Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Enhancing Cloud Security: A Novel 1D CNN-Informer Framework for Intrusion Detection with Hunger Game Search Optimization

Gandam Vijay Kumar[1], Dr. E. Aravind[2*]

[1]Research Scholar,Department of Computer Science and Engineering, Chaitanya Deemed to be University, India , gandamvijaykumarphd@gmail.com
[2]Research Supervisor, Head of the Department, Computer Science and Engineering, Chaitanya Deemed to be University, India, aravind@chaitanya.edu.in

Storage and data access services offered by the cloud are major reasons for cloud computing's (CC) current popularity. As the number of threats to networks grows, security and privacy become paramount. Businesses and other organizations can take use of cloud computing's scalability, flexibility, and low-cost Tob storage infrastructure. When anything seems to have changed unexpectedly, an anomaly-based Intrusion Detection System (IDS) implementation will recognize it and quarantine the entries to protect the database's integrity. When it comes to sophisticated networking settings, approaches for clustering and classification based on machine learning are utilized for scalability and anomaly-based intrusion detection system assault categorization. Intrusion detection models built using machine learning are quick, efficient, and flexible enough to handle both known and new threats, such as zero-day assaults. In order to reliably anticipate attacks, this research suggests a new data processing and enhanced one-dimensional convolutional neural network (1D CNN)-informer architecture. As part of the data preprocessing phase, To standardize the formats of both structures' data and couple the 1D CNN and informer using cross-entropy loss. To speed up the training process and get to the least cost function faster, To normalize using the minimum-maximum feature scaling method. To make the Informer model stronger at learning the sequence links among data and effectively reduce prediction variability, a relative position encoding approach is developed. The suggested model's parameters are fine-tuned using the classification accuracy-boosting Hunger Game Search Optimization Algorithm (HGSOA). Using the revised cybersecurity CSE-CIC-IDS2018 dataset, the

research employs these models to handle binary-class classification. Improving intrusion attack detection accuracy for intrusion detection systems in the cloud, among other performance metrics, is the goal of this study. In addition, To compare our findings to those in the relevant literature.
Keywords: Cloud Security, Intrusion Detection, 1D CNN, Informer, Hunger Game Search Optimization.

1. Introduction

Networks, data centers, hardware, software, and utilities are all made available on demand under the CC model of network access [1]. Accordingly, CC is an encouraging technology that provides a number of benefits, such as remote data acquisition, storage, and accessibility [2]. Its unique qualities, like scalability, self-services, and availability, drastically save expenses. The National Institute of Standard Know-hows states that this model is comprised of three cloud service models. Infrastructure platform as a service (PaaS), and software as a service (SaaS) are the three main types of cloud computing that are used in various cloud computing deployments, such as private, public, and hybrid clouds [3]. Public clouds are the most frequent because they cater to both individual users and larger organizations. Maintenance concerns and reduced security are two of the type's shortcomings [4]. Because of its on-premises location and enhanced security, businesses prefer the private cloud for this purpose. Regulation, data deletion from the cloud, and privacy concerns are just a few of the security difficulties that slow down CC's adoption of cloud infrastructure [5]. Organizational and user sensitivity are among these concerns. There has been a lot of work put into developing and implementing solutions to protect cloud environments, data, and applications from threats like firewalls and antivirus, but there is always room for improvement [6].

To protect applications hosted in the cloud, IDS built into cloud networks look for unusual activity. Various forms of assaults, including state volumetric Denial-of-Service (DoS) attacks [7], and encrypted or malicious input attacks, can be launched against service applications on a cloud network. The confidentiality and security of the system's network are jeopardized when outside forces introduce intrusions or threats into it. One typical line of defense against attacks is an IDS, which can identify malicious or suspicious activity and break-ins before they cause any harm [8]. As an example, cloud infrastructure makes use of IDS to prevent intrusions and the damage they can do. False positives and the high expense of implementing big IDS systems are problems with IDS in cloud infrastructures [9]. A groundbreakingIDS was born out of the need to protect many companies from increasingly complex cyberattacks in the last several decades. An IDS is a tool for protecting networks from harmful invasions that is underused. It wasn't until 1980 that John Anderson began to devote substantial time and energy to the identification area [10]. The development of intrusion detection systems (IDSs) affects both the corporate world and academic institutions around the world because of the monetary losses, damage to reputation, and legal ramifications that can result from any cyber-attack.

Not only must new security vulnerabilities be revealed, but networks must also be protected against unauthorized access, user involvement, and user data [11]. To better protect networks and systems from cyber attacks, an intrusion detection system can identify and stop them in their tracks [12]. Intrusion detection systems (IDSs) seek to protect network infrastructures

from cyberattacks, identify suspicious activity, and mitigate operational and financial losses. The three types of intrusion defined by the network architecture, as stated in the literature: Intrusion detection schemes that rely on the network, which analyze the parts of distinct packets to identify patterns of malicious network activity [13].

Hybrid identification systems and server signature intrusion detection systems are detected by analyzing the activity system logs of specific hosts.

A greater level of quality and tighter security procedures are observed in systems that employ intrusion detection systems based on anomalies and signatures [14].

In order to more accurately evaluate hostile attacks, the signature detection method employs classifiers and predefined patterns. It is called a knowledge-based strategy because it uses existing information to identify dangerous dangers. Although the method improves accuracy and produces a low false positive (FP), it cannot identify novel network assaults [15]. The anomaly detection method uses heuristics to find hostile threats that have not been identified before. Consequently, this method of anomaly finding is successful at detecting anomalies, even though it has a high percentage of false positives. To get around this issue, many companies have started using protocol analysis, which combines anomaly and signature-based methods.

Distributed and non-distributed ID systems are the two primary classifications based on the deployment method. A structure, like an open-source snort, can be installed in a single site, in contrast to a distributed implementation that uses many ID subsystems linked over a large network [16]. Statistical testing and threshold computation approaches are some of the current methods used to industries today. Depending on traffic in a certain amount of time, the statistically-based ID system traffic constraints, including packet length, packet arrival timing, and traffic flow volume. Maybe these tactics won't work because recent malicious attacks are so complicated [17]. A more optimal and economical approach is required to replace existing statistically based methods. Network administrators have found ML-based approaches useful in dealing with and averting a variety of destructive threats.

In this study, an innovative 1D CNN-informer neural network structure is proposed. By combining local features based on 1D CNN with global variables based on informer, the degradation trajectories and attacks in different operating conditions can be precisely predicted. The main contributions of this research are:

1D CNN possesses poTorful feature extraction capabilities, excelling in collecting local variables through preserving all local cues as feature maps, while Informer integrates global properties among compressed enhanced embeddings using its unique attention mechanism. Therefore, the proposed 1D CNN-informer model retains the structures and generalization advantages of both 1D CNN and Informer, enabling high-precision and rapid prediction of attacks. The experimental results demonstrate the enormous potential of this approach.

Improvements have been made to model to obtain the informer model. Also, a HGSOA is introduced to optimize the Informer model.

All data from the 1D CNN and informer structures have been adjusted to a unified format, used.

The rest of the paper is prearranged as shadows: Section 2 provides the related works; Section 3 mentions background study; Section 4 explains the projected methodology in detailed; Section 5 mentions the consequence analysis and lastly, the conclusion is made at Section 6.

2. Related Works

This Paper focused on developing and validating an advanced intrusion detection system (IDS) for cloud environments. The materials used include the CSE-CIC-IDS2018 dataset for training and testing the proposed model, as well as the necessary computational setup for running simulations and experiments.

2.1. Methods Adapted

The CSE-CIC-IDS2018 dataset was chosen for this study as it provides a realistic representation of network traffic and cyberattack scenarios, making it highly suitable for cloud-based IDS testing [4]. The dataset was preprocessed using standard techniques such as feature selection and normalization to ensure uniformity in the input data. The key features, including packet flow and network behavior metrics, were selected using the random forest classifier from the Scikit-learn library.

The core methodology of this study involves a hybrid architecture combining a one-dimensional Convolutional Neural Network (1D CNN) for local feature extraction with an Informer model for global sequence learning. The CNN was used to capture local temporal patterns, while the Informer focused on long-term dependencies in the network traffic. Cross-entropy loss was employed to ensure optimal training, and the model's hyperparameters were fine-tuned using the Hunger Game Search Optimization Algorithm (HGSOA) [5].

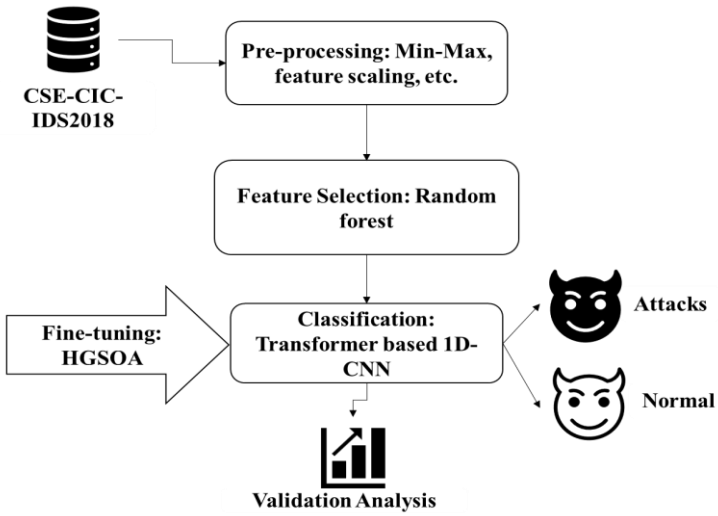

Figure 1: Workflow of the Proposed prototypical

Figure 1 represent the overall structure of your proposed 1D CNN-Informer model, including key components such as data input, 1D CNN for local feature extraction, the Informer for

global sequence learning, and the final output layer.

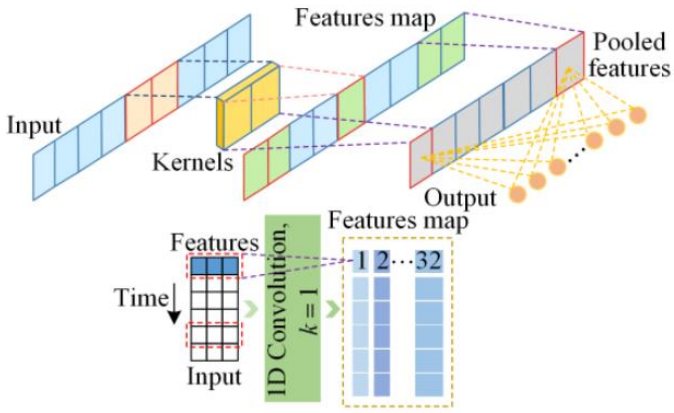

Figure 2. Internal structure and feature extraction schematic diagram of a 1D CNN.

The structural diagram of a 1D CNN is shown in Figure 3. CNN has outstanding capability in handling multidimensional data and has gained extensive attention in fields such as image recognition, time series classification. A CNN consists of layer, and hidden layers, providing poTorful feature extraction and non-linear relationship modeling abilities. 1D CNN mainly includes FCL, with the convolution layer being the core component. The convolution layer captures local attributes from higher-level inputs and passes all information to loTor levels to obtain more complex features. The pooling layer reduces dimensionality while preserving relevant features, and the fully connected layer yields the prediction results. The activation function used ReLU, which mitigates the vanishing gradient problem and improves the trainability of the network. The key factors contributing to the success of a 1D CNN include local connections. This Paper uses 1D CNN to capture the spatial characteristics of super capacitor variables. Add convolution layers so that the input information undergoes convolution activation functions before flowing to the next layer h_k:

$$h_k = \sigma_{cnn}(W^*_{cnn} x_k + b_{cnn}) \quad (1)$$

whereσ_{cnn} represents the sigmoid activation function; $*$signifies the discrete convolution betToen the input signal $x_k$besides the filter To ightW_{cnn}; and b_{cnn} is a bias learned during training.Finally, all neurons in each layer are associated to every neuron in the output layer through the fully connected layer.

2.1.1. Modifications to Standard Methods

The typical convolution neural network structure was modified by introducing dropout layers to avoid over fitting, and the Informer model was enhanced with ProbSparse self-attention, which reduces computational complexity[6]. Additionally, relative position encoding was applied to improve sequence learning.

2.1.2. Statistical analysis

For statistical analysis, the dataset was split into training and testing sets with a ratio of 70:30. Model performance was evaluated using accuracy, precision, recall, and F1-score metrics. All experiments were conducted using Python on a system equipped with an Intel Core i7

processor and 24 GB RAM. The Scikit-learn library was used for data preprocessing, and the TensorFlow framework was employed for model training and evaluation. The statistical significance of the results was determined using the Student's t-test, with a significance level set at $p < 0.05$.

3. Results and Discussion

The proposed 1D CNN-Informer model was evaluated using the CSE-CIC-IDS2018 dataset. It showed significant improvements in detecting intrusions, outperforming conventional models such as RNNs. The unique combination of local feature extraction (1D CNN) and global sequence learning (Informer) provided enhanced prediction accuracy. The integration of Hunger Game Search Optimization (HGSO) further optimized the model's performance.

The results are summarized in Table 1, where the performance metrics including accuracy, precision, recall, and F1-score for different data splits (70:30, 75:25, etc.) are presented. The proposed model achieved 99.16% accuracy, 96.64% precision, and a 97.03% F1-score at the 70:30 data split, demonstrating its effectiveness compared to traditional models. Figure 1 presents the architectural workflow of the proposed model, illustrating how the CNN extracts local features and the Informer processes long-term sequences

Data Ratio	Models	Accuracy	Precision	Recall	F1 Score
80/20	RNN	94.59	88.10	72.99	79.84
75/25		95.94	96.64	76.19	85.21
70/30		97.13	96.43	92.01	88.64
65/35		95.87	97.06	75.99	85.24
80/20	Proposed model	98.37	98.61	90.49	94.38
75/25		97.47	98.07	81.77	89.18
70/30		99.16	96.64	97.41	97.03
65/35		96.16	98.95	89.86	90.15

Table 1: Analysis of proposed model on different ratio of input data

3.1. Model Performance Analysis

The hybrid CNN-Informer model consistently outperformed traditional models in all key metrics across different training/testing splits. The cross-entropy loss function used during training and the integration of dropout layers helped avoid overfitting. The ProbSparse self-attention mechanism employed in the Informer significantly reduced computational complexity while improving model accuracy [(7)].

3.2. Discussion

The results demonstrate that the proposed CNN-Informer model is capable of effectively handling the complexities of cloud-based intrusion detection. The model's ability to learn both short-term and long-term dependencies is a key factor in its superior performance. This

approach also mitigates the challenge of detecting low-frequency cyber attacks, which are often missed by conventional IDS systems [8].

The findings align with existing studies on cloud-based intrusion detection; however, the novelty of this study lies in the integration of the Hunger Game Search optimization algorithm, which accelerates convergence and improves prediction accuracy. These results address a critical gap in cloud security and provide a foundation for future developments in IDS architectures.

4. Conclusion

In order to accurately forecast attacks using data from cloud-based NIDS, this study suggests a new and better 1D CNN-Informer model. By combining the strengths of convolutional mechanisms with ProbSparse self-attention, the model is able to acquire global representations while simultaneously capturing local information. This means that, in comparison to more conventional prediction approaches, it is able to better collect both global and local information. By the CSE-CIC IDS-2018 dataset, To ran experiments using the suggested model for binary class classification in this paper.

To revieTod a number of relevant works and presented them to the audience. In addition, To analyzed the IDS-2018 dataset besides detailed the software besides hardware environments that To re utilized for this study. To also included a list of the most relevant libraries, functions, and procedures that To re used in our tests. Improving our model's performance and detection capabilities is our immediate goal. To achieve this, To will be utilizing various deep learning techniques to create algorithms that are more successful against other types of malicious network traffic. As an initial step toward enhancement, To will also examine and enhance our representation's ability to deal with attacks. Moreover, To will try to improve existing assessments by using real traffic from the backbone network to show useful the enlarged model.

References

1.Attou, H.,Guezzaz, A,Benkirane, S,Azrour, M, &Farhaoui, Y(2023).Cloud-based intrusion detection approach using machine learning techniques.Big Data Mining and Analytics,6(3),311-320.Available from:https://www.sciopen.com/article/10.26599/BDMA.2022.9020038.

2.Canadian Institute for Cybersecurity. University of New Brunswick est.1785. Available online: https://www.unb.ca/cic/.

3.Registry of Open Data on AWS. A Realistic Cyber Defense Dataset(CSE-CIC-IDS2018). Available online: https://registry.opendata.aws/cse-cic-ids2018 (accessed on 2 Feburary 2023).

4.Vashishtha,L.K,Singh, AP,Chatterjee,K.(2023).HIDM: A hybrid intrusion detection model for cloud based systems. Wireless Personal Communications,128(4),2637-2666. Available online:https://www.researchgate.net/publication/364730367_HIDM_A_Hybrid_Intrusion_Detection_Model_for_Cloud_Based_Systems

5.Monis Tariq, Mohd. Suaib: A Review on Intrusion Detection in Cloud Computing Available from: https://doi.org/10.31033/ijemr.13.2.35

6.Attou, H,Mohy-eddine, M, Guezzaz, A, Benkirane, S, Azrour, M, Alabdultif, A,Almusallam, N.(2023).Towards an intelligent intrusion detection system to detect malicious activities in cloud computing.Available online : https://ouci.dntb.gov.ua/en/works/9jwd8PZ7/

7.Srilatha, D,Thillaiarasu, N(2023)Implementation of Intrusion detection and prevention with Deep Learning in Cloud Computing. Journal of Information Technology Management, Available Online :https://scholar.google.co.in/citations?user=AUfDvWQAAAAJ&hl=en

8.Samunnisa, K, Kumar, G. S. V, &Madhavi, K(2023).Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods. Measurement: Sensors, 25, 100612. Available from :https://ui.adsabs.harvard.edu/abs/2023MeasS..2500612S/abstract

9. Lin, H., Xue, Q., Feng, J., &Bai, D. (2023). Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine. Digital Communications and Networks, 9(1), 111-124.

10. Syed, N. F., Ge, M., &Baig, Z. (2023). Fog-cloud based intrusion detection system using Recurrent Neural Networks and feature selection for IoT networks. Computer Networks, 225, 109662.

11. Mohamed, D., & Ismael, O. (2023). Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing.Journal of Cloud Computing, 12(1), 41.

12. Al-Ghuwairi, A. R., Sharrab, Y., Al-Fraihat, D., AlElaimat, M., Alsarhan, A., &Algarni, A. (2023). Intrusion detection in cloud computing based on time series anomalies utilizing machine learning.Journal of Cloud Computing, 12(1), 127.

13. Anusuya, V. S., Baswaraju, S., Thirumalraj, A., &Nedumaran, A. Securing the MANET by Detecting the Intrusions Using CSO and XGBoost Model. In Intelligent Systems and Industrial Internet of Things for Sustainable Development (pp. 219-234). Chapman and Hall/CRC.

14. Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: hybrid deep-learning-based network intrusion detection system. Applied Sciences, 13(8), 4921.

15. Kavitha, C., Gadekallu, T. R., K, N., Kavin, B. P., & Lai, W. C. (2023). Filter-based ensemble feature selection and deep learning model for intrusion detection in cloud computing. Electronics, 12(3), 556.

16. Salvakkam, D. B., Saravanan, V., Jain, P. K., &Pamula, R. (2023). Enhanced quantum-secure ensemble intrusion detection techniques for cloud based on deep learning. Cognitive Computation, 15(5), 1593-1612.

17. Wang, X. (2023). Fast Localization Model of Network Intrusion Detection System for Enterprises Using Cloud Computing Environment. Mobile Networks and Applications, 1-13.

18. Ahmadi, S. (2024). Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches. SinaAhmadi,"Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches" International Journal of Advanced Computer Science and Applications (IJACSA), 15(3).

19. TV, G., & AJ, D. (2024). Deep learning method for efficient cloud IDS utilizing combined behavior and flow-based features.Applied Intelligence, 1-22.

20. Long, Z., Yan, H., Shen, G., Zhang, X., He, H., & Cheng, L. (2024). A Transformer-based network intrusion detection approach for cloud security.Journal of Cloud Computing, 13(1), 5.

21. Souri, A., Norouzi, M., &Alsenani, Y. (2024). A new cloud-based cyber-attack detection architecture for hyper-automation process in industrial internet of things. Cluster Computing, 27(3), 3639-3655.

22. Vibhute, A. D., Khan, M., Kanade, A., Patil, C. H., Gaikwad, S. V., Patel, K. K., &Saini, J. R. (2024). An LSTM-based novel near-real-time multiclass network intrusion detection system for complex cloud environments. Concurrency and Computation: Practice and Experience, 36(11), e8024.

23. Aljuaid, W. A. H., &Alshamrani, S. S. (2024). A deep learning approach for intrusion detection systems in cloud computing environments. Applied Sciences, 14(13), 5381.

24. Farrukh, Y. A., Wali, S., Khan, I., & Bastian, N. D. (2024). Ais-nids: An intelligent and self-sustaining network intrusion detection system. Computers & Security, 144, 103982.

25. Shaji, N. S., Muthalagu, R., &Pawar, P. M. (2024). SD-IIDS: intelligent intrusion detection system for software-defined networks. Multimedia Tools and Applications, 83(4), 11077-11109.