of the coati to examine and predict current features. The CATP is used to predict attack types and classification using various classifications. The comparative analysis indicates that the proposed model demonstrates superior stability compared to existing models. The effectiveness of the model is evaluated through various metrics, including Precision, F1-score, error rate, accuracy, and recall. Furthermore, a case study was conducted to confirm the performance of the developed model. The suggested model exhibits an outstanding success rate, achieving an F1-score of 99.98%, a recall of 99.98%, a precision of 99.98%, an error rate as minimal as 0.02%, and an accuracy of 99.98%. Future work should include advanced deep learning models, hybrid feature selection strategies, adaptive learning mechanisms, and a larger dataset range to improve the CATP system's prediction accuracy, classification efficiency, and resilience. Furthermore, the models investigated in this study will be included in an IDS prototype for testing with various data, including a variety of threats, to confirm the system's multi-class capability and efficacy.

References

Abdallah, A., Alkaabi, A., Alameri, G., Rafique, S.H., Musa, N.S. and Murugan, T. (2024), "Cloud network anomaly detection using machine and deep learning techniques-recent research advancements", *IEEE Access*, **12**, 56749 - 56773. https://doi.org/10.1109/ACCESS.2024.3390844

Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.E.A. and Prokop, L. (2024), "Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks", *Results Eng*., 102647. https://doi.org/10.1016/j.rineng.2024.102647

Abdulganiyu, O.H., Tchakoucht, T.A. and Saheed, Y.K. (2024), "Towards an efficient model for network intrusion detection system (IDS): systematic literature review", *Wirel. Netw*., **30**(1), 453-482. https://doi.org/10.1007/s11276-023-03495-2

Acampa, S., Crescentini, N. and Padricelli, G.M. (2023), "Between alternative and traditional social platforms: the case of gab in exploring the narratives on the pandemic and vaccines", *Front. Sociol*., **8**, 1143263. https://doi.org/10.3389/fsoc.2023.1143263

Ahmad, R. and Alsmadi, I. (2024), "Data fusion and network intrusion detection systems", *Cluster Comput*., **27**(6), 7493-7519. https://doi.org/10.1007/s10586-024-04365-y

Ali, B.S., Ullah, I., Al Shloul, T., Khan, I.A., Khan, I., Ghadi, Y.Y. and Hamam, H. (2024), "ICS-IDS: application of big data analysis in AI-based intrusion detection systems to identify cyberattacks in ICS networks", *J. Supercomput*., **80**(6), 7876-7905. https://doi.org/10.1007/s11227-023-05764-5

Altunay, H.C. and Albayrak, Z. (2024), "A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks", *Eng. Sci. Technol. Int. J*., **38**, 101322. https://doi.org/10.1016/j. jestch.2022.1013 22

Asif, S. (2025), "OSEN-IoT: An optimized stack ensemble network with genetic algorithm for robust

intrusion detection in heterogeneous IoT networks", *Expert Syst. Appl.*, **276**, 127183. https://doi.org/10.1016/j.eswa.2025.127183

Benmalek, M. and Seddiki, A. (2025), "Particle swarm optimization-enhanced machine learning and deep learning techniques for Internet of Things intrusion detection", *Data Sci. Manag.*, In Press. https://doi.org/10.1016/j.dsm.2025.02.005

Dehghani, M., Montazeri, Z., Trojovská, E. and Trojovský, P. (2023), "Coati Optimization Algorithm: A new bio-inspired metaheuristic algorithm for solving optimization problems", *Knowl. Based Syst.*, **259**, 110011. https://doi.org/10.1016/j.knosys.2022.110011

Ehiane, S.O., Olumoye, M.Y. (2023), "Introduction and Contextual Background of Cybercrime as an Emerging Phenomenon in Africa", *In Cybercrime and Challenges in South Africa Singapore: Springer Nature Singapore*, 1-28. https://doi.org/10.1007/978-981-99-3057-9_1

Ferrag, M.A., Ndhlovu, M., Tihanyi, N., Cordeiro, L.C., Debbah, M., Lestable, T. and Thandi, N.S. (2024), "Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices", *IEEE Access*, **12**, 23733-23750. https://doi.org/10.1109/ACCESS.2024.3363469

Gangula, R., Mohan. V.M. and Kumar. R. (2022), "Comprehense study of DDoS Attack Detecting algorithm using GRU-BWFA classifier", *Measur. Sens.*, **24**, 100570. https://doi.org/10.1016/j.measen.2022.100570.

Gangula, R., Pratapagiri, S., Bejugama, S.M., Ray, S., Nandam, G. and Saturi, S. (2023), "A novel intelligent intrusion prevention framework for network applications", *Wirel. Pers. Commun.*, **131**(3), 1833-1858. https://doi.org/10.1007/s11277-023-10523-z

Gangula, R., Vutukuru, M.M. and Kumar, R. (2024), "Hybridization of bottlenose dolphin optimization and artificial fish swarm algorithm with efficient classifier for detecting the network intrusion in Internet of Things (IoT)", *Int. J. Intell. Syst. Appl. Eng.*, **12**, 220-232.

Gangula, R. and Vutukuru, M.M. (2022), "Network intrusion detection system for Internet of Things based on enhanced flower pollination algorithm and ensemble classifier", *Concurr. Comput. Pract. Exp.*, **34**(21), e7103. https://doi.org/10.1002/cpe.7103

Gangula, R., Vutukuru, M.M. and Kumar M.R. (2024), "Stacked autoencoder with weighted loss function for intrusion detection in IoT application", *Multimed. Tool Appl.*, 1-29. https://doi.org/10. 1007/s11042-024-19962-7.

Gangula, R., Vutukuru, M.M. and Kumar M.R. (2023), "Network intrusion detection method using stacked bilstm elastic regression classifier with aquila optimizer algorithm for internet of things (IoT)", *Int. J. Recent Innov. Trends Comput. Commun.*, **11**(2s), 118-131. https://doi.org/10.17762/ijritcc.v11i2s.6035

Gangula, R., Vutukuru, M.M. and Ranjeeth Kumar, M. (2023), "Intrusion attack detection using firefly optimization algorithm and ensemble classification model", *Wirel. Pers. Commun.*, **132**(3), 1899-1916. https://doi.org/10.1007/s11277-023-10687-8

Govindaraj, M., Asha, V., Marutheesha, H., Kumar, M.D.S., Muniprasad, M. and Ramesh, N. (2024), "IntelliSecure AI-powered intrusion detection framework", *Proceedings of the 2024 International Conference on Inventive Computation Technologies (ICICT)*, 365-370. https://doi.org/10.1109/ICICT60155.2024.105444 35

Hajarian, M., Diaz, P. and Aedo, I. (2024), "On privacy, security and trust for misuse prevention in social networks", *Proceedings of the 2024 International Symposium on Networks, Computers and Communications (ISNCC)*, 1-4. https://doi.org/10.1109/ISNCC62547.20 24.10759034

Hang, F., Xie, L., Zhang, Z., Guo, W. and Li, H. (2024), "Research on the application of network security defence in database security services based on deep learning integrated with big data analytics", *Int. J. Intell. Netw.*, **5**, 101-109. https://doi.org/10.1016/j.ijin.2024.0 2.006

Hnamte, V., Nhung-Nguyen, H., Hussain, J. and Hwa-Kim, Y. (2023), "A novel two-stage deep learning model for network intrusion detection: LSTM-AE", *IEEE Access*, **11**, 37131-37148. https://doi.org/10.1109/ACCESS.2023.3266979

Jothi, B. and Pushpalatha, M. (2023), "WILS-TRS—A novel optimized deep learning based intrusion detection framework for IoT networks", *Pers. Ubiquit. Comput.*, **27**(3), 1285-1301. https://doi.org/10.1007/s00779-021-01578-5

Kamyab, H., Khademi, T., Chelliapan, S., SaberiKamarposhti, M., Rezania, S., Yusuf, M. and Ahn, Y. (2023), "The latest innovative avenues for the utilization of artificial Intelligence and big data analytics in water resource management", *Results Eng*., **20**, 101566. https://doi.org/10.1016/j.rineng.2023.101566

Kandhro, I.A., Alanazi, S.M., Ali, F., Kehar, A., Fatima, K., Uddin, M. and Karuppayah, S. (2023), "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures", *IEEE Access*, **11**, 9136-9148. https://doi.org/10.1109/ACCESS.2023.3238664

Keshk, M., Koroniotis, N., Pham, N., Moustafa, N., Turnbull, B. and Zomaya, A.Y. (2023), "An explainable deep learning-enabled intrusion detection framework in IoT networks", *Inf. Sci*., **639**, 119000. https://doi.org/10.1016/j.ins.2023.119000

Kizza, J.M. (2024), *System Intrusion Detection and Prevention*, In *Guide to computer network security*, Cham: Springer international publishing, 295-323. https://doi.org/10.1007/978-3-031-47549-8_13

Lu, H., Liu, J., Peng, J. and Lu, J. (2025), "Adversarial attacks based on time-series features for traffic detection", *Comput. Secur*., **148**, 104175. https://doi.org/10.1016/j.cose.2024.104175

Madhuridevi, L. and Sree Rathna Lakshmi, N.V.S. (2025), "Metaheuristic assisted hybrid deep classifiers for intrusion detection: a big data perspective", *Wirel. Netw*., **31**(2), 1205-1225. https://doi.org/10.1007/s11276-024-03815-0

Mansouri, F., Tarhouni, M., Alaya, B. and Zidi, S. (2025), "Distributed intrusion detection framework for vehicular ad hoc networks via federated learning and blockchain", *Ad Hoc Netw*., **167**, 103677. https://doi.org/10.1016/j.adhoc.2024.10 3677

Mary, D.S., Dhas, L.J.S., Deepa, A.R., Chaurasia, M.A. and Sheela, C.J.J. (2024), "Network intrusion detection: An optimized deep learning approach using big data analytics", *Expert Syst. Appl*., **251**, 123919. https://doi.org/10.1016/j.eswa.2024.123919

Mishra, A.K. and Paliwal, S. (2023), "Mitigating cyber threats through integration of feature selection and stacking ensemble learning: the LGBM and random forest intrusion detection perspective", *Cluster Comput*., **26**(4), 2339-2350. https://doi.org/10.1007/s10586-022-03735-8

Mishra, R. (2023), "Machine learning based intrusion detection system for network security using self-organizing map", *Proceedings of the 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, 1-6. https://doi.org/10.1109/ICDCECE57866.2023.10150881

Möller, D.P. (2023), "Guide to cyber security in digital transformation", *Gewerbestrasse*, **11**, 6330. https://doi.org/10.1007/978-3-031-26845-8

Nivaashini, M., Suganya, E., Sountharrajan, S., Prabu, M. and Bavirisetti, D.P. (2024), "FEDDBN-IDS: federated deep belief network-based wireless network intrusion detection system", *EURASIP J. Inf. Secur*., **2024**(1), 8. https://doi.org/10.1186/s13635-024-00156-5

Noori, M.S., Sahbudin, R.K., Sali, A. and Hashim, F. (2023), "Feature drift aware for intrusion detection system using developed variable length particle swarm optimization in data stream", *IEEE Access*, **11**, 128596-128617. https://doi.org/10.1109/ACCESS.2023.3333000

Qaddos, A., Yaseen, M.U., Al-Shamayleh, A.S., Imran, M., Akhunzada, A. and Alharthi, S.Z. (2024), "A novel intrusion detection framework for optimizing IoT security", *Sci. Rep*., **14**(1), 21789. https://doi.org/10.1038/s41598-024-72049-z

Rekha, S., Thirupathi, L., Renikunta, S. and Gangula, R. (2023), "Study of security issues and solutions in Internet of Things (IoT)", *Mater. Today Proc*., **80**, 3554-3559. https://doi.org/10.1016/j.matpr.2021.07.295

Salehin, I. and Kang, D.K. (2023), "A review on dropout regularization approaches for deep neural networks within the scholarly domain", *Electronics*, **12**(14), 3106. https://doi.org/10.3390/electronics12143106

Salehpour, A., Balafar, M.A. and Souri, A. (2025), "An optimized intrusion detection system for resource-constrained IoMT environments: enhancing security through efficient feature selection and classification", *J. Supercomput*., **81**(6), 783. https://doi.org/10.1007/s11227-025-07253-3

Shailaja, K., Srinivasulu, B., Thirupathi, L., Gangula, R., Boya, T.R. and Polem, V. (2023), "An intelligent deep feature based intrusion detection system for network applications", *Wirel. Pers. Commun*., **129**(1), 345-370. https://doi.org/10.1007/s11277-022-10100-w

Singh, A., Singh, S.K., Chhabra, A., Singh, G., Kumar, S. and Arya, V. (2025), *Detailed Evolution Process of CNN-Based Intrusion Detection in the Context of Network Security*, In *Digital Forensics and Cyber Crime Investigation*, 70-87, CRC Press.

Vellela, S.S., Roja, D., Purimetla, N.R., Thalakola, S., Vuyyuru, L.R. and Vatambeti, R. (2025), "Cyber threat detection in industry 4.0: Leveraging GloVe and self-attention mechanisms in BiLSTM for enhanced intrusion detection", *Comput*. *Electr*. *Eng*., **124**, 110368. https://doi.org/10.1016/j.compeleceng.2025.110368

CC