WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Threat Detection Utilizing CNN-GRU Architecture Network Security

Katikam Mahesh

Assistant Professor in Tirumula Engineering College Jonnalagadda Narasaraopet India
katikammahesh@gmail.com

ABSTRACT:

The volume of data that is conveyed has grown as a result of the increasing importance of Internet and communication technology-related developments. Large-scale exchange of information across several networks is made feasible by the growth of wireless networks. Network attacks are able to target data that is transferred across wireless networks. Unauthorized access to network data is gained by the attackers, who may then introduce threats into the system to possibly take or modify data. The increase in these cyberthreats is regarded as a significant barrier to attack detection since it raises major questions about the security of network the system. The present study offers an effective framework that utilizes the Gated Recurrent Unit (GRU) algorithm with a hybrid Convolutional Neural Network (CNN) for the recognition and classification of different online dangers. The offered hybrid CNN-GRU approach to attack detection makes use of both the benefits of the CNN and GRU algorithms. Through simulation research, the hybrid CNN-GRU model's efficiency is evaluated and verified. As can be seen from the findings, the CNN-GRU model performs better than other conventional models, classifying different security attacks with an outstanding accuracy of 90.14%.

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

1. Introduction

The term cyber system and wireless network denotes the global environment facilitating the exchange of electronic information across the globe. It serves as a universal platform for accessing information and resources without any restrictions. Currently, cyberspace dominates data transfer and information exchange, but faces significant risks and security threats (Ullah et al., 2019) [1] (Lee et al., 2019) [2]. With the surge in cyber threats, network security has undergone a significant transformation to mitigate cybercrimes. Network security involves technologies, experts, and processes aimed at safeguarding the information from being exploited by the attackers (Sagduyu et al., 2019) [3]. In general, there are two primary approaches for mitigating cyber threats i.e., traditional and automated. Traditional techniques suffer from drawbacks such as inaccurate detection, poor system configurations, and limited access to data, which dynamically change attributes of cyber-attacks (Kumar et al., 2021) [4] (Dixit & Silakari, 2021) [5] The future of cybersecurity lies in automated techniques capable of learning from experience to detect evolving cybercrimes effectively. Cyber threats incorporate various malicious acts in order to steal information, compromise integrity, or damage computing devices and networks (Sarker, 2021) [6]. Some of the potential attacks include malware, SQL injection, phishing, eavesdropping, unauthorized intrusions, Denial of Service (DoS) attacks etc (Biju et al., 2019) [7] (Zaman et al., 2021) [8] (Mishra & Pandya, 2021) [9]. These attacks are capable of disrupting the network operations completely and damage the sensitive information. The attacks and security threats in the network systems and devices can be mitigated by identifying vulnerabilities, using different signature-based and rule-based techniques (Malek et al., 2020) [10] (Soe et al., 2019) [11]. A number of researchers have suggested employing deep learning (DL) and machine learning (ML) technique. for securing network systems because of their flexibility, reliability and superior accuracy (Gupta et al., 2022) [12] (Halbouni et al., 2022) [13] (Geetha & Thilagam, 2021) [14]. Both of these models have emerged as a fundamental strategy to combat cyber threats and surpass conventional security system limitations. Despite its significance, ML techniques have constraints. These models are the subset of artificial intelligence, learned from experience without explicit programming, offering promising applications in cybersecurity and various other domains. These algorithms play a crucial role in identifying malware and malicious network activity within network systems (Choi et al., 2020) [15]. Traditional methods of detecting attacks rely on predefined strategies and features to detect and classify network attacks. However, they often struggle to recognize novel attack types and are limited to specific detection capabilities. This limitation can be addressed by employing ML and DL algorithms to analyze the entirety of network traffic rather than relying solely on predetermined rules and specifications (Thakkar & Lohiya, 2021) [16]. Such techniques, as suggested by (Chesney et al., 2021) [17] and (Yang et al., 2021) [18], demonstrate significant promise in monitoring network traffic, as well as accurately classifying and predicting network attacks. This research intends to leverage the advantage of a hybrid DL model which combines two algorithms for achieving effective results.

2. Related Works

Numerous existing surveys have emphasized the application of machine learning and deep learning approaches for improving the security of cyber security systems (Dalal & Rele, 2018) [19] (Alqahtani et al., 2020) [20] (Ferrag et al., 2020) [21]. The main aim of these review studies is to investigate the implementation of different machine learning algorithms for securing the network systems. These review analyses play a prominent role in assisting the researchers intending to carry out their analysis in this domain. However, these review articles have focused mainly on implementation of ML techniques and have not focused much on the analysis of problems related to cyber security in network systems. The authors in (Shaukat et al., 2020) [22] presented a comprehensive analysis on the application of ML algorithms for strengthening the security of network systems. The study mainly focused on three different algorithms such as deep belief network (DBN), decision tree (DT) and support vector machine (SVM). It can be observed from the review that there is a great demand for a new benchmark dataset to evaluate the latest advancements in the field of ML for detecting cyber threats. Existing datasets suffer from limitations such as lack of diversity, insufficient representation of sophisticated attacks, and incomplete data. There is a demand for tailored learning models specifically crafted for cybersecurity applications. The review also suggests that there is a need to explore additional learning methods for the detection of cyber threats. The work presented in (Chethana et al., 2022) [23] employed a DL-based method for identifying different security threats in wireless ad-hoc networks. A trust-based secure routing protocol is designed in this work for mitigating the attacks caused by black hole nodes during routing in mobile ad-hoc networks. The presence of black hole nodes along the route adversely affects the overall network performance by potentially leading to packet loss. Thus, the routing protocol designed in this work minimizes the risk of packet loss caused due to black hole nodes. Through experimental testing, it is ensured that this routing system selects the most secure path for packet delivery between a source and destination. Furthermore, the intrusion of wormholes into wireless networks can lead to network segmentation and routing irregularities. To address this problem, an effective method is designed by utilizing ordinal multidimensional scaling and round trip duration to identify wormholes in wireless ad hoc networks, regardless of their topology density.the utilized datasets, showcasing its superior performance. A hybrid CNN-GRU model is presented in (Imrana et al., 2024).

3. Proposed Research Methodology

The core of the attack detection approach's architecture is the security system's continuous surveillance of network system data traffic to identify and classify various security attack types. To be able to detect cyberattacks in network systems that are introduced into the system by the attackers, a hybrid Convolutional Neural Network (CNN) and Gated Recurrent Unit (GRU) system is used in the attack detection approach. Attackers can take use of system data and get unauthorized access to private network information via opposing network attacks. The CNN-GRU model's performance efficiency is increased and its computational complexity reduced by the selection of important features. The CNN-GRU model is taught to detect and classify cyberattacks using the features that were chosen for every different kind of attack in this study using the RFE and Decision Tree Classifier. The subsections that follow provide a description of each phase in putting the outlined CNN-GRU model for attack detection into effect.

3.1 Data Collection

In this research, the data for the experimental analysis is collected from the CICIDS-2017 (Canadian Institute for Cybersecurity Intrusion Detection Systems Evaluation Dataset 2017) dataset. The dataset consists of information related to network traffic and attack related data. The data is organized into separate CSV files, each representing a different day of the week or a specific type of network activity. The total number of samples considered for the analysis is 154290 out of which 123432 samples are used as training data and 30858 samples are used as validation data with a split ratio of 80:20. For data extraction, initially the dataset is loaded for each day of the week and each .CSV file containing network traffic data is recorded for a specific day or time period, capturing various activities and potentially malicious behavior. After loading the dataset for all the individual days, the data samples for the week are combined into a single comprehensive dataset. This step involves concatenating the separate Data-frames representing each day into one large DataFrame. By doing this, a unified dataset is created that encompasses network traffic data from the entire week, providing a more complete picture of network activity and potential threats.

3.2 Data Preprocessing

After creating a unified dataset, the data is preprocessed to eliminate uncertainties and redundancies from the dataset. The EDA provides insights into data characteristics, facilitating informed preprocessing decisions. In addition, the outliers from the data are removed by defining lower and upper bounds for the values within which data points are considered normal. The values outside these bounds are treated as potential outliers. For each column a “NumPy's np” function is used to replace values outside the upper and lower bounds with the corresponding bounds. This effectively "clips" the values to be within a certain range, removing potential outliers. In addition, a Synthetic Minority Over-sampling Technique (SMOTE) technique is applied to handle the issue of class imbalance. The SMOTE algorithm addresses imbalanced data by oversampling, ensuring the balance within the original training dataset. Instead of restructuring minority class datasets, the SMOTE algorithm creates synthetic instances. This approach mitigates overfitting issues commonly associated with random oversampling. By concentrating on the feature space, SMOTE generates new samples through interpolation among clustered positive samples. By effectively addressing the imbalance issue, the SMOTE algorithm contributes to the high attack detection and classification accuracy.

3.3 Feature Selection

Using a decision tree classifier (DTC) and the Recursive Feature Elimination method, the most critical and relevant features are selected. To extract some of the most significant characteristics from the dataset, using the RFE feature selection method. After the least significant parts have been completely removed multiple times, the process involves developing a model with the remaining features until the required number of features is reached. The DTC is initially developed and employed as an estimator. The estimator is used to initialize the RFE, and a step size is used to define the number of features to be selected. 30 features with a step size equal to one are chosen for investigation in the present investigation.

3.4 CNN-GRU for Attack Detection

The network layers of the CNN and GRU systems merge in the hybrid CNN-GRU model. The layers of the CNN are connected with the GRU model in the hybrid architecture, suggesting that the output of CNN can be mixed with GRU to precisely define the cyberattack. In comparison to a single classifier, hybrid model provides a higher detection accuracy since it combines the outputs of all individual layers of the classifier. In addition, hybrid approaches are capable of handling complex data with high uncertainties and high-dimensional features.

3.4.1 CNN Module

CNN is one of the prominent neural network models extensively utilized in classification tasks, chosen for its capacity to autonomously learn hierarchical features from raw pixel data. This research employs CNN whose architecture consists of convolutional layers, pooling layers, and fully connected (FC) layers. At the input layer, the attack related data is given as input. Convolutional layers, the fundamental building blocks of CNNs which incorporate multiple learnable filters or kernels sliding over input images to extract features. These filters help in detecting specific patterns or features such as type of attack with features becoming increasingly abstract in deeper layers. The network's depth grows with more layers, enhancing its ability to capture complex patterns. Following convolutional layers, FC layers are introduced, where final feature maps are flattened into one-dimensional vectors. These vectors then traverse one or more fully connected (dense) layers responsible for classification. The output layer, comprising multiple units corresponding to classes in the classification task, employs a softmax activation function to generate class probabilities. This layer yields class probabilities for each possible class, with the class possessing the highest probability being deemed the predicted class for the input image.

4. Experimental Results

Accuracy is main defines the percentage of number of correctly identified cyber-attacks which is defined in the below equation:

$$\textbf{\textit{Accuracy}} = \frac{TP+TN}{TP+TN+Fp+FN}$$

Table 2. Comparative Analysis

Algorithm	**Accuracy**
KNN	85 %
DT	86 %
ANN	88 %
CNN-GRU	90%

5. Conclusion

The implementation of a hybrid classifier which utilizes CNN and GRU to identify cyberthreats in computer networks is covered in this research study. The introduction of potential attacks that adversely affect network system performance is one of the major security problems related to network security. In order to identify and detect cyberattacks such as SQL injection attacks, Web attacks, DoS attacks, DDoS attacks, and damage attacks, the CNN-GRU model was created and simulated to continually monitor the network. This work introduces a CNN-GRU hybrid framework. The proposed approach was evaluated using the CICIDS-2017 dataset with a split training and testing ratio of 80% and 20%. To guarantee consistency, the data undergone preparation, and the issue of data imbalance was addressed. In order to make the classification process simpler, all of the relevant and significant features have been selected and extracted from the dataset using an RFE with Decision Tree classifier. For noticing the security attacks, the CNN-GRU model is trained to classify the data instances into normal or attack. Various metrics are employed to assess the hybrid model's performance. The results indicate that the

CNN-GRU model achieves a higher accuracy of 90.11% than the other models used for machine learning in future work detecting more attacks with improve accuracy.

6.References

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

2. 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.

3. 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.

4. 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.

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

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

7. Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber-attacks and its different types. *International Research Journal of Engineering and Technology*, *6*(3), 4849-4852.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

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

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. Dalal, K. R., & Rele, M. (2018, October). Cyber Security: Threat Detection Model based on Machine learning Algorithm. In *2018 3rd International Conference on Communication and Electronics Systems (ICCES)* (pp. 239-243). IEEE.

20. Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In *Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1* (pp. 121-131). Springer Singapore.

21. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419.

22. 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.

23. 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.