JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

INTRUSION DETECTION IN CLOUD COMPUTING NETWORK USING DEEP LEARNING

[1]Mala K, [2]Ranjitha H N, [3]Roopa R

[1]Assistant Professor, Department of ISE, CIT, Gubbi, Tumakuru
[2] Student, Department of ISE, CIT, Gubbi, Tumakuru
[3] Student, Department of ISE, CIT, Gubbi, Tumakuru

Abstract : **Cloud computing (CC) is the rapidly evolving landscape of IT. It focuses on implementing intrusion detection systems (IDS) leveraging deep learning (DL) methodologies. Utilizing hierarchical long short-term memory (HLSTM), the study evaluates its efficacy for feature selection via variance threshold-based regression (VTR) on Bot-IoT and NSL-KDD datasets, achieving notable accuracies of 99.50% and 0.995, respectively. Comparative analysis against existing methods highlights the superiority of DL-based IDS. Additionally, a deep learning model for network intrusion detection (DLNID) is proposed, integrating attention mechanism and bidirectional long short-term memory (Bi-LSTM) networks, surpassing other methods with accuracies of 90.73% and 89.65% on the NSL-KDD dataset. Furthermore, a novel network intrusion detection method combining CNN and Bi-LSTM networks is introduced, achieving an average accuracy improvement to 95.50% and notable reductions in false- positive rate, underscoring the efficacy of DL-based approaches in enhancing intrusion detection performance amidst escalating network threats.**

Index Terms – **Intrusion detection, deep learning, CNN, RNN, Bi-LSTM.**

I.INTRODUCTION

An intrusion detection system (IDS) monitors network activity to identify any potentially dangerous activities. The Internet has fundamentally changed the way people trade information and communicate with one another. However, because cyberattacks continue to grow in frequency and sophistication, these advancements also pose significant cybersecurity risks. Traditional security solutions, such as firewalls, are insufficient for high-security scenarios, even though they can be somewhat successful. This is because these systems require human configuration and cannot respond quickly enough to new threats. To address these problems, intrusion detection systems, or IDSs, have become a crucial component of network security. Intrusion detection systems (IDSs) examine networks to find potentially hazardous activities and alert administrators to it. They employ a variety of detecting methods, including as irregularities, questionable conduct, and acknowledged threats, in that order. The KDD99 dataset, for instance, categorizes a wide range of network attack types, such as denial-of-service and probing attacks. In response to these problems, deep learning (DL) techniques have become more and more popular because of their ability to automatically extract complex features from unprocessed data, eliminating the need for human feature engineering. Deep belief networks(DBNs), convolutional neural networks (CNNs), recurrent neural networks (RNNs), and probabilistic neural networks (PNNs) have all shown encouraging performance in a range of applications, including network intrusion detection. Issues like unequal data distribution and feature correlation persist despite the advancements made in DL-based intrusion detection systems.

To address these issues, a novel DL-based network intrusion detection (DLNID) model is offered. network intrusion over the course of this study. The model uses a combination of an attention mechanism and bidirectional long short-term memory (Bi-LSTM) to accurately identify network data. Additionally, adaptive synthetic sampling is used for data augmentation to ensure adequate learning of minority class samples and lessen imbalanced data distribution. Also employed is a modified stacked autoencoder to decrease data dimensionality and enhance information fusion and detection performance. Information security has become essential due to the rapid growth of computer networks and the substantial and widespread usage of cloud computing technology. The way individuals communicate and access services has radically altered on a global scale thanks to the Internet and cloud computing. However, increased connectivity also brings with it a plethora of new security threats, such as network attacks and data breaches. Among other things, firewalls Considering how quickly established security procedures have shown to be ineffectual in the face of an ever-changing environment.

II.LITERATURE SURVEY

Efficiency of Deep Learning Methods: The use of deep learning methods has emerged as a more efficient approach compared to traditional machine learning methods, particularly in handling high-dimensional data and extracting hierarchical feature representations. Deep learning's ability to learn hierarchical features and capture long-term dependencies contributesto its superior performance in cyber security strategies and data analysis tasks.

Feature Selection and Data Balancing: Feature selection techniques, coupled with deep learning methods, can enhance IDS performance by reducing training complexity and improving accuracy. Additionally, addressing data balancing issues through oversampling techniques and Generative Adversarial Networks (GANs) aids in improving the class distribution of datasets for more effective intrusion detection.

Evaluation Metrics and Dataset Importance: The performance of IDS based on machine learning and deep learning algorithms is evaluated using various statistical metrics suchas accuracy, precision, recall, and F1- score. A good dataset plays a vital role in model training, with up-to-date datasets containing valuable information about new attacks and ensuring balanced class distribution.

Ensemble Learning and Model Performance: Ensemble learning techniques aim to improve the overall performance of IDS by combining multiple classifiers. The superior performance of deep learning methods in IDS is attributed to their high accuracy rates and improved generalization ability compared to traditionalmethods. Intrusion Detection System Architecture: Intrusion detection systems employ a combination of signature-based and learning-based approaches to detect and prevent security breaches in cloud computing environments.

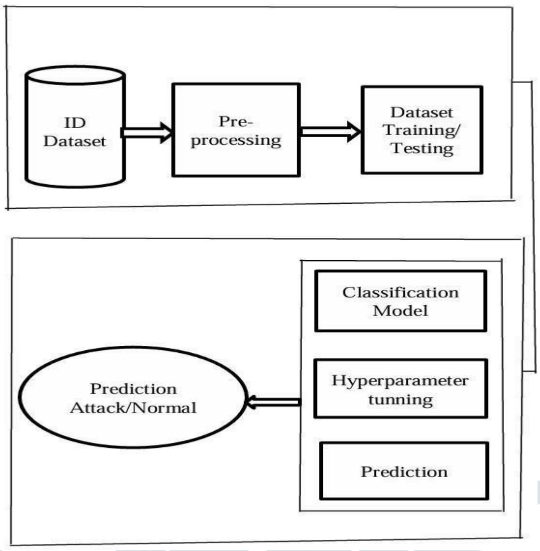
In the domain of intrusion detection within cloud computing networks using deep learning, an expanding corpus of literature highlights the importance and potential of harnessing sophisticated methods to fortify cybersecurity measures. Deep learning methodologies have emerged as efficient strategies, surpassing conventional machine learning techniques, particularly in managing high-dimensional data and extracting hierarchical feature representations. Their capacity to comprehend hierarchical features and capture prolonged dependencies contributes to their enhanced efficacy in cyber security endeavors and data analysis undertakings. When integrated with deep learning techniques, feature selection methodologies have demonstrated the ability to augment the performance of Intrusion Detection Systems (IDS), reducing training complexity and enhancing accuracy. Moreover, the mitigation of data balancing challenges through techniques such as oversampling and Generative Adversarial Networks (GANs) facilitates the enhancement of dataset class distributions, thereby bolstering the effectiveness of intrusion detection efforts.

Commonly employed evaluation metrics, such as accuracy, precision, recall, and F1-score, serve as yardsticks to gauge the performance of IDS grounded on both machine learning and deep learning algorithms. Furthermore, the caliber of the dataset utilized holds pivotal significance in model training endeavors, with contemporary datasets housing valuable insights into emerging threats and ensuring equitable class distributions, thereby influencing the efficacy of intrusion detection systems. Ensemble learning methodologies strive to ameliorate the comprehensive performance of IDS by amalgamating diverse classifiers, leveraging the superior accuracy rates and refined generalization capabilities inherent in deep learning methods.

Several significant studies contribute to our understanding of intrusion detection in cloud computing networks using deep learning. Fasola Olufemi and Oduwole Abdulganiyu (2019) offer an extensive review covering various intrusion detection system (IDS) methodologies, including signature-based, anomaly-based, and hybrid approaches, shedding light on existing challenges and potential areas for advancement. In a pioneering effort, Nguyen Cong Luong et al. (2018) propose a deep learning-based IDS tailored specifically for software-defined networking (SDN) within cloud environments. Through the utilization of convolutional and recurrent neural networks, their model showcases promising capabilities in identifying diverse network attacks, highlighting the efficacy of deep learning in bolstering the security posture of cloud infrastructures.

Additionally, Souvik Pal et al. (2018) explore machine learning-driven IDS solutions customized for cloud computing environments. Their research, which integrates feature selection techniques and employs various classification algorithms like decision trees and support vector machines, underscores the effectiveness of machine learning paradigms in detecting intrusions within cloud networks. Collectively, these studies underscore the growing interest and importance of leveraging deep learning and machine learning techniques to enhance the security resilience of cloud computing networks against evolving cyber threats.

III.METHEDOLOGY



1. Data Collection:

Compile information from a range of cloud network sources. In addition to other pertinent data, this may comprise logs, network traffic information, and system call traces.

2. Preparing the Data:

Eliminate extraneous information and noise from the data. Ascertain that every feature has a comparable scale by normalizing or standardizing the data. Form training, validation, and testing sets out of the data.

3. Feature Engineering:

Take into account pertinent aspects that can be used to discern between harmful and legitimate activity. To find the most discriminative features, this stage may involve trying different things and using domain expertise.

4. Model Selection:

Select the right deep learning architecture to use in intrusion detection. CNNs, or Convolutional Neural Networks,

and Recurrent Neural.

The methodology for detecting intrusions in cloud computing networks using deep learning typically involves several primary stages. Initially, data collection is crucial, where relevant network traffic data from cloud computing setups is amassed, encompassing network packets, logs, and related data. Following this, preprocessing ensues, where the collected data undergoes cleaning, normalization, and transformation to a suitable format for deep learning algorithms. Additionally, feature extraction may be conducted to derive pertinent features from the data, thereby augmenting the model's efficacy.

Subsequently, the construction and training of the deep learning model commence employing the pre process data. Various architectures such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), or their derivatives such as long short-term memory (LSTM) networks may be utilized to capture intricate patterns and dependencies within the network traffic data. The model is trained utilizing label data, wherein instances of normal and malicious network activities are presented to enable the model to discern between them. Model evaluation and validation constitute vital steps to gauge the performance of the trained model. Techniques like cross-validation and metrics including accuracy, precision, recall, and F1-score are commonly employed to evaluate the model's ability to accurately detect intrusions while minimizing false positives. Ultimately, the trained model is deployed within the cloud computing network environment to continuously monitor and identify potential intrusions in real-time, thus enhancing the overall security posture of the cloud infrastructure.

IV.RESULT AND DISCUSSION

In the context of intrusion detection in cloud computing networks utilizing deep learning, research outcomes typically center on evaluating the performance metrics achieved by the developed models. These metrics, including accuracy, precision, recall, F1-score, and possibly the area under the receiver operating characteristic curve (AUC-ROC), serve as measurable indicators of the model's proficiency in accurately detecting intrusions amidst network traffic data. Moreover, the results highlight the model's efficacy in distinguishing normal network activities from various intrusion types, thus underlining its significance in enhancing the security posture of cloud environments.

Additionally, research findings often illuminate challenges encountered during the development and training of deep learning models. Issues such as overfitting, data imbalance, or computational complexity may surface, potentially affecting the intrusion detection system's performance. Researchers typically delve into these challenges, discussing them comprehensively and outlining strategies deployed to address or mitigate them. This discussion not only fosters transparency regarding the limitations of the proposed methodology but also offers valuable insights into potential avenues for refinement and improvement.

The subsequent discussion section of research outcomes delves deeper into the implications of the achieved results. Researchers analyze both the strengths and limitations of the proposed intrusion detection system, drawing comparisons with existing methodologies or benchmarks to demonstrate its efficacy. Furthermore, the discussion may explore potential avenues for further enhancement, such as optimizing model architectures, fine-tuning hyperparameters, or integrating additional data sources. Through critical evaluation and discussion of potential enhancements, researchers contribute to advancing intrusion detection systems in cloud computing networks.

Moreover, the discussion often extends to consider the broader implications of the research within the field of intrusion detection in cloud computing networks. Researchers reflect on how their findings address existing challenges and push forward the state-of-the-art in cybersecurity. Furthermore, they may identify potential real-world applications of their proposed approach and discuss practical implications for cloud security practitioners and stakeholders.

Ultimately, the discussion section serves to contextualize the research outcomes within the wider landscape of intrusion detection in cloud computing networks. By offering valuable insights and recommendations for future research and development endeavors, researchers aim to steer the evolution of intrusion detection systems towards more robust and effective solutions for safeguarding cloud environments against evolving cyber threats.

V.CONCLUSION

Intrusion detection that the significance of theVTR-HLSTM method in enhancing the performance of cloud-based Intrusion Detection Systems (IDS). The recommendation of this method, which involves variance threshold-based regression feature selection coupled with hierarchical Long Short-Term Memory (LSTM) classification, reflects its effectiveness in bolstering the accuracy and efficiency of IDS in cloud computing environments. By leveraging pre-processing techniques such as data normalization and feature selection via Pearson correlation and variance thresholding, the VTR-HLSTM method demonstrates robustness over alternative approaches, as evidenced by metrics including recall, F1-score, precision, accuracy, sensitivity, and specificity. These outcomes underscore the method's suitability for effective intrusion detection within cloud networks, offering improved accuracy while minimizing computation. Moreover, the commendable performance of the VTR-HLSTM method on datasets such as Bot-IoT and NSL-KDD, with achieved accuracies of 99.5% and 99.50% respectively, further validates its efficacy inreal-world scenarios. Looking ahead, the integration of deep learning techniques and feature optimization strategies holds promise for advancing IDS capabilities within cloud networks, paving the way for even more efficient and robust intrusion detection systems.

REFERENCES

[1] G. Nagarajan and P. J. Sajith, “Optimization of BPN parameters using PSO for intrusion detection in cloud environment,” Soft Comput., Jun. 2023, doi: 10.1007/s00500-023-08737-1.

[2] D. Selvapandian and R. Santhosh, “Deep learning approach for intrusion detection in IoT-multi cloud environment,” Autom. Software Eng., vol. 28, no. 2, p. 19, Sep. 2021, doi: 10.1007/s10515-021-00298-7.

[3] X. Wang, “A collaborative detection method of wireless mobile network intrusion based on cloud computing,” Wireless Commun. Mobile Comput., vol. 2022, p. 1499736, Oct. 2022, doi: 10.1155/2022/1499736.

[4] J. Gao, “Network intrusion detection method combining CNN and biLSTM in cloud computing environment,” Comput. Intell. Neurosci., vol. 2022, p. 7272479, Apr. 2022, doi: 10.1155/2022/7272479.

[5] In Soft Computing, June 2023, M.G. Raj and S.K. Pani published "DeepCNN-TL for intrusion detection in fuzzy cloud computing using hybrid feature selection and BWTDO enabled," doi:10.1007/s00500-023-08573-3.

[6] Patel, A.; Qassim, Q.; Wills, C. A survey of intrusion detection and prevention systems. Inf. Manag. Comput. Secur. 2010, 18, 277–290. [Cross Ref]

[7]Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity 2019, 2, 20. [CrossRef]

[8] Tao, P., Sun, Z., and Sun, Z. An enhanced intrusion detection method based on SVM and GA. 13624–13631 in IEEE Access 2018, 6. [Reference Cross]

[9] Haitao, H.; Xiaolin, Z.; Qian, W.; Xinqian, L.; Jiadong, R. a multi-level intrusion detection technique built on random forests and KNN outlier detection. 2019; 56, 566; J. Comput. Res. Dev.

[10] Shapoorifard, H.; Shamsinejad, P.: "A novel hybrid approach for intrusion detection that incorporates an improved KNN." 2017, 173, 5–9; Int. J. Comput. Appl. [Cross Reference]

[11] Kim, G.; Lee, S.; Kim, S.: An innovative hybrid intrusion detection technique that combines misuse and anomaly detection. 2014, 41, 1690–1700; Expert Syst. Appl. [Cross Reference]

[12] Wang, S.; Li, Y.; Su, T.; Sun, H.; Zhu, J. BAT: Using the NSL-KDD dataset, deep learning techniques for network intrusion detection. 2020 IEEE Access, 8, 29575–29585. [Cross Reference]

[13] Srivastava, N., Salakhutdinov, R.; Hinton, G.; Sutskever, I.; Krizhevsky, A. Dropout: An easy method to stop neural networks from overfitting. Journal of Machinist Learning Res. 2014, 15, 1929–1958.

[14] Lin, T., Giles, C.L.; Horne, B.G.; Tino, P.; Long-term dependency learning in NARX Resistant Neural Nets. IEEE Trans. Neural Netw. 7, 1329–1338 (1996–1996). [PubMed]

[15] Tama, B.A.; Comuzzi, M.; Rhee, K. TSE-IDS: An intelligent anomaly-based intrusion detection system using a two-stage classifier ensemble. 2019 IEEE Access 7, 94497–94051. [Cross Reference]

[16] Al-Janabi, S., and Al-Shourbaji, I. (2017). Wireless Network Intrusion Detection and Prevention Systems. Kurdish Journal of Practical Studies, 2(3), 267–272.

[17] Chapman, J. W., & Garbis, J. (2021). Systems for detecting and preventing intrusions. 117–126 in Zero Trust Security. Berkeley, CA: Apress.

[18] Vemuri, R., and Labib, K. (2002). NSOM: A self-organizing map-based intrusion detection system that operates in real-time over a network. 21(1) Networks and Security.

[19] Jasim, Y. A. (2018). Improving intrusion detection systems using artificial neural networks. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 7(1), 49-65.

[20] Ieracitano, C.; Hussain, A.; Adeel, A.; Morabito, F.C. a unique statistical analysis and intelligent intrusion detection method driven by autoencoders. 2020; Neurocomputing, 387: 51–62.[Cross Reference]

[21] Giles, C.L.; Tino, P.; Horne, B.G.; Lin, T. NARX recurrent neural networks: learning long-term dependencies. IEEE Trans. Neural Netw. 7, 1329–1338 (1996–1996). [PubMed] 24.

[22] Hochreiter, S. The issue of the vanishing gradient when learning recurrent neural networks and their solutions. International Journal of Uncertainty in Fuzziness-Based Systems, 6, 107–116, 1998.

[23] Engen, V.; Phalp, K.; Vincent, J. investigating differences in results using the KDD Cup 99 data set. 2011; Intell. Data Anal. 15, 251-276. [Cross Reference]

[24] Jie, H.; Li, S.; Gang, S. Squeeze-and-excitation networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018.

[25] Wang, S.; Li, Y.; Su, T.; Sun, H.; Zhu, J. BAT: Using the NSL-KDD dataset, deep learning techniques for network intrusion detection. 2020 IEEE Access, 8, 29575–29585. [Cross Reference]