International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Strategic Innovations and Future Directions in Deep Learning -Based Intrusion Detection Models

Dr. Jayeshkumar Madhubhai Patel

Associate Professor – PG Department [M.C.A.], Ganpat University, Gujarat, INDIA.

Abstract

With the advancement of deep learning (DL) technology, intrusion detection models based on deep learning have become a significant research topic in the field of cyber security. This paper reviews the datasets commonly employed in such research, laying the groundwork for subsequent studies and analyses. The following section collates the most prevalent data preprocessing methods and feature engineering techniques within intrusion detection, while outlining seven deep learning-based intrusion detection models: deep auto encoders, deep belief networks, deep neural networks, convolutional neural networks, recurrent neural networks, generative adversarial networks, and transformer models. Each model is evaluated from multiple perspectives, emphasising its unique architecture and application scenarios within cyber security. Furthermore, this paper extends the scope to include two large-scale prediction models: methods integrating BERT and GPT series for auxiliary penetration detection. These models leverage the advantages of the Transformer architecture and attention mechanisms, demonstrating exceptional performance in understanding and processing sequential data. Building upon these findings, this paper adopts a forward-looking perspective to explore future research directions, identifying four core research domains.

Keywords: Artificial Intelligence, Deep Learning, Engineering, Systematic Literature Review, Neural Networks, Machine learning algorithm, Deep neural network architectures and convolution neural network

1. Introduction

The rapid development of the Internet has made networks an integral part of personal and professional life. At the same time, the network environment has seen an increase in security vulnerabilities that arise on the very first day[1], Trojan horses, worms, and other forms of attacks that threaten cryptocurrencies. Figure 1 shows the most common types of network attacks. Preventive security mechanisms such as firewalls, policy management, encryption, and authentication have long been the primary means of defense against network attacks[2]. However, these mechanisms are passive protection strategies. The level of security they provide is insufficient to counter internal attacks and is highly dependent on historical traffic data. This has led to the emergence of intrusion detection technologies that can effectively respond to anomalies in the network.

Proactive intrusion detection techniques for addressing network anomalies focus on monitoring network traffic and activities within cybersecurity systems to actively identify and counter potential security

threats. The essence of these technologies lies in moving beyond post hoc analysis and response to detecting anomalous behaviors and traffic in the network, swiftly identifying signs of potential attacks, and implementing appropriate defensive measures before threats materialize. In contrast to traditional passive intrusion detection systems, proactive intrusion detection techniques are more anticipatory and preventive. They can handle a diverse range of threat scenarios and are particularly effective at dealing with unknown attacks and zero-day exploits. These technologies typically integrate various detection methods, such as machine learning algorithms and big data analytics. By actively monitoring and analyzing network activities, the system can promptly intercept or alert administrators about potential threats before attack behaviors cause substantial harm, thereby minimizing security risks to the greatest extent possible. The application of such technologies has transitioned network security from a reactive to a proactive defense stance, thereby offering more effective strategies to counter cyber threats.

2. Methods

This study's research framework was adapted from the model proposed by Borrego et al. The research process was divided into three phases (Identification, Screening, and Analysis), outlined as follows:

2.1 Identification

The first phase employed the search term "deep learning + engineering" to retrieve relevant papers across multiple databases. The databases utilized included Xplore Library, Compendex, Scopus, Google Scholar, Wiley Online Library, Web of Science, and ERIC.

2.2 Screening,

Following the identification phase, articles were screened to determine their relevance to the research topic. Abstracts were initially reviewed against a set of exclusion criteria to filter out irrelevant publications.

2.3 Analysis

Articles selected based on the full text proceed to the synthesis stage. At this stage, a comprehensive analysis of the final articles is conducted. Key details such as title, year of publication, research question, study design, sampling strategy and sample size, data collection methods, and analytical techniques are compiled in a document. Initially, the work is done manually by reading each article and extracting the relevant information. Subsequently, an artificial intelligence tool called Elicit AI was introduced to assist in information extraction. By designing targeted prompts, this tool allows detailed and actionable information to be extracted from each article, with results comparable in quality to manual processing but more efficient. A team of authors manually verifies the results generated by Elicit AI to ensure their accuracy and reliability. While this qualitative synthetic analysis captured key patterns and thematic insights, the research team simultaneously conducted a formal metric analysis of the literature (e.g., citation frequency and journal impact indicators). These quantitative techniques provide added value for future research through a more structured assessment of academic impact and topic evolution.

3. Data Preprocessing Methods and Feature Engineering Techniques

Data preprocessing techniques and feature engineering are essential because they directly affect the performance and accuracy of detection systems. With accurate data preprocessing and feature engineering, intrusion detection systems can identify normal and malicious traffic and distinguish between them with greater accuracy. This improvement increases accuracy and response speed, which is essential for creating an effective intrusion detection system. An intrusion detection model acts as a

classification tool capable of distinguishing between normal and abnormal data in a data set. Preprocessing refers to a series of operations performed before main tasks, such as model training.

Feature engineering techniques are essential for improving model performance because they enable the model to effectively capture patterns and relationships within the data. While data preprocessing focuses on ensuring data quality, feature engineering typically focuses on improving model performance.

Below are some data preprocessing techniques and feature engineering methods commonly used in anomaly detection models.

4. Common Data Preprocessing Methods

4.1. Numerical data processing

This dataset contains symbolic features, while deep learning-based intrusion detection models can only process numerical features [3]. Two common encoding methods are used to convert character features into numerical values: specific label encoding and one-hot encoding [4]. The use of one-hot encoding is a common practice. Its fundamental principle involves encoding multiple states using a multibit state register. One-hot encoding technology was initially employed to convert categorical feature representations into numerical formats. This method divides the features in a dataset into continuous and categorical dimensions. [8]

4.2. Data standardization processing

Even after numerical processing of intrusion detection data, significant disparities between attribute values remain. Without standardization, gradients in the back propagation algorithm may be lost, potentially reducing learning speed and threshold values in intrusion detection models. This hinders effective attribute extraction.[7]

4.3. Handling unbalanced datasets

The model's shortcomings suggest that certain IDS schemes have a lower detection accuracy for specific attacks than the model's overall detection rate, which can be attributed to imbalances in the dataset. The accuracy of detecting low-frequency attacks is lower than the accuracy of detecting high-frequency attacks. This problem can be solved by improving the techniques for handling low-frequency attacks.[9]

4.4. Graphical data processing

Common intrusion detection models require input data to be presented as two-dimensional graphs. For example, the original dimension was 122 after data processing according to Lin et al. [5]. After removing the marked feature columns, the dimension was reduced to 121.

5. Intrusion Detection Model Based on Deep Learning

Since Professor Hinton proposed the theory and technology of deep learning in 2006, some differences between deep learning and machine learning have been carefully analyzed. First, unlike traditional machine learning, which requires manual feature selection, deep learning can automatically learn effective features and directly perform training from start to finish. Second, deep learning is more suitable for processing large amounts of data. At the model training stage, deep learning takes more time than machine learning, but at the testing stage, the advantages of its algorithms become more apparent. Third, deep learning can enhance the feature learning process by step-by-step optimization of feature representation, thereby improving the prediction or classification accuracy of the model. Therefore, current research focuses on deep learning-based intrusion detection models.[6]

6. Summary and conclusion

By exploring intrusion detection technology and related deep learning models, more advanced solutions are provided compared to traditional intrusion detection methods. This article briefly summarizes and analyzes the latest research in the field of intrusion detection systems (IDS) using deep learning, focusing on key areas such as intrusion detection datasets, data preprocessing methods, and model classification. Although many innovative and effective methods have already been proposed and implemented, there is still room for improvement in detection effectiveness in practical applications. Given the rapid proliferation of Internet of Things devices and complex network environments, future deep learning-based intrusion detection models must not only effectively and quickly and accurately recognize complex network traffic, but also address practical challenges such as reducing model size and optimizing performance in resource-constrained environments. Future research will therefore focus on optimizing computational resources and model response times while maintaining high detection accuracy to better adapt to evolving network threats and application scenarios.

References

1 Deep Learning: Concepts, Architectures, Workflow, Applications and Future Directions - Jayeshkumar Madhubhai Patel - IJFMR Volume 5, Issue 6, November-December 2023. DOI 10.36948/ijfmr.2023.v05i06.11497
2 Assortment of Machine Learning model on Gujarati Web Page Sets. CD Patel, J Patel. GRADIVA REVIEW JOURNAL 8 (7), 1081-1087, 2022. 2022
3 Natural computing algorithms–a survey; B Chawda, J Patel; International Journal of Emerging Technology and Advanced Engineering 6 (6)
4 Stock Market Portfolio Management: A Walk-through BV Chawda, JM Patel International Journal on Recent and Innovation Trends in Computing
5 Bharat V. Chawda, Jayeshkumar Madhubhai Patel,"Investigating Performance of Various Natural Computing Algorithms", International Journal of Intelligent Systems and Applications(IJISA), Vol.9, No.1, pp.46-59, 2017. DOI:10.5815/ijisa.2017.01.05
6 Serinelli, B.; Collen, A.; Nijdam, N. Training Guidance with KDD Cup 1999 and NSL-KDD Datasets of ANIDINR: Anomaly-Based Network Intrusion Detection System. Procedia Comput. Sci. 2020, 175, 560–565.
7 Hindy, H.; Atkinson, R.; Tachtatzis, C.; Colin, J.; Bellekens, X. Utilizing Deep Learning Techniques for Effective Zero-Day Attack Detection. Electronics 2020, 9, 1684.
8 Gumusbas, D.; Yildirim, T.; Genovese, A. A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems. IEEE Syst. J. 2020, 15, 1717–1731.
9 Tidjon, L.N.; Frappier, M.; Mammar, A. Intrusion Detection Systems: A Cross-Domain Overview. IEEE Commun. Surv. Tutor. 2019, 21, 3639–3681.