International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Next-Generation Cyber Threat Detection: Leveraging CNN-GRU Architecture and Honey Badger Algorithm Optimization for Network Security

Katikam Mahesh*, Dr. Kunjam Nageswara Rao

Submitted:11/03/2024 **Revised**: 26/04/2024 **Accepted**: 03/05/2024

Abstract: The rising significance of Internet and Communication Technology (ICT) has resulted in the increased volume of transmitted data. The attackers gain unauthorized access to the network data and inject potential threats into the system for stealing or manipulating the data hence it is considered as a major obstacle for attack detection. This study offers an effective framework that combines the Gated Recurrent Unit (GRU) technique with a hybrid Convolutional Neural Network (CNN). This work's primary goal is to identify cyberthreats and categorize various attacks on security. The future hybrid CNN-GRU approach leverages the strengths of both CNN and GRU algorithms for attack detection. The hybrid model is optimized using a Honey Badger Optimization Algorithm (HBOA). The HBOA is used to adjust the model parameters in order to improve the performance metrics for different sorts of cyberattacks, such as Precision, Recall, f1-score, and others. The hybrid model is intended to extract high-level features from the network data. Simulation analysis is used to assess and validate the hybrid CNN-GRU model's effectiveness and support. The CNN-GRU model produces the classification output with an accuracy of 94.22% in terms of identifying various security attacks. The model is trained using input data taken from the CICIDS-2017 dataset.

Keywords*: Classification Accuracy, Cyber Threat Detection, Convolutional Neural Network, Feature Extraction, Gated Recurrent Unit, Honey Badger Optimization Algorithm, Network Security, Optimization*

1. Introduction

Threat detection and response solutions are essential for identifying and mitigating security threats in real-time. These solutions utilize advanced technologies like machine learning, artificial intelligence, and behavioural analysis to predict and prevent threats across various sectors, including networks, cloud, endpoints, email, and applications. Next-generation endpoint protection is crucial for thwarting sophisticated attacks targeting endpoint devices and data, leveraging cloud-enabled real-time detection methods like AI and ML to stay ahead of threats. The Traditional Deep Learning and Machine learning techniques such as K-Nearest Neighbour (KNN) Algorithm, A decision tree (DT), Artificial Neural Networks (ANN) are used with old Dataset (KDD-CUP 99) Knowledge Discovery in Databases. But These Techniques with this dataset not able to classify and detection Different types of class attacks with Additional dangers [1].The Traditional Deep Learning and Machine learning techniques such as K-Nearest Neighbour (KNN) Algorithm, A decision tree (DT), Artificial Neural Networks (ANN) but these ML and DL Approaches still confront hurdles in increasing detection rate, fails to identifying novel attacks like Malwares Attacks, Web attacks, No Detailed accuracy for different classes of attacks Dataset imbalance also one of the major concerns. And finally existing machine learning approaches only deal with small

quantity datasets. To Achieve all these with our proposed method, the hybrid model is optimized using a Honey Badger Optimization Algorithm (HBOA). The hybrid model is designed to extract high-level structures after the network data and the HBOA is active to fine-tune the model parameters to enhance the accuracy and strength of the perfect. The asset of the hybrid model is optimized using a Honey Badger Optimization Algorithm (HBOA). An effective attack detection approach which uses a hybrid CNN-GRU model for securing the network systems from different types of security attacks. A Honey Badger Optimization Algorithm (HBOA) is employed in this research for optimizing the presentation of the CNN-GRU model to enhance the efficacy of the model for attack detection. With 94.22% Accuracy The proposed hybrid model employs a feature extraction and selection mechanism which selects the relevant features using a Recursive Feature Elimination (RFE) technique with Decision Tree classifier

2. Related Works

The utilization of deep learning and machine learning techniques to increase the safety of systems for cyber security has been highlighted in a number of previous

[1]*Andhra University College of Engineering Visakhapatnam, INDIA*
ORCID ID: 0009-0000-0707-1117
[2] *Andhra University College of Engineering Visakhapatnam, INDIA*
ORCID ID: 0009-0005-2779-0238

studies. To create a network intrusion detection system (NIDS), the hybrid CNN-GRU model is provided in [2]. In place of the traditional entropy cross, a changed focus loss function is used in the CNN-GRU-FF dual-layer extracted features and fusion method used in the creation of the NIDS to solve the imbalances in classes in IDS datasets. We evaluate our model's effectiveness using the NSL-KDD and UNSW-NB15 datasets. Based on results from experiments, the CNN-GRU-FF technique maintains a small number of false alarms in each of the datasets (UNSW-NB15 and NSL-KDD), achieving an accuracy rate of 98.22% and 99.68%, respectively. A DL-based technique was used in the work reported in [3] to distinguish between various security risks in ad hoc networks that are wireless. In this study, a trust-based safe routing method is devised to mitigate black hole component assaults while routing in mobile ad hoc networks. Utilizing computational models, the authors in [4] created and put into practice a malware detection system. In order to differentiate amongst phishing and anti-phishing correspondence, the DL model is intended to capture both the inherent characteristics of email content and extra features. Three different datasets are used in the model's training. In particular, the enhanced tree decision-making approach demonstrated its superior reliability by yielding accuracy ratings of 88%, 100%, and 97% consecutively throughout the datasets used. However, it was unable to handle cyberattacks involving various categories. The contributors of [5] provided a thorough examination of the use of ML algorithms to improve network infrastructure security. The three primary techniques that were the subject of the study were support vector machines (SVM), decision trees (DT), and deep belief networks (DBN). The research indicates that there is a significant need for an additional benchmark dataset to assess the most recent developments in machine learning for online threat detection. The review also makes the case that more research on learning strategies is necessary in order to identify security risks.

3. Proposed Methodology

The design of the attack detection method is constructed on the principle of the security system which continuously monitors the data traffic in the network systems to identify and classify different types of security attacks. The attack detection approach is designed using a hybrid Gated Recurrent Unit (GRU) and Convolutional Neural Network (CNN) system for detecting the cyber-attacks in the system organizations that are injected into the system by the attackers. The malicious attacks in the network allows the attackers to exploit the system data and obtain unauthorized access to the confidential network information The preliminary aim of the proposed attack detection framework is to develop an efficient model based on feature selection and optimization using a metaheuristic HBOA algorithm. In this study, the CNN-GRU network is trained to identify and categorize assaults using characteristics that have been determined for each distinct type of attack using the RFE and Decision Tree Learner. The parts that follow provide a description of each step in putting the proposed CNN-GRU model for attack detection into practice.

3.1 Data Collection

The CICIDS-2017 dataset (Canadian Institute for Cybersecurity Intrusion Detection Systems Evaluation Dataset 2017) is the source of data used in this study's experimental analysis. The collection includes data about network traffic as well as information about attacks. The information is arranged into distinct CSV files, one for each day of the week or category of network activity. A total of 154290 samples were taken into consideration for the analysis; 123432 of these samples were utilized as training data, while 30858 of them were used as validation data, with an 80:20 split ratio.

3.2 Data Preprocessing

After creating a unified dataset, the data is preprocessed to eliminate uncertainties and redundancies from the dataset. Different uncertainties such as handling missing values, removing duplicates are filtered out to ensure data consistency. It is crucial to preprocess the data in order to safeguard the superiority and integrity of the dataset before further analysis or modeling. In this stage, an Exploratory data analysis (EDA) is performed to analyze and visualize the data along with basic exploration tasks such as displaying the first and last rows to understand data structure, checking shape (number of rows and columns, examining column names to identify features, checking for null values to ensure data integrity and analyzing the distribution of the target column ('Label') to understand class distribution. Furthermore, to address the problem of class inequalities, a Synthetic Minority Over-sampling Technique (SMOTE) approach is used.

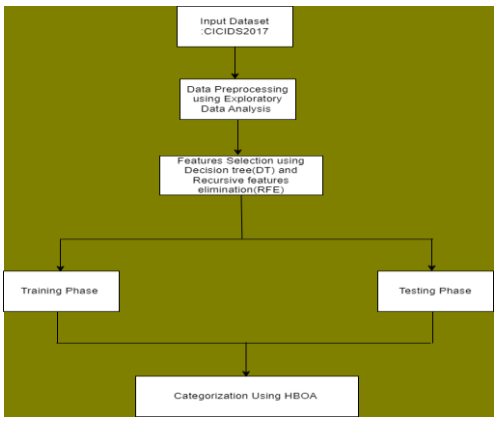

Fig. 1 Framework of the proposed hybrid HBOA Model

3.3 Feature Selection

The essential and relevant features are selected using a Recursive Feature Elimination technique with a decision tree classifier (DTC). The RFE is a feature selection method used for identifying the key features from the dataset. Once the most insignificant components are consistently eliminated until the required number of qualities is reached, the method

entails creating representation with the residual characteristics. Initially, the DTC is created and is used as an estimator. The RFE is initialized with the estimator and the number of features to be selected are defined with a step size. In this research, 30 features are selected for the analysis with a step size of 1.

3.4 CNN-GRU Model for Attack Detection

The hybrid CNN-GRU model combines the network layers of both CNN and GRU model. In the hybrid architecture, the layers of the CNN are integrated with GRU model i.e., the output CNN is merged into GRU for accurate identification of the cyber-attack as shown in figure 3.1.

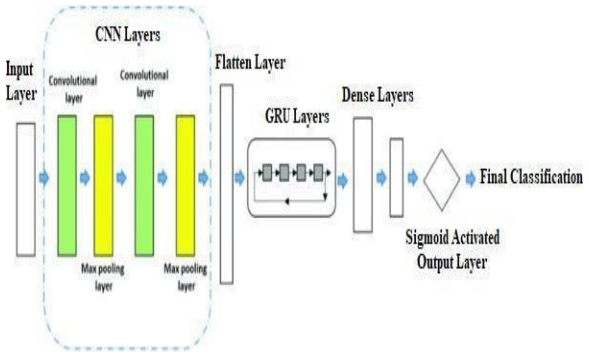

Fig 2 Architecture of the CNN-GRU model

3.5 Honey Badger optimization Algorithm

The HBOA is an algorithm that imitates Honey Badgers' ingenious foraging techniques, including how they dig and locate honey, as well as how they explore and utilize the search area. The method has two main phases: excavation and honey, which are similar to how honey badger's search. The honey badger uses its acute sense of smell to identify prey throughout the Excavation stage, and it follows the honey bird to find beehives through the Honey stage. The first stage in the HBOA process is to use this formula to set the starting agent significance:

$$Z_i = LB_i + r_1 * (UB_i - LB_i), \quad i = 1, 2, \ldots, N, \tag{1}$$

where r1 is the smallest possible number and LB and UB are the searching space's bottom and higher boundaries, respectively.

Equation 6 shows how the density factor (α) is used to balance both extraction (honey) and investigation (digging).

$$\alpha = C * exp^{(-t/T)} \tag{2}$$

where T is the entire number of repetitions, C is an integer, and t is the current stage of iteration. C is a constant with a value larger than 1. Additionally, as indicated by equation 8, the responses are modified using the Digging operations.

$$Z^{new} = Z_b + F * \beta * I * Z_b + F * \alpha * d^i * r_3 * \left|\cos(2\pi r_4) * [1 - \cos(2\pi r_5)]\right|. \tag{3}$$

where r3, r4, r5, and r6 are random values, B is a constant, F is a parameter that controls the search direction, and Znew denotes the new value of Zb and Zi indicates the best solution discovered thus far. The value of F is obtained using the subsequent equation:

$$F = \begin{cases} 1, & \text{If } (r_6 \le 0.5), \\ -1, & \text{Else.} \end{cases} \tag{4}$$

As seen in equations 10 and 11, where I is the prey's smell intensity (xb) and is utilized to describe the distance among xb and xi:

$$Ii = r2 * (S / 4\pi d^2 i) \tag{5}$$

$$S = (Z^i - Z^{i+1})^2 \tag{6}$$

The Honey stage operators are used to update the solutions, and the following formula is used to accomplish this process:

$$Z^{new} = Zb + F * r1 * \alpha * di \tag{7}$$

where r1 is a random number.

The pseudocode of the HBOA algorithm

Input: Dataset CICIDS2017

Step-1 Initially seed the search space with an estimated number of honey badgers at random sites.

Step-2 Evaluate the fitness of each honey badger in the population.

Step-3 Set the best honey badger as the one with the highest fitness.

Step-4 Repeat until a termination condition is met (e.g., maximum number of iterations reached) For each honey badger in the population:

Determine the exploration probability (pr) for this honey badger with probability pr, perform exploration: Generate a random direction vector the honey badger should be moved in this way to update its position. If the new position is within the search space, accept it, else reject it

with probability (1 - pr), perform exploitation: Select a random honey badger from the population (different from itself) Update the position of the honey badger towards the selected honey badger If the new position is within the search space, accept it, else reject it Evaluate the fitness of the honey badger's new position If the new fitness is better than the previous fitness, update the best honey badger Return the best value

Output: To detect cyber threats and classify different security attacks of improved Accuracy

Stop:

4. Experiment Results

The evaluation of the proposed CNN-GRU model is covered in this part utilizing various evaluation criteria, which are expressed mathematically in the following equations:

Accuracy is the proportion of successfully detected online assaults, as expressed in the calculation below:

TP+TN/TP+TN+FP+FN

Recall The ratio of attacks that are correctly identified determines a function's recall, which is expressed as follows:

TP/TP+FN

F**1 score** the CNN-GRU model's accuracy is measured by F1, which displays values between 1 and 0. where the best value is denoted by 1 and the poorest value by 0. Likewise, an F1 score is described as follows:

F**1 score** = $2 * Precision*Recall/Precision+Recall$

Precision The number of accurate positive classifications is the definition of precision. It is determined by dividing correctly classified network attacks by the total number of attacks. It has the following definition:

Precision=TP+FP

TP stands for true positive, which indicates the quantity of correctly classified cyberattacks; TN for true negative, which indicates the quantity of correctly detected normal attacks; FP for false positive score, which indicates the quantity of incorrectly detected cyberattacks; and FN for false negative, which indicates the quantity of incorrectly identified cyberattacks.

```
# Target column distribution
df[' Label'].value_counts()
BENIGN                      2096134
DoS Hulk                    172846
DDoS                        128016
PortScan                    90819
DoS GoldenEye               10286
FTP-Patator                 5933
DoS slowloris               5385
DoS Slowhttptest            5228
SSH-Patator                 3219
Bot                         1953
Web Attack  Brute Force     1470
Web Attack  XSS             652
Infiltration                36
Web Attack Sql Injection    21
Heartbleed                  11
Name:  Label, dtype: int64
```

Table 1. Comparative Analysis

Metric / Model	**Accuracy**	**Precision**	**Recall**	**F1-score**
KNN	92 %	92 %	92 %	92 %
DT	91 %	91 %	91 %	91 %
ANN	91 %	93 %	91 %	89 %
The proposed CNN-GRU With HBOA	94.22 %	94 %	94 %	94 %

As inferred from the experimental results, The CNN-GRU that recommended The HBOA Model achieves extraordinary accuracy, outperforming other models. Results validate the effectiveness of the optimized CNN-GRU model.

5. Conclusion

This research work discusses the implementation of a hybrid classifier combining CNN-GRU for identifying the cyber threats in the network system. The CNN-GRU model was designed and simulated for monitoring the network continuously in order to identify and detect cyber-attacks such as SQL injection attacks, Web attacks, DoS attacks, DDoS attacks, and infiltration attacks. This paper presents a hybrid CNN-GRU framework which is optimized using a HBOA algorithm. The proposed approach was evaluated using the CICIDS-2017 dataset with a split training and testing ratio of 80% and 20%. The data was pre-processed to ensure the consistency and the problem of data imbalance was addressed using the SMOTE technique.

The essential and relevant features are extracted and selected from the dataset using a RFE with Decision Tree classifier in order to simplify the classification process. The CNN-GRU model is trained to distinguish between normal and attack data instances in order to detect attacks on security. Several metrics are used to assess the hybrid model's performance, and the findings indicate that the CNN-GRU model with HBOA algorithm performs better than other ML models in terms of reaching an accuracy level of 94.22%. For future work, the study intends to investigate the application of Generative AI models with Explainable AI models for achieving explainability and interpretability. Hence, in future we can use them for extending the study to Enhance the accuracy with less computation time.

Acknowledgement:

I would like to express my profound gratitude to Dr. Kunjam Nageswara Rao Professor Department of Computer Science and System Engineering in Andhra University Andhra Pradesh, Visakhapatnam India, for giving Guidance and Support to Review and Given suggestion.

Author Contribution:

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Katikam Mahesh, Dr Kunjam Nageswara Rao, and all authors commented on previous versions of the manuscript.

Conflicts of interest

The authors declare no conflicts of interest

References

[1] Nadir Omer a, *Ahmed H. Samak b, Ahmed I. Taloba c,d , Rasha M. Abd El-Aziz c A novel optimized probabilistic neural network approach for intrusion detection and categorization. Alexandria Engineering Journal (2023) 72, 351–361

[2] Imrana, Y., Xiang, Y., Ali, L., Noor, A., Sarpong, K., & Abdullah, M. A. (2024). CNN-GRU- FF: a double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units. *Complex & Intelligent Systems*, 1-18.

[3] Chethana, C., Pareek, P. K., de Albuquerque, V. H. C., Khanna, A., & Gupta, D. (2022, October). Deep learning technique-based intrusion detection in cyber-security networks. In *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)* (pp. 1-7). IEEE.

[4] Mughaid, A., AlZu'bi, S., Hnaif, A., Taamneh, S., Alnajjar, A., & Elsoud, E. A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, *25*(6), 3819-3828.

[5] Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020, October). Cyber threat detection using machine learning techniques: A performance evaluation perspective. In *2020 international conference on cyber warfare and security (ICCWS)* (pp. 1-6). IEEE.

[6] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in the internet of things using a deep learning approach. *IEEE access*, *7*, 124379-124389.

[7] Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. *Ieee Access*, *7*, 165607-165626.

[8] Sagduyu, Y. E., Shi, Y., & Erpek, T. (2019, June). IoT network security from the perspective of adversarial deep learning. In *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)* (pp. 1-9). IEEE.

[9] Kumar, C., Bharati, T. S., & Prakash, S. (2021). Online social network security: a comparative review using machine learning and deep learning. *Neural Processing Letters*, *53*(1), 843-861.

[10] Dixit, P., & Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer Science Review*, *39*, 100317.

[11] Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science*, *2*(3), 154.

[12] Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber-attacks and its different types.

[13] *International Research Journal of Engineering and Technology*, *6*(3), 4849-4852.

[14] Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence-based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, *9*, 94668-94690.

[15] Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review.

IEEE Access, *9*, 59353-59377.

[16] Malek, Z. S., Trivedi, B., & Shah, A. (2020, July). User behavior pattern-signature based intrusion detection. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)* (pp. 549-552). IEEE.

[17] Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2019). Rule generation for signature-based detection systems of cyber-attacks in iot environments. *Bulletin of Networking, Computing, Systems, and Software*, *8*(2), 93-97.

[18] Gupta, C., Johri, I., Srinivasan, K., Hu, Y. C., Qaisar, S. M., & Huang, K. Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. *Sensors*, *22*(5), 2017.

[19] Halbouni, A., Gunawan, T. S., Habeebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine learning and deep learning approaches for cybersecurity: A review. *IEEE Access*, *10*, 19572-19585.

[20] Geetha, R., & Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering*, *28*(4), 2861-2879.

[21] Choi, Y. H., Liu, P., Shang, Z., Wang, H., Wang, Z., Zhang, L., ... & Zou, Q. (2020). Using deep learning to solve computer security challenges: a survey. *Cybersecurity*, *3*, 1-32.

[22] Thakkar, A., & Lohiya, R. (2021). A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges. *Archives of Computational Methods in Engineering*, *28*(4), 3211-3243.

[23] Chesney, S., Roy, K., & Khorsandroo, S. (2021). Machine learning algorithms for preventing IoT cybersecurity attacks. In *Intelligent Systems and Applications: Proceedings of the 2020 Intelligent Systems Conference (IntelliSys) Volume 3* (pp. 679-686). Springer International Publishing.

[24] Yang, H., Zeng, R., Xu, G., & Zhang, L. (2021). A network security situation assessment method based on adversarial deep learning. *Applied Soft Computing*, *102*, 107096.