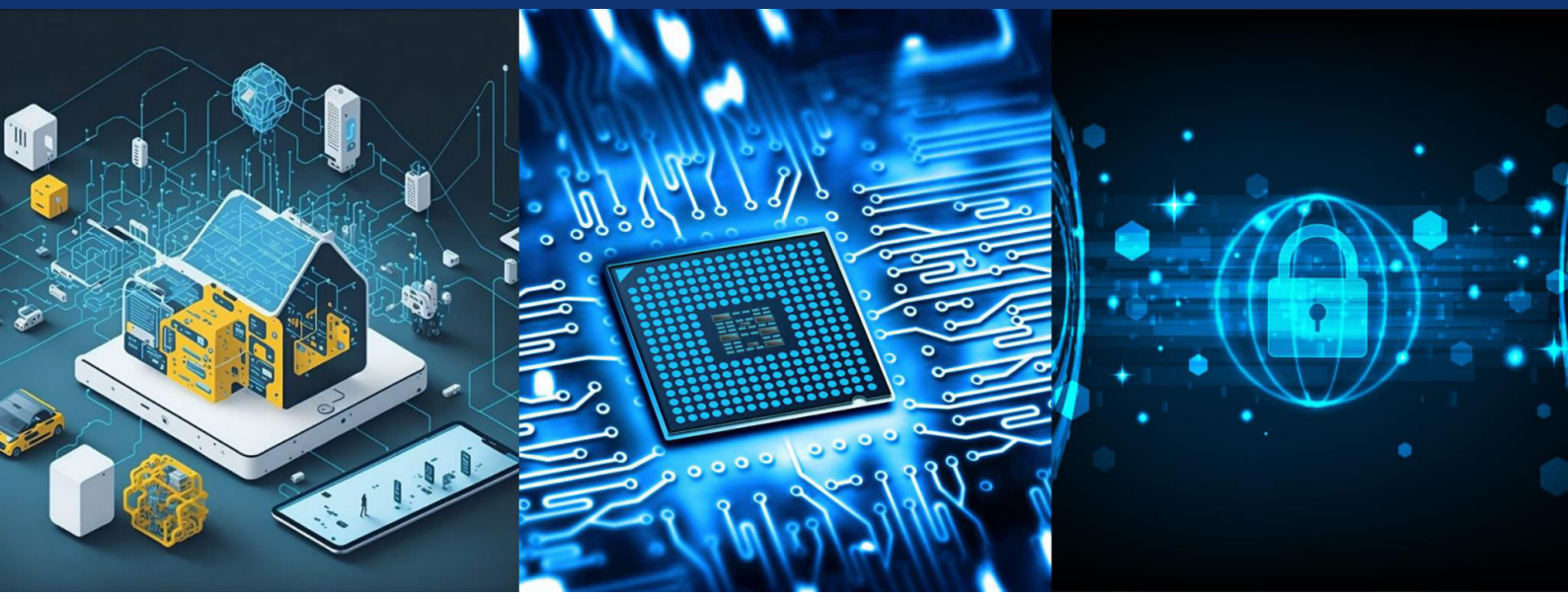
IJIRCCE

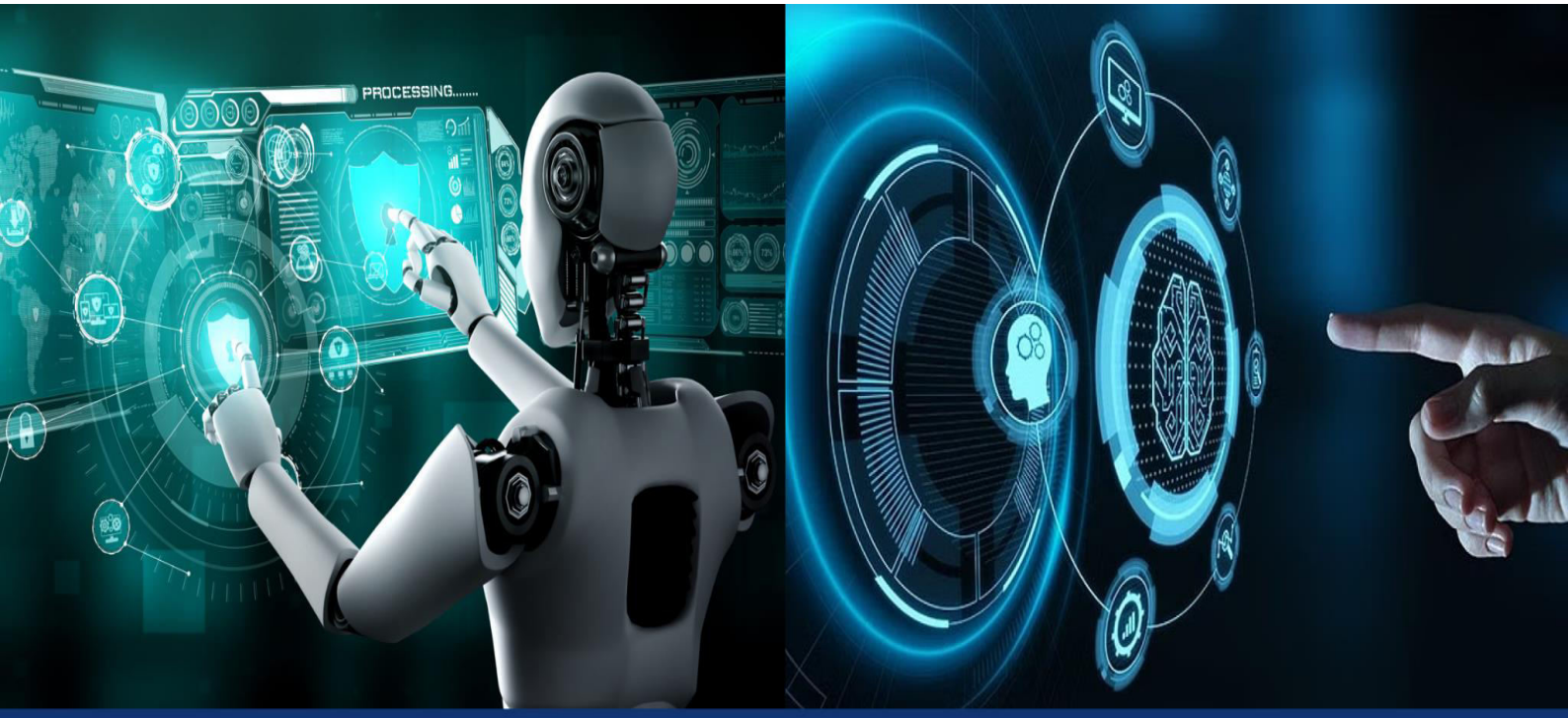
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 5, May 2025

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305024

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Secure Optimized Bi-Gru-Based Flow – Based Attacker Detection Model Using Grey Wolf Optimizer

Deepa P[1*], Arunachalam R[2], Bhuvaneswar R[3], Balamurugan R[4]

Assistant Professor, Department of ECE, Sethu Institute of Technology, Virudhunagar Dt., Tamil Nadu, India[1]

UG student, Department of ECE, Sethu Institute of Technology, Virudhunagar Dt., Tamil Nadu, India[2-4]

ABSTRACT: The increasing sophistication of cyber-attacks poses significant threats to network security, necessitating advanced detection mechanisms. This study introduces a Secure Optimized Bidirectional Gated Recurrent Unit (Bi-GRU) Based Flow-Based Attacker Detection Model that leverages deep learning and optimization for robust intrusion detection. The Bi-GRU architecture is designed to capture both forward and backward dependencies in network traffic data, enabling precise identification of anomalous patterns indicative of cyber-attacks such as Distributed Denial of Service (DDoS), phishing, and advanced persistent threats. To enhance the model's performance, the hyper parameters of the Bi-GRU, including the number of units, learning rate, and dropout rate, are meticulously tuned using the Grey Wolf Optimizer (GWO). This metaheuristic algorithm mimics the hierarchical hunting behavior of grey wolves to achieve global optimization, ensuring optimal model configuration and reduced computational overhead. The model's efficacy is further amplified by integrating specialized technologies, including feature extraction techniques tailored to high-dimensional flow data and a secure data preprocessing pipeline to handle encrypted traffic. The proposed solution demonstrates high accuracy, reduced false positive rates, and adaptability across various network environments.

KEYWORDS: Neural Network, Distributed Denial of Service, Grey Wolf Optimizer, Bidirectional Gated Recurrent Unit, K nearest neighbors

I. INTRODUCTION

Cybersecurity is increasingly vital as more services and data move online, exposing systems to a range of cyber-attacks like malware, phishing, Distributed Denial of Service (DDoS), Advanced Persistent Threats (APTs), and ransomware.

These attacks cause severe damage across industries, and traditional security methods like firewalls and antivirus software are no longer enough. These methods often rely on predefined patterns, which struggle to detect new and evolving threats. As a result, there is a growing need for more advanced, adaptive security solutions.

Machine learning (ML) and deep learning (DL) have become essential in combating these challenges. Unlike traditional approaches, ML algorithms such as Support Vector Machines (SVM) and Random Forests learn from data to detect known attack patterns. However, as threats become more complex, DL models, like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown greater promise due to their ability to handle unstructured data, such as network traffic. RNNs, specifically Long Short-Term Memory (LSTM) networks, excel at identifying sequential patterns, which is crucial for detecting anomalies in network traffic.

However, DL models require large datasets and significant computational power, making optimization critical. Traditional optimization methods can be expensive, so bio-inspired algorithms like Grey Wolf Optimizer (GWO) have emerged as efficient solutions. GWO mimics the hunting behavior of grey wolves and efficiently explores complex search spaces to fine-tune hyper parameters, improving model performance.

This study proposes a Secure Optimized Bi-GRU-Based Flow-Based Attacker Detection Model that combines the Bi-GRU model, which captures both forward and backward dependencies in sequential data, with GWO for optimization. The model is designed to detect a variety of cyber- attacks, such as DDoS and phishing, and adapt to new, unseen threats. By using GWO to optimize hyper parameters, the model ensures better performance while reducing computational Costs.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Additionally, the model incorporates feature extraction techniques for high- dimensional flow data and handles encrypted traffic, a growing concern in modern networks. This adaptability is a significant advantage over traditional systems, which struggle to detect unknown threats. Evaluations on real-world datasets show that the model achieves high accuracy, low false positives, and generalizes well across different network environments.

In conclusion, the proposed model integrates Bi-GRU deep learning with GWO optimization to offer a scalable, adaptive, and efficient solution for real-time cyber- attack detection. By combining these technologies, the model provides an advanced, dynamic approach to addressing the growing challenges of cybersecurity.

II. CLASSIFICATION OF VARIOUS CYBER ATTACKS IN NETWORK

Attacks Based on Location of an Intruder:

External Attack:
Most cyber-attacks are external in nature, where an intruder is outside the range of Network. External attacks are performed by jamming the network , exhausting the resources or denial of service (DOS).

Internal Attack:
In this type of attack, an intruder is in the range of Network. This type of attack is performed by physical tampering of node, revelation of confidential information, causing denial of service to authorized node etc.

The structure of the paper is as follows: Section II provides a comprehensive overview of the soil monitoring systems. Section III presents a proposed system of soil monitoring and forecasting aimed at improving crop yield. Section IV presents experimental results demonstrating the performance of the real-time soil monitoring system. Finally, Section V offers concluding remarks.

III. RELATED WORK

A modern network intrusion detection technology, which employs a deep feed-forward neural network method and reinforcement learning, which is based on Q- learning. In order to detect various sorts of intrusions in the network using an automated trial- and-error method and continually improve its detection skills, the Deep Q- Learning (DQL) model is proposed. The accuracy of the model proposed is 91.4%, while the accuracy of other self-taught learning models is 88.4% and it is a similar case for recall rate and precision as well which are 90.2% and 92.8%. Our experimental findings further demonstrate that our suggested DQL beats other comparable machine learning methods and is very good at identifying various intrusion classifications.

The proposed model with convolutional neural network (CNN) and deep neural network (DNN) models to create a versatile and effective IDS. Adapting IDS to handle evolving network behaviours and increasing assaults necessitates dynamic approaches with large datasets. Combining autoencoders (AE) and Long Short-Term Memory (LSTM) in our new two-stage deep learning method demonstrates effectiveness in detecting assaults using CICIDS2017 and CSE-CICDIS2018 datasets.

The comparative study of the use of modern deep learning models such as Fully Convolutional Network (FCN) and Autoencoder combined with Fully Connected Network (Autoencoder-FCN) to distinguish normal network data from attack data. This study uses CICIDS2017 dataset (over 2.8M network data records) representing real-world data and contains both normal data and attack data corresponding to the most up to date common attacks seen in modern network environments. The performance of both FCN and Autoencoder-FCN was observed to be highly accurate with the accuracy parameter being above 97% and low error rates. FCN model performs slightly better than the Autoencoder-FCN model. However, FCN model exhibited lower training time in a local deployment environment

A hybrid detection approach that uses deep learning techniques to improve intrusion detection accuracy and efficiency. The proposed prototype combines the strength of the XGBoost and MaxPooling1D algorithms within an ensemble model, resulting in a stable and effective solution. Through the fusion of these methodologies, the hybrid detection system achieves superior performance in identifying and mitigating various types of intrusions. This paper provides an overview of the prototype's architecture, discusses the benefits of using deep learning in intrusion detection, and

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

presents experimental results showcasing the system's efficacy.The identification of field crop yields stands as an extremely difficult agricultural research problem that led researchers to create multiple solution approaches. Machine learning stands as one of the technological developments which both drives and quickens learning processes. Through advanced algorithms and properly designed models he delivers specified results. Different supervised machine learning methods serve agriculture by boosting agricultural production quantities while making agricultural management operations more effective. The selection process for particular crops depends on their characteristics and environmental factors through machine learning algorithms [12]. Plant breeding has always depended on land as its most essential resource.

A deep learning (DL) based algorithm for computer network security intrusion detection is to enhance detection accuracy and minimize false alarms. This algorithm leverages the DL model to autonomously extract deep- level features from network traffic data and accurately recognize network intrusion behaviors through the construction of an efficient neural network architecture. Experimental results reveal that the proposed DL-based intrusion detection algorithm surpasses traditional ML detection methods in terms of accuracy and processing speed. This algorithm not only accurately identifies known attack behaviors but also effectively responds to unknown attack patterns, exhibiting remarkable generalization capabilities.

The intrusion detection hybrid model based on CNN (Convolutional Neural Network) and a BiLSTM (Bidirectional Long-Short Term Memory) with attention mechanism. The model consists of three main components: a CNN layer, a BiLSTM layer, and an attention layer. The CNN layer extracts local features from the network traffic data. The BiLSTM layer learns the temporal dependencies between the local features. The attention layer selects the most relevant features from the BiLSTM output for each intrusion type. Our hybrid model can effectively detect a wide range of intrusions, including Brute force, Web attacks, DDoS (Distributed Denial-of-Service). The hybrid model has several advantages over the state- of-the-art intrusion detection models. First, our model can effectively capture the complex network traffic patterns. Second, it can identify intrusions with high accuracy.

OBJECTIVES

The primary objective of this project is to develop a Secured and Optimized Bi- GRU-Based Flow-Based Attacker Detection Model for identifying malicious network activities. The model leverages Bidirectional Gated Recurrent Units (Bi- GRU) and flow-based traffic analysis to enhance the accuracy, speed, and robustness of attack detection in network environments.

IV. METHODOLOGY

The proposed system introduces a Secure Optimized Bidirectional Gated Recurrent Unit (Bi-GRU) Based Flow-Based Attacker Detection Model, designed to improve network security by effectively identifying cyber-attacks. The system begins with the collection of network traffic data, which includes flow-based features such as packet size, source and destination IP, and protocols. To address the challenge of encrypted traffic, the system integrates a secure data preprocessing pipeline that extracts essential features, ensuring the model can handle encrypted flows without compromising data privacy.

Once the data is preprocessed, feature extraction techniques are employed to reduce the dimensionality of the high-dimensional flow data, focusing on the most relevant indicators for attack detection. The heart of the system lies in the Bi-GRU architecture, chosen for its ability to capture both forward and backward temporal dependencies in network traffic. This enables the detection of complex attack patterns such as Distributed Denial of Service (DDoS), phishing, and Advanced Persistent Threats (APTs), which evolve over time. The Bi-GRU architecture is trained to learn these dependencies, providing an in-depth understanding of both short-term and long-term network behavior.

Once deployed, the model continuously monitors incoming network traffic, classifying it as either benign or malicious based on learned attack patterns. The system is capable of detecting a wide range of cyber-attacks, alerting network administrators in real time when potential threats are identified. The proposed system's ability to adapt to encrypted traffic and its scalability across different network environments make it a robust solution for protecting digital infrastructures against an increasing variety of cyber threats.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305024

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

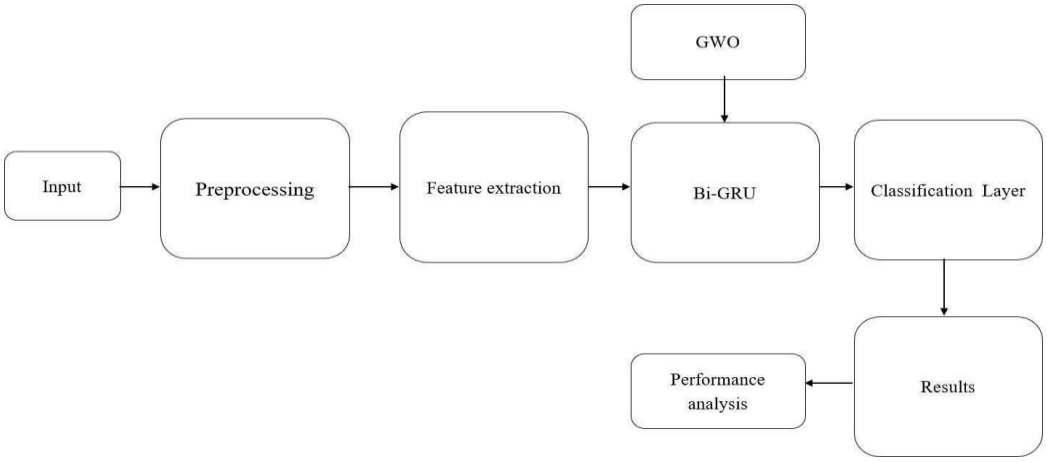


Fig.1 Proposed system

In order to mathematically model the social hierarchy of wolves when designing GWO, we consider the fittest solution as the alpha (α). Consequently, the second and third best solutions are named beta (β) and delta (δ) respectively. The rest of the candidate solutions are assumed to be omega (ω). In the GWO algorithm the hunting (optimization) is guided by α , β, and δ. The ω wolves follow these three wolves.

Encircling prey:
As mentioned above, grey wolves encircle prey during the hunt. In order to mathematically model encircling behavior the following equations are proposed:

V. EXPERIMENTAL RESULTS

The implementation of the portable real-time soil monitoring system, as shown in Figure 2, has been assessed for its accuracy, efficiency and effectiveness in measuring critical soil and crop parameters. The system has been tested in several agricultural environments and the results have been analysed to assess its effectiveness.

$$\vec{D} = |\vec{C}.\overrightarrow{X_p}(t) - \vec{X}(t)|$$

$$\vec{X}(t+1) = \overrightarrow{X_p}(t) - \vec{A}.\vec{D}$$

where t indicates the current iteration, A and C are coefficient vectors , ⃗Xp is the position vector of the prey, and indicates the position vector of a grey wolf.

The vectors A and C are calculated as follows

$$\vec{A} = 2\vec{a}.\overrightarrow{r_1} - \vec{a}$$

$$\vec{C} = 2.\overrightarrow{r_2}$$

To see the effects of equations, a two-dimensional position vector and some of the possible neighbors are illustrated in Fig.. As can be seen in this figure, a grey wolf in the position of (X, Y) can update its position according to the position of the prey (X*, Y*). Different places around the best agent can be reached with respect to the current position by

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305024

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

adjusting the value of A and C vectors. For instance, (X*-X,Y*) can be reached by setting A=(1,0) and C=(1,1) . The possible updated positions of a grey wolf in 3D space are depicted in Fig. 3. Note that the random vectors R1 and R2 allow wolves to reach any position between the points illustrated in Fig. So a grey wolf can update its position inside the space around the prey in any random location by using equations of vector A and C.

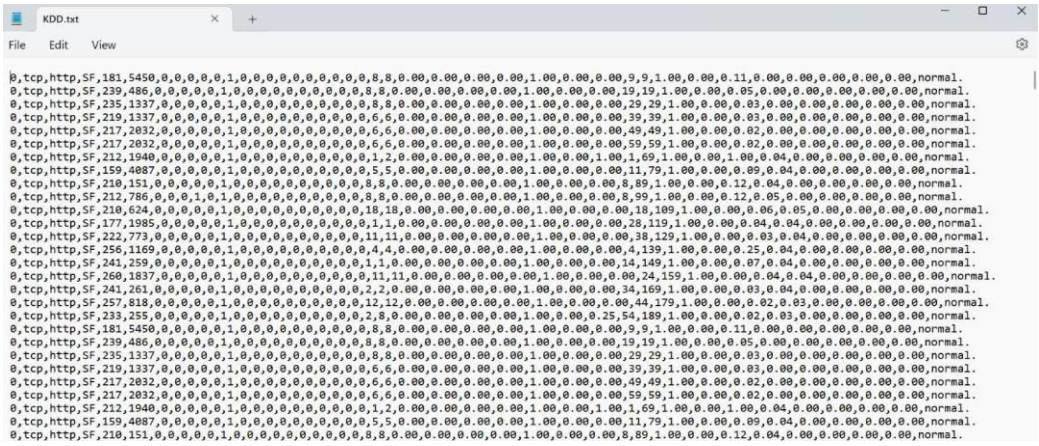


Fig 2. Dataset Description

```
999:    learn: 0.0025399        total: 12.1s    remaining: 0us
Confusion Matrix:
[[57224    36]
 [    0 36651]]

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     57260
           1       1.00      1.00      1.00     36651

    accuracy                           1.00     93911
   macro avg       1.00      1.00      1.00     93911
weighted avg       1.00      1.00      1.00     93911


Accuracy: 99.96%
>>>
```

Fig 3. Confusion Matrix

This matrix summarizes the model's predictions against the actual values.

- 57224: True Positives (TP) - The model correctly predicted 57224 instances of class 0.
- 36: False Positives (FP) - The model incorrectly predicted 36 instances as class 0 when they were actually class 1.
- 0: False Negatives (FN) - The model incorrectly predicted 0 instances as class 1 when they were actually class 0.
- 36651: True Negatives (TN) - The model correctly predicted 36651 instances of class 1management of soil health.

In summary, the Bi-GRU with GWO model appears to be the most effective among those tested, offering a significant improvement in performance compared to the other models, particularly the traditional machine learning models like NN and SVM. The Bi-GRU with GWO model demonstrates the strongest performance across all metrics, achieving an F1-Score of 98.5, Accuracy of 99.5, Precision of 98.9, and Specificity of 98.5. This suggests that Bi-GRU with GWO excels at correctly identifying both positive and negative cases, with minimal false positives and false negatives.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305024

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

CatBoost also performs exceptionally well, with high scores in all metrics, closely followed by AdaBoost. The SVM model shows moderate performance, while the NN model exhibits the lowest scores among the evaluated models.

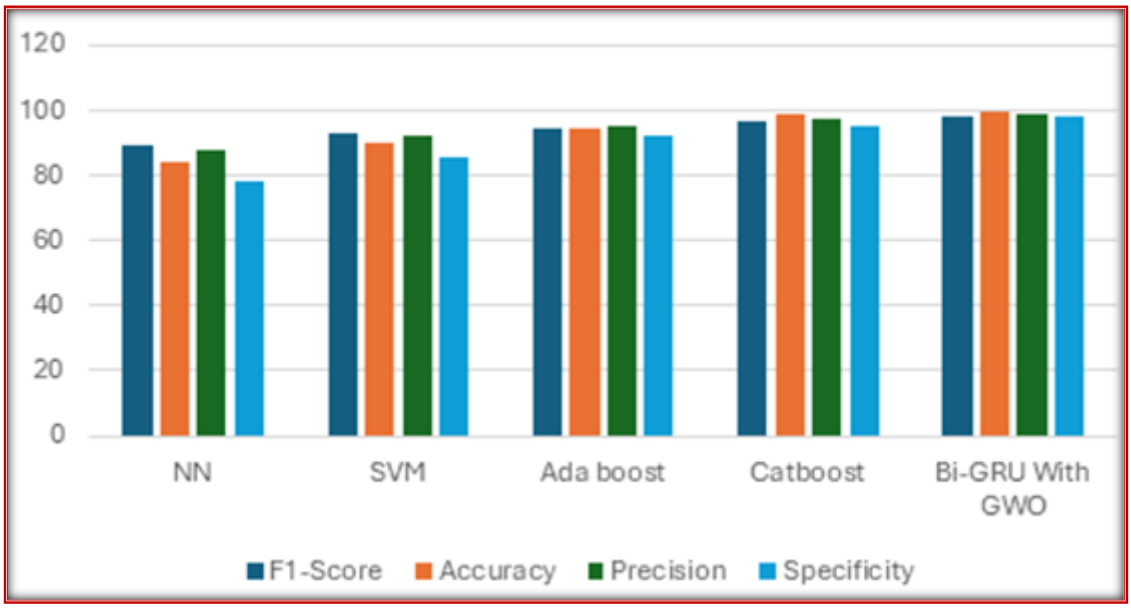


Fig 4. Performance Comparison

Figure 4 shows the comparative analysis of various machine learning models, evaluating their performance across four key metrics: F1-Score, Accuracy, Precision, and Specificity. The models under consideration include NN (Neural Network), SVM (Support Vector Machine), AdaBoost, CatBoost, and Bi-GRU with GWO (Grey Wolf Optimization).

VI. CONCLUSION

In conclusion, the proposed Secure Optimized Bidirectional Gated Recurrent Unit (Bi- GRU) Based Flow-Based Attacker Detection Model represents a significant advancement in the field of network security. By leveraging the power of deep learning, specifically the Bi-GRU architecture, and optimizing it through the Grey Wolf Optimizer (GWO), the system can efficiently capture both forward and backward dependencies in network traffic data, providing an in-depth understanding of attack patterns. This enables the detection of sophisticated cyber- attacks such as Distributed Denial of Service (DDoS), phishing, and Advanced Persistent Threats (APTs).The model's integration of secure data preprocessing and feature extraction techniques ensures it can handle high- dimensional and encrypted network traffic, making it adaptable across various network environments. The use of GWO for hyperparameter optimization results in a highly accurate and computationally efficient system, capable of providing real-time attack detection with minimized false positives.Furthermore, the scalability of the system allows it to be deployed in diverse network settings, from enterprise environments to IoT networks, ensuring robust protection of critical digital infrastructures. Overall, this system offers a reliable, scalable, and efficient solution for safeguarding against the growing threats in the digital landscape, making it a valuable tool for enhancing cybersecurity measures across various industries.

REFERENCES

[1] V. Sujatha, K. L. Prasanna, K. Niharika, V. Charishma and K. B. Sai, "Network Intrusion Detection using Deep Reinforcement Learning," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 1146- 1150, doi: 10.1109/ICCMC56507.2023.10083673..

[2] R. Padmaja and P. R. Challagundla, "Exploring A Two-Phase Deep Learning Framework For Network Intrusion Detection," 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2024, pp. 1-5, doi: 10.1109/SCEECS61402.2024.10482198.M. Kuriakose and T.

Singh, "Indian Crop Yield Prediction using LSTM Deep Learning Networks," 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2022, pp. 1-5

[3] S. K. Kodali and C. H. Muntean, "An Investigation into Deep Learning Based Network Intrusion Detection System for IoT Systems," 2021 IEEE International Conference on Data Science and Computer Application (ICDSCA), Dalian, China, 2021, pp. 374-377, doi: 10.1109/ICDSCA53499.2021.9650111.

[4] V. Kurnala, S. A. Naik, D. C. Surapaneni and C. B. Reddy, "Hybrid Detection: Enhancing Network & Server Intrusion Detection Using Deep Learning," 2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), Hamburg, Germany, 2023, pp. 248-251, doi: 10.1109/ICCCMLA58983.2023.10346699.

[5] X. Song, M. Song and X. Li, "A Computer Network Security Intrusion Detection Algorithm Based on Deep Learning," 2024 3rd International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS), Bristol, United Kingdom, 2024, pp. 472-476, doi: 10.1109/AIARS63200.2024.00093.

[6] C. -F. Hsieh and C. -M. Su, "DNNIDS: A Novel Network Intrusion Detection Based on Deep Neural Network," 2021 7th International Conference on Applied System Innovation (ICASI), Chiayi, Taiwan, 2021, pp. 22-25, doi: 10.1109/ICASI52993.2021.9568439.

[7] R. B. Said and I. Askerzade, "Attention-Based CNN-BiLSTM Deep Learning Approach for Network Intrusion Detection System in Software Defined Networks," 2023 5th International Conference on Problems of Cybernetics and Informatics (PCI), Baku, Azerbaijan, 2023, pp. 1- 5, doi: 10.1109/PCI60110.2023.10325985.

[8] S. Amutha, K. R, S. R and K. M, "Secure network intrusion detection system using NID- RNN based Deep Learning," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-5, doi: 10.1109/ACCAI53970.2022.9752526.

[9] K. Roshan, A. Zafar and S. B. Ul Haque, "A Novel Deep Learning based Model to Defend Network Intrusion Detection System against Adversarial Attacks," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 386-391

[10] D. S. P. Puvvala, G. Madala, M. Kada and U. Hariharan, "Improved Network Intrusion Detection System Using Deep Learning," 2023 7th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), Kolkata, India, 2023, pp. 1-6, doi: 10.1109/IEMENTech60402.2023.10423459.

[11] M. Masum and H. Shahriar, "TL-NID: Deep Neural Network with Transfer Learning for Network Intrusion Detection," 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST), London, United Kingdom, 2020, pp. 1- 7, doi: 10.23919/ICITST51030.2020.9351317.

[12] S. Hemalatha, M. Mahalakshmi, V. Vignesh, M. Geethalakshmi, D. Balasubramanian and J. Anand A., "Deep Learning Approaches for Intrusion Detection with Emerging Cybersecurity Challenges," 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India, 2023, pp. 1522-1529, doi: 10.1109/ICSCNA58489.2023.10370556.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details