International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

A REVIEW ON ARTIFICIAL INTELLIGENCE BASED INTRUSION DETECTION SYSTEM

Mrs.Maria Sowmini[1], Dr.Isaac Sajan R[2], Dr.M.R.Geetha[3], Mrs. Joselin Kavitha[4]

[1] Assistant Professor, CSE, Ponjesly College of Engineering, Nagercoil.
[2] Professor, ECE, Ponjesly College of Engineering, Email: isaacsajan@gmail.com
[3] Professor & Head, ECE, Ponjesly College of Engineering, Nagercoil.
[4] Assistant Professor ECE, Marthandam College of Engineering & Technology, Kuttakuzhi.

ABSTRACT

Communication technology advances, various and heterogeneous data are communicated in distributed environments through network systems. Meanwhile, along with the development of communication technology, the attack surface has expanded, and concerns regarding network security have increased. Accordingly, to deal with potential threats, research on network intrusion detection systems has been actively conducted. Among the various NIDS technologies, recent interest is focused on artificial intelligence (AI)-based anomaly detection systems, and various models have been proposed to improve the performance of NIDS. However, there still exists the problem of data imbalance, in which AI models cannot sufficiently learn malicious behavior and thus fail to detect network threats accurately. In this study, we propose a novel AI-based NIDS that can efficiently resolve the data imbalance problem and improve the performance of the previous systems. To address the aforementioned problem, we leveraged a state-of-the-art generative model that could generate plausible synthetic data for minor attack traffic.

INTRODUCTION

The development of the fifth-generation (5G) mobile communication technology that diversifies the access environments and constructs distributed networks, various and heterogeneous data are communicated through network systems. In general, these data originate from diverse domains, such as sensors, computers, and the Internet of Things (IoT), and the capacity of network systems has been expanded to process these data reliably. However, as the access points are diversified, the attack surface expands, thereby leaving the network systems vulnerable to potential threats[40].

One of the fundamental challenges in cybersecurity is the detection of network threats, and various results have been reported in the field of network intrusion detection systems (NIDSs). In particular, the most recent studies have been focused on applying the artificial intelligence (AI) technology to NIDS, and AI-based intrusion detection systems have achieved remarkable performance. Initially, the research primarily focused on applying traditional machine learning models, such as decision trees [1] (DTs) and support vector machines [2] (SVMs) to existing intrusion detection systems, and it has now been extended to deep learning approaches [3], such as convolutional neural networks (CNNs), long short-term memory (LSTM), and autoencoders. Although these results have achieved remarkable performance in detecting anomalies, there still exist limitations in deploying them in real systems.

In this study, to address this inherent problem, we propose a novel AI-based NIDS that can resolve the data imbalance problem and improve the performance of the previous systems. To address the aforementioned problem, we leveraged a state-of-the-art deep learning architecture, generative adversarial networks [4] (GANs), to generate synthetic network traffic data. In particular, we focused on the reconstruction error and Wasserstein distance-based GAN architecture [5], which can generate plausible synthetic data for minor attack traffic. By combining the generative model with anomaly detection models, we demonstrated that the proposed systems Moreover, cyber-attack techniques have become more complex and sophisticated, and the frequency of attacks has also increased. Accordingly, the importance of cybersecurity is emphasized, and various studies have been actively conducted to prevent potential network threats.

LITERATURE REVIEW

In the field of AI-based NIDSs, many studies have been conducted to apply machine learning and deep learning technologies as anomaly detection. Ingre and Yadav [10] proposed multilayer perceptron-based intrusion detection system and showed that the proposed approach achieve 81% and 79.9% accuracy in experiments on the NSL-

KDD data set for binary and multiclassification, respectively. Gao et al. [11] proposed a semi-supervised learning approach for NIDSs based on fuzzy and ensemble learning and reported that the proposed system achieved 84.54% accuracy on the NSL-KDD data set. By applying the deep belief network (DBN) model, Alrawashdeh and Purdy, [12] developed an anomaly intrusion detection system and showed that the proposed DBN-based IDS exhibited a superior classification performance in subsampled testing sets (sampled subsets from the original data set). By considering the software-defined networking environment, Tang et al. [13] proposed a DNN-based anomaly detection system and reported that the DNN-based approach outperformed traditional machine learn- ing model approaches (e.g., Naïve Bayes, SVM, and DT). Imamverdiyev and Abdullayeva [14] proposed a restricted Boltzmann machine (RBM)-based intrusion detection system and showed that the Gaussian–Bernoulli RBM model outper-formed other RMB-based models (such as Bernoulli-Bernoulli RBM and DBN). From the perspective of utilizing both behavioral (network traffic characteristics) and content fea- tures (payload information), Zhong et al. [15] introduced a big data and tree architecture-driven deep learning system into the intrusion detection system, where the authors combined shallow learning and deep learning strategies and showed that the system is particularly effective at detecting subtle patterns for intrusion attacks. With the ensemble model-like approach, Haghighat et al. [16] proposed an intrusion detec- tion system based on deep learning and voting mechanisms. Haghighat and Li [16] aggregated the best model results and showed that the system can provide more accurate detec- tions. Moreover, they showed that the false alarms can be reduced up to 75% compared to the conventional deep learn- ing approaches.

Considering data streams in industrial IoT environments, Yang et al. [17] proposed a tree structure- based anomaly detection system, where the authors incorporate the window sliding, detection strategy changing, and model updating mechanisms into the locality-sensitive hashing-based iForest model [18], [19] to handle the infiniteness of data streams in real-time scenario. Similarly, Qi et al. [20] proposed an intrusion detection system for multiaspect data streams by combining locality-sensitive hashing, isolation forest, and prin- cipal component analysis (PCA) techniques. Qi et al. [20] showed that the proposed system can effectively detect group anomalies while dealing with multiaspect data and process each data row faster than the previous approaches.

From the perspective of dealing with time-series data, sev- eral results have been reported focusing on recurrent models. Kim et al. [21] proposed an LSTM-based IDS model and proved the efficiency of the proposed IDS. Yin et al. [22] proposed a recurrent neural network-based intrusion detec- tion system and achieved 83.3% accuracy and 81.3% accuracy in binary and multiclassification, respectively. Xu et al. [23] developed a recurrent neural network-based intrusion detec- tion model and reported that the gated recurrent unit was more suitable as a memory unit for intrusion detection than the LSTM unit. By considering supervisory control and data acquisition (SCADA) networks, Gao et al. [24] proposed an omni-intrusion detection system. Gao et al. [24] com- bined LSTM and a feedforward neural network through an ensemble approach and showed that the proposed system can effectively detect intrusion attacks regardless of tempo- ral correlation. Moreover, they demonstrated that the proposed omni-IDS outperformed previous deep learning approaches through experiments on a SCADA testbed.

In addition to the previous approach of applying supervised learning as an anomaly detection model, several studies have focused on the application of unsupervised learning, espe- cially autoencoder models. Javaid et al. [25] proposed a sparse autoencoder-based NIDS and reported that the proposed model achieved 79.1% accuracy for multiclassification on the NSL- KDD data set. Similarly, Yan and Han [26] leveraged the sparse autoencoder model to extract high-level feature repre-sentations of intrusive behavior information and demonstrated that the stacked sparse autoencoder model could be applied as an efficient feature extraction method. Shone et al. [27] proposed a stacked nonsymmetric deep autoencoder-based intrusion detection system. Shone et al. [27] showed that the proposed model could achieve 85.42% accuracy in multiclassi- fication. As one of the significant results, Ieracitano et al. [28] proposed an autoencoder-driven intrusion detection model. Ieracitano et al. [28] proposed autoencoder-based and LSTM- based IDS models and compared their performance with conventional machine learning models. Through experiments on the NSL-KDD data set, they reported that the proposed autoencoder-based systems outperformed other models and achieved 84.21% and 87% accuracy for binary and multiclas- sification, respectively.

As another approach to applying unsupervised learning, several studies have investigated using generative models to improve the performance of existing NIDS. In particular, they have focused on applying the basic GANs [4], which are based on the Jensen–Shannon divergence (or Kullback– Leibler divergence) [29], [30], [31]. Thereafter, along with the development of various GAN models, studies have been conducted to apply appropriate

GAN models for specific purposes. Li et al. [32] and Lee et al. [33] utilized the Wasserstein divergence-based GAN model to generate the syn- thetic data, and Dlamini et al. [34] proposed a conditional GAN-based anomaly detection model to improve the classi- fication performance in the minority classes. By focusing on specific industrial environments, Li et al. [35] and Alabugin and Sokolov [36] proposed LSTM-GAN and bidirectional GAN-based anomaly detection models, respectively. Through experiments on the secure water treatment (SWaT) data set, they demonstrated that GAN models could be effectively applied to IDS. Siniosoglou et al. [37] proposed an anomaly detection model that could simultaneously detect anomalies and categorize the attack types. Siniosoglou et al. [37] encap- sulated the autoencoder architecture into the structure of the basic GAN model (i.e., deploying the encoder as a discrimina- tor and the decoder as a generator) and proved the efficiency of the proposed model in various smart grid environments.

Unlike previous GAN approaches that are based on the distance between data distributions, we considered the recon- struction error-based GAN model to generate more plausible synthetic data. In particular, we leveraged the boundary equi- librium GAN (BEGAN) model [5], which is based on the concept of autoencoders and the Wasserstein distance between reconstruction error distributions of samples (real and synthetic samples). Moreover, we incorporated the autoencoder model into the detection models to extract meaningful features from the data and extend the adaptability and demonstrated that the AI-based NIDS framework outperforms previous AI-based network intrusion detection models.

CONCLUSION

In this study, we found a novel AI-based NIDS that can efficiently resolve the data imbalance problem and improve the classification performance of the previous systems. To address the data imbalance problem, we leveraged a state-of- the-art generative model that could generate plausible synthetic data and measure the convergence of training. Moreover, autoencoder-driven detection models based on DNN and CNN and found that the AI-based NIDS models outperforms previous machine learning and deep learning approaches. The AI-based NIDS system was analyzed on various data sets, including two benchmark data sets, an IoT data set, and a real data set. In particular, the AI-based NIDS models achieved accuracies of up to 93.2% and 87% on the NSL-KDD data set and the UNSW-NB15 data set, respectively, and showed remarkable performance improvement in the minor classes[40]. In addition, through experiments on an IoT data set, we identified that the AI-based NIDS can efficiently detect network.

REFERENCE

[1] J. R. Quinlan, *C4.5: Programs for Machine Learning* (Morgan Kaufmann Series in Machine Learning). San Mateo, CA, USA: Morgan Kaufmann, 1993.

[2] N. Cristianini and J. Shawe-Taylor, *An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[3] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge,MA, USA: MIT Press, 2016.

[4] I. J. Goodfellow et al., "Generative adversarial nets," in *Proc. 27th Int. Conf. Neural Inf. Process. Syst. (NIPS)*, 2014, pp. 2672–2680.

[5] D. Berthelot, T. Schumm, and L. Metz, "BEGAN: Boundary equilibrium generative adversarial networks,"2017, *arXiv:1703.10717*.

[6] S. Hettich and S. D. Bay. "KDD cup 1999 data." 1999. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[7] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed anal- ysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6.

[8] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),"in *Proc. Military Commun. Inf. Syst. Conf. (MilCIS)*, 2015, pp. 1–6.

[9] A. Parmisano, S. Garcia, and M. J. Erquiaga, "A labeled dataset with malicious and benign IoT network traffic." 2020. [Online]. Available: https://www.stratosphereips.org/datasets-iot23

[10] B. Ingre and A. Yadav, "Performance analysis of NSL-KDD dataset using ANN," in *Proc. Int. Conf. Signal Process. Commun. Eng. Syst.*, Andhra Pradesh, India, Jan. 2015, pp. 92–96.

[11] Y. Gao, Y. Liu, Y. Jin, J. Chen, and H. Wu, "A novel semi-supervised learning approach for network intrusion detection on cloud-based robotic system," *IEEE Access*, vol. 6, pp. 50927–50938, 2018.

[12] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in *Proc. IEEE 15th Int. Conf. Mach. Learn. Appl. (ICMLA)*, Anaheim, CA, USA, 2016, pp. 195–200.

[13] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *Proc. Int. Conf. Wireless Netw. Mobile Commun.(WINCOM)*, 2016, pp. 258–263.

[14] Y. Imamverdiyev and F. Abdullayeva, "Deep learning method for denial of service attack detection based on restricted Boltzmann machine," *Big Data*, vol. 6, no. 2, pp. 159–169, Jun. 2018.
[15] W. Zhong, N. Yu, and C. Ai, "Applying big data based deep learn- ing system to intrusion detection," *Big Data Min. Anal.*, vol. 3, no. 3, pp. 181–195, Sep. 2020.
[16] M. H. Haghighat and J. Li, "Intrusion detection system using vot- ingbased neural network," *Tsinghua Sci. Technol.*, vol. 26, no. 4,pp. 484–495, Aug. 2021.
[17] Y. Yang et al., "ASTREAM: Data-stream-driven scalable anomaly detec- tion with accuracy guarantee in IIoT environment," *IEEE Trans. Netw. Sci. Eng.*, early access, Mar. 8, 2022, doi: 10.1109/TNSE.2022.3157730.
[18] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation-based anomaly detection," *ACM Trans. Knowl. Discov. Data*, vol. 6, no. 1, pp. 1–39, Mar. 2012.
[19] X. Zhang et al., "LSHiForest: A generic framework for fast tree isolation based ensemble anomaly analysis," in *Proc. IEEE 33rd Int. Conf. Data Eng. (ICDE)*, Apr. 2017, pp. 983–994.
[20] L. Qi, Y. Yang, X. Zhou, W. Rafique, and J. Ma, "Fast anomaly identification based on multi-aspect data streams for intelligent intru- sion detection toward secure industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 18, no.9, pp. 6503–6511, Sep. 2022.
[21] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *Proc. Int. Conf. Platform Technol. Service (PlatCon)*, 2016, pp. 1–5.
[22] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intru- sion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.
[23] C. Xu, J. Shen, X. Du, and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018.
[24] J. Gao et al., "Omni SCADA intrusion detection using deep learn-ing algorithms," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 951–961,Jan. 2021.
[25] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," *EAI Endorsed Trans. Security Safety*, vol. 3, no. 9, p. e2, May 2016,
[26] B. Yan and G. Han, "Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system," *IEEE Access*, vol. 6, pp. 41238–41248, 2018.
[27] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2018.
[28] C. Ieracitano, A. Adeel, F. C. Morabito, and A. Hussain, "A novel sta- tistical analysis and autoencoder driven intelligent intrusion detection approach," *Neurocomputing*, vol. 387, pp. 51–62, Apr. 2020.
[29] J. Y. Kim, S. J. Bu, and S. B. Cho, "Malware detection using deep transferred generative adversarial networks," in *Proc. Int. Conf. Neural Inf. Process.*, 2017, pp. 556–564.
[30] M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso, "G-IDS: Generative adversarial networks assisted intrusion detection system," in *Proc. IEEE 44th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jul. 2020, pp. 376–385.
[31] I. Yilmaz, R. Masum, and A. Siraj, "Addressing imbalanced data problem with generative adversarial network for intrusion detection," in *Proc. IEEE 21st Int. Conf. Inf. Reuse Integr. Data Sci. (IRI)*, Las Vegas, NV, USA, 2020, pp. 25–30.
[32] D. Li, D. Kotani, and Y. Okabe, "Improving attack detection performance in NIDS using GAN," in *Proc. IEEE 44th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jul. 2020, pp. 817–825.
[33] W. Lee, B. Noh, Y. Kim, and K. Jeong, "Generation of network traf-fic using WGAN-GP and a DFT filter for resolving data imbalance," in *Proc. Int. Conf. Internet Distrib. Comput. Syst. (IDCS)*, Oct. 2019,pp. 306–317.
[34] G. Dlamini and M. Fahim, "DGM: A data generative model to improve minority class presence in anomaly detection domain," *Neural Comput. Appl.*, vol. 33, pp. 13635–13646, Apr. 2021.
[35] D. Li, D. Chen, J. Goh, and S.-K. Ng, "Anomaly detection with generative adversarial networks for multivariate time series," 2018, *arXiv:1809.04758*.
[36] S. K. Alabugin and A. N. Sokolov, "Applying of generative adversarial networks for anomaly detection in industrial control systems," in *Proc. Global Smart Ind. Conf. (GloSIC)*, Nov. 2020, pp. 199–203.
[37] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A unified deep learning anomaly detection and classification approach for smart grid environments," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1137–1151, Jun. 2021.
[38] D. E. Rumelhart and J. L. McClelland, "Learning internal representations by error propagation," in *Parallel Distributed Processing: Explorations in*

the Microstructure of Cognition: Foundations, vol. 1. Cambridge, MA, USA: MIT Press, 1987, pp. 318–362.

[39] G. E. Hinton and R. S. Zemel, "Autoencoders, minimum description length and helmholtz free energy," in *Proc. 6th Int. Conf. Neural Inf. Process. Syst.*, 1993, pp. 3–10.

[40] C. Park, J. Lee, Y. Kim, J. -G. Park, H. Kim and D. Hong, "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," in *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2330-2345, 1 Feb.1, 2023, doi: 10.1109/JIOT.2022.3211346.